Mandate

As Canada's financial intelligence unit and anti-money laundering and anti-terrorist financing supervisor, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), or 'the Centre', helps to combat money laundering, terrorist activity financing and threats to the security of Canada, while ensuring the protection of personal information under its control.

FINTRAC is one of 13 federal departments and agencies that play a key role in Canada's Anti-Money Laundering and Anti Terrorist Financing regime.

The Centre's mandate is to ensure the compliance of businesses subject to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and associated Regulations, and to generate actionable financial intelligence for police, law enforcement and national security agencies to assist in the investigation of money laundering and terrorist activity financing offences or threats to the security of Canada. The Centre acts at arm's length and is independent from the police services, law enforcement agencies and other entities to which it is authorized to disclose financial intelligence.

FINTRAC is headquartered in Ottawa, with regional offices located in Montréal, Toronto, and Vancouver. It reports to the Minister of Finance, who is in turn accountable to Parliament for the activities of the Centre.

Money laundering

Money laundering is the process used to disguise the source of money or assets derived from criminal activity. There are three recognized stages in the money laundering process:

1. **Placement** involves placing the proceeds of crime in the financial system.
2. **Layering** involves converting the proceeds of crime into another form and creating complex layers of financial transactions to disguise the trail and the source and ownership of funds. This stage may involve transactions such as the buying and selling of stocks, commodities or property.
3. **Integration** involves placing the laundered proceeds back into the economy to create the perception of legitimacy.

The money laundering process is continuous, with new 'dirty' money constantly being introduced into the financial system.

Terrorist activity financing

Terrorist activity financing is the use of funds, property or other services to encourage, plan, assist or engage in acts of terrorism, where the primary motivation is not financial gain.

Two main differences distinguish terrorist activity financing from money laundering:

- Funds can be from legitimate sources, not just criminal acts; and
- Money is the means, not the end—the goal is to use funds to facilitate or implement terrorist activities.

Threats to the security of Canada

FINTRAC's role is to provide CSIS with financial intelligence to assist that agency in fulfilling its mandate of investigating threats to the security of Canada. Threats to the security of Canada are defined in the Canadian Security Intelligence Service Act as:

1. espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage;
2. foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive, or involve a threat to any person;
3. activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political, religious or ideological objective within Canada or a foreign state; and,
4. activities directed toward undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of the constitutionally established system of government in Canada, but does not include lawful advocacy, protest or dissent, unless carried on in conjunction with any of the activities referred to in paragraphs (a) to (d).
5. and intelligence agencies.

Canada's anti-money laundering and anti-terrorist financing regime

FINTRAC occupies an important position in the constellation of organizations involved in Canada's fight against money laundering and terrorism. Each of these organizations has a particular relationship with FINTRAC. Due to the nature of its mandate, the Centre's work is situated at the beginning of a process that starts with the reports to FINTRAC by financial institutions and intermediaries. With the assistance of specialized automated tools, skilled staff analyze the reported transactions and information from other sources to extract financial intelligence that would be relevant to the investigation or prosecution of money laundering offences, terrorist activity financing offences, and threats to the security of Canada.

Money laundering and terrorist financing cases can be extremely complex, often involving many players implicated in transnational and covert illicit activity. The investigations are often time and resource intensive. For this reason, the

time between FINTRAC's initial disclosure and the conclusion of an investigation can be quite lengthy.

FINTRAC's core product is case-specific financial intelligence. FINTRAC is also well situated to provide strategic intelligence about trends and typologies of money laundering and terrorist financing. Because money laundering and terrorist financing are almost always transnational in character, and because an important part of FINTRAC's role is to exchange information with like bodies in other countries, it is also well placed to provide a strategic overview from an international perspective.

The Centre has signed information exchange agreements with certain foreign FIUs worldwide, enabling it to provide financial intelligence to its counterparts that can be crucial to investigations of cases involving the international movement of funds. Equally, it can receive information from these FIUs, which is useful to its own analysis.

When FINTRAC is satisfied that it has reasonable grounds to suspect that the information would be relevant to such investigations or prosecutions, it discloses this financial intelligence to law enforcement and/or intelligence agencies. These agencies, where appropriate, conduct investigations, and if warranted, bring charges against the individuals involved. The recipients of the intelligence include the Royal Canadian Mounted Police (RCMP), provincial and municipal police agencies, CSIS, CRA, IRCC and foreign FIUs with which the Centre has a Memorandum of Understanding (MOU) for the exchange of information.

FINTRAC is also active in many initiatives aimed at fostering international cooperation at the policy level. Notable among these is its participation in the Egmont Group, where FINTRAC is engaged in the sharing of best practices and other activities designed to strengthen support for member countries' anti-money laundering and anti-terrorist financing regimes.

Responsibilities

FINTRAC fulfills its mandate by engaging in the following activities:

- Receiving financial transaction reports and voluntary information in accordance with the PCMLTFA and Regulations;
- Safeguarding personal information under its control;
- Ensuring compliance of reporting entities with the PCMLTFA and Regulations;
- Maintaining a registry of money services businesses in Canada;
- Producing financial intelligence relevant to investigations of money laundering, terrorist activity financing and threats to the security of Canada;
- Researching and analyzing data from a variety of information sources that shed light on trends and patterns in money laundering and terrorist activity financing; and

- Enhancing public awareness and understanding of money laundering and terrorist activity financing.

In addition, FINTRAC is part of the Egmont Group, an international network of financial intelligence units that collaborate and exchange information to combat money laundering and terrorist activity financing.

FINTRAC also contributes to other multilateral fora such as the Financial Action Task Force (FATF), the Asia-Pacific Group on Money Laundering (APG) and the Caribbean Financial Action Task Force (CFATF), lending participation in international policymaking and the provision of technical assistance to other FIUs.

Privacy and protection of personal information

FINTRAC is subject to the *Privacy Act*, which strictly regulates how federal institutions can use and disclose personal information collected about individuals.

In addition, the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* stipulates that FINTRAC is to ensure that the personal information under its control is protected from unauthorized disclosure. Any unauthorized use or disclosure of information is prohibited and can result in severe penalties, including a fine of up to $500,000 or up to five years' imprisonment.

The Act also sets out that information can only be disclosed to law enforcement where there are reasonable grounds to suspect that the information would be relevant to investigating or prosecuting a money laundering offence or a terrorist activity financing offence, or to CSIS when there are reasonable grounds to suspect that it is relevant to threats to the security of Canada. Even in those circumstances, only "designated information" can be disclosed.

A financial transaction report is retained by FINTRAC for ten years. If it was not disclosed, it must be destroyed.

The complementary roles of the Office of the Superintendent of Financial Institutions and FINTRAC

Who is the Office of the Superintendent of Financial Institutions?

The Office of the Superintendent of Financial Institutions (OSFI) is Canada's prudential regulator and supervisor of most banks, federal insurance companies, and trust and loans companies. Its role is to determine whether they are in sound financial condition. OSFI also regulates and supervise federally regulated private pension plans to determine whether they meet their minimum funding requirements.

What does OSFI do?

OSFI is an independent agency of the Government of Canada, established to protect depositors, policyholders, financial institution creditors, and pension plan members, while allowing financial institutions to compete and take reasonable risks.

OSFI's overarching mandate is to contribute to public confidence in the Canadian financial system by:

fostering sound risk management and governance practices through a regulatory framework designed to control and manage risk supervising and intervening early if there are material deficiencies, and taking corrective measures, or requiring that institution act to address the situation monitoring and evaluating system-wide or sectoral developments that may have a negative impact on the financial condition of federally regulated financial institutions balancing the rights and interests of depositors, policyholders, financial institution creditors, and pension plan beneficiaries, while allowing financial institutions to compete effectively and take reasonable risks In 2023, OSFI's mandate was expanded to include ensuring that financial institutions have appropriate policies in place to protect themselves from threats to their integrity and security, including foreign interference.

Prudential regulation and supervision have traditionally focused on financial elements, such as capital and liquidity. Over the last few years, OSFI has focused on non-financial elements, such as technology and cyber, and culture risks. This change recognizes that inadequate mitigation of non-financial risks, just like financial risks, can have prudential consequences.

How does OSFI work with FINTRAC?

FINTRAC's sharing financial intelligence and regulatory compliance information is important to OSFI given its new expanded mandate.

When a financial institution fails to meet its regulatory compliance requirements of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, it could indicate weakness in an institution's risk control environment or corporate culture.

Based on this information, OSFI will undertake supervisory examinations to verify that the institution is adhering to the appropriate regulatory guidelines, as money laundering has a direct impact on the security and integrity of a financial institution, prudential considerations are elevated.

OSFI's high-risk tolerance for early intervention means that it will respond proactively to address where risks could jeopardize the public's confidence in the soundness and integrity of the Canadian financial system, including vulnerabilities associated with money laundering.

Who is FINTRAC?

FINTRAC is Canada's financial intelligence unit and anti-money laundering and anti-terrorist financing supervisor. The Centre helps to combat money laundering, terrorist activity financing, sanctions evasion and threats to the security of Canada.

What does FINTRAC do?

FINTRAC ensures the compliance of thousands of businesses with requirements under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA), including financial entities, securities dealers, life insurance companies, brokers and agents, casinos, money services businesses, and real estate brokers and sales representatives, among others.

With this mandate, FINTRAC is the primary agency responsible for conducting anti-money laundering and anti-terrorist financing assessments of federally regulated financial institutions and ensuring their compliance with the PCMLTFA.

Businesses subject to the PCMLTFA are required to establish a compliance program, identify clients, keep records and report certain types of financial transactions to FINTRAC, including international electronic funds transfers, large cash transactions, large virtual currency transactions, casino disbursements and suspicious transactions.

FINTRAC applies a risk-based approach to ensuring the compliance of businesses subject to the PCMLTFA, including:

Monitoring and assessing the quality, timeliness and volume of financial transaction reporting Undertaking hundreds of supervisory activities every year, including examinations and follow-up examinations Enforcing action plans in cases of non-compliance Issuing administrative monetary penalties Disclosing cases of non-compliance to law enforcement for criminal investigation Compliance with the PCMLTFA helps deter criminals, terrorist financiers and sanctions evaders from using Canada's financial system for illicit purposes. It also ensures that FINTRAC receives the information that it needs to produce financial intelligence to assist in the investigation and prosecution of money laundering, terrorist activity financing, sanctions evasion and threats to the security of Canada.

FINTRAC analyzes the reporting it receives from businesses, as well as the information it receives from law enforcement, government departments and agencies, foreign financial intelligence units and members of the public, to determine whether a disclosure of tactical financial intelligence is required to recipients listed in the Act.

How does FINTRAC work with OSFI?

In fulfilling its core supervisory and financial intelligence mandates, FINTRAC works closely with OSFI.

Under the PCMLTFA and the OSFI Act, FINTRAC and OSFI have respective authorities to share information related to the compliance of federally regulated financial institutions with Parts 1 and 1.1 of the PCMLTFA.

FINTRAC and OSFI can also share compliance-related information for the purpose of assessing risks to the integrity of Canada's financial system that may arise from the grant, revocation, suspension or amendment of an approval under the Bank Act, the Insurance Companies Act and the Trust and Loan Companies Act where this information also relates to money laundering activities or terrorist activity financing.

Separately, the PCMLTFA authorizes FINTRAC to disclose tactical financial intelligence to OSFI where there are reasonable grounds to suspect that the information would be relevant to threats to the security of Canada and that the information is relevant to the exercise of the powers or performance of the duties and functions of the Superintendent of OSFI.

Finally, under the PCMLTFA, FINTRAC is able to share with OSFI its strategic intelligence products related to money laundering, terrorist activity financing, sanctions evasion and the financing of threats to the security of Canada

Reporting suspicious transactions to FINTRAC : FINTRAC's compliance guidance

This guidance explains the requirement to report suspicious transactions to FINTRAC.

1. Who must comply

All reporting entities and their employees must report suspicious transactions.

If you are **a person who is an employee of a reporting entity** and your employer is actively reporting suspicious transactions, we do not require duplicate reporting. An employee is only expected to report suspicious transactions to FINTRAC in the rare instances where they believe that their employer has not submitted a Suspicious Transaction Report as required by the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (the Act) and associated Regulations. To submit a Suspicious Transaction Report in this scenario, the employee may use the paper report form as explained in section 4 below.

A **service provider** can submit and correct a Suspicious Transaction Report on your behalf. However, as the reporting entity, you are ultimately responsible for meeting the requirements under the Act and associated Regulations, even if a service provider is reporting on your behalf. This legal responsibility **cannot** be delegated.

No person or entity will be prosecuted for sending a Suspicious Transaction Report in good faith or for providing FINTRAC with information about suspicions

of money laundering or terrorist financing.

2. What is a Suspicious Transaction Report

A suspicious transaction report is a type of report that you must submit to FINTRAC when a financial transaction occurs, or is attempted, in the course of your activities and there are **reasonable grounds to suspect** that the transaction is related to the commission or the attempted commission of a money laundering or terrorist activity financing offence.

Note: You are not allowed to inform anyone, including the client, of the contents of a Suspicious Transaction Report, or that you have made or will make such a report, if the intent is to prejudice a criminal investigation. This applies whether such an investigation has begun or not. It is important to not tip off your client about the fact that you are filing a Suspicious Transaction Report—therefore, you should not be requesting information that you would not normally request during a transaction if you believe this would tip off the client.

The Suspicious Transaction Report is one of the most valuable and unique report types submitted to FINTRAC. In addition to the prescribed information, Suspicious Transaction Reports allow you to expand the descriptive details surrounding a transaction that is derived from your assessment of what you are seeing through your business interactions and activities.

FINTRAC uses the following types of information in its analysis and production of financial disclosures:

- aliases
- nicknames
- other names and initials
- beneficial ownership information
- IP addresses
- account numbers
- email addresses
- virtual currency transaction addresses and their details
- email money transfers (EMTs)
- mobile money transfers
- details of purchases
- locations
- relationships
- background information

Because of the importance of FINTRAC's financial intelligence to the overall safety and security of Canadians and Canada's financial system, FINTRAC reviews and assesses every Suspicious Transaction Report it receives. When warranted, such as in the case of Suspicious Transaction Reports related to threats to the security of Canada, FINTRAC expedites its analysis in order to disclose financial intelligence to law enforcement and other intelligence partners

within 24 hours.

3. What are reasonable grounds to suspect

Reasonable grounds to suspect is the required threshold to submit a Suspicious Transaction Report to FINTRAC and is a step above simple suspicion, meaning that there is a **possibility** that a money laundering or terrorist activity financing offence has occurred.

You **do not** have to verify the facts, context or money laundering or terrorist activity financing indicators that led to your suspicion, nor do you have to prove that a money laundering or terrorist activity financing offence has occurred in order to reach this threshold. Your suspicion must be reasonable and therefore, not biased or prejudiced.

Reaching this threshold means that you considered:

- the facts
- the context
- the money laundering or terrorist activity financing indicators
- the sanctions evasion characteristics related to a financial transaction

After having reviewed this information, you concluded that there are reasonable grounds to suspect that this particular financial transaction is related to the commission of a money laundering or terrorist activity financing offence. It also means that you are able to demonstrate and articulate your suspicion of money laundering or terrorist activity financing in such a way that another individual with similar knowledge, experience, or training would likely reach the same conclusion based on a review of the same information.

Many factors will support your assessment and conclusion that a money laundering or terrorist activity financing offence has possibly occurred. These factors, along with an explanation of your assessment, should be included in the narrative section of the Suspicious Transaction Report, specifically, the Details of suspicion section.

The reasonable grounds to suspect threshold may be better understood when you have an understanding of other thresholds:

- simple suspicion
- reasonable grounds to believe

Simple suspicion is a lower threshold than reasonable grounds to suspect and is synonymous with a “gut feeling” or “hunch”. In other words, simple suspicion means that you have a feeling that something is unusual or suspicious, but do not have any facts, context or money laundering or terrorist activity financing indicators to support that feeling or to reasonably conclude that a money laundering or terrorist activity financing offence has occurred. Simple suspicion could prompt you to assess related transactions to see if there is any additional information that would support or confirm your suspicion.

Reasonable grounds to believe is a higher threshold than reasonable grounds to suspect and is **beyond** what is required to submit a Suspicious Transaction Report. Reasonable grounds to believe means that there are verified facts that support the **probability** that a money laundering or terrorist activity financing offence has occurred. In other words, there is enough evidence to support a reasonable and trained person to **believe**, **not just suspect**, that a money laundering or terrorist activity financing offence has occurred. For example, **law enforcement** must reach reasonable grounds to believe that criminal activity has occurred before they can obtain judicial authorizations, such as a **production order**.

If you are in receipt of a production order from law enforcement related to a predicate offence, you must perform an assessment of the facts, context, and money laundering or terrorist activity financing indicators to determine whether you have reasonable grounds to suspect that a particular transaction is related to the commission of a money laundering or terrorist activity financing offence.

4. When to submit a Suspicious Transaction Report

You must submit the Suspicious Transaction Report to FINTRAC **as soon as practicable** after you have completed measures that enable you to establish that there are reasonable grounds to suspect that the transaction or attempted transaction is related to the commission of a money laundering or terrorist activity financing offence.

Note: There is no monetary threshold associated with the reporting of a suspicious transaction.

Measures you can take to establish the reasonable grounds to suspect threshold

The measures you can take to establish that there are reasonable grounds to suspect that the transaction or attempted transaction is related to the commission of a money laundering or terrorist activity financing offence include the following:

- screening for and identifying suspicious transactions
- assessing the facts and context surrounding the suspicious transaction
- linking money laundering or terrorist activity financing indicators to your assessment of the facts and context
- explaining your grounds for suspicion in a Suspicious Transaction Report, where you articulate how the **facts**, **context** and **money laundering and terrorist activity financing indicators** allowed you to reach your grounds for suspicion

Your measures must be described in your compliance policies and procedures.

What is a fact A fact, for the purpose of completing a suspicious Transaction Report, is defined as an event, action, occurrence or element that exists or is known to have happened or existed. It cannot be an opinion.

For example:

- Facts about a transaction could include the date, time, location, amount or type.
- Facts known to a reporting entity could include account details, particular business lines, a client's financial history or information about a person or entity (for example, that the person has been convicted of a designated offence or is the subject of a production order, or that an entity is being investigated for fraud or any other indictable offence).

What is context Context, for the purpose of completing a Suspicious Transaction Report, is defined as information that clarifies the circumstances or explains a situation or transaction. This type of information is essential to differentiate between what may be suspicious and what may be reasonable in a given scenario.

You may observe or understand the context of a transaction through:

- a general awareness of the events occurring in a person or entity's business environment or community
- your knowledge of the typical financial activities found within your business
- regular know your client activities (for example, verifying the identity of persons and entities, their occupation or business, how they generate their wealth, their typical or expected transactional behaviours)
- the information obtained through the application of your risk assessment
- illustrative client details (for example, the financial background, behaviour and actions of your client)

A transaction may not appear suspicious in and of itself. However, a review of additional contextual elements surrounding the transaction may create suspicion. Conversely, the context of a particular transaction, which may have seemed unusual or suspicious from the onset, could lead you to reassess your client's current and past transactions and conclude that they are reasonable in that circumstance.

Your suspicion of money laundering or terrorist activity financing will likely materialize from your assessment of multiple elements (transactions, facts, context, and any other related information that may or may not be an indicator of money laundering or terrorist activity financing. When these elements are viewed together, they create a picture that will either support or negate your suspicion of the commission of a money laundering or terrorist activity financing offence.

Examples of how suspicion may arise

- **A person:**
  - asks several questions about your reporting obligations to FINTRAC (context)
  - wants to know how they can avoid their transaction being reported to FINTRAC (context)
  - structures their amounts to avoid client identification or reporting thresholds (fact)
  - keeps changing their explanation for conducting a transaction or knows few details about its purpose (context)
- **Transactions constantly being made on behalf of another person or entity:**
  - a client conducts a transaction while accompanied, overseen or directed by another party (fact)
  - payments to or from unrelated parties (foreign or domestic) (fact)
  - client appears to be or states that they are acting on behalf of another party (context)

For reporting entity sectors that deal with accounts:

- **A person making a deposit to a personal account, where the person:**
  - has an income or job or account history that is not consistent with the deposit amounts (fact)
  - keeps changing their reason for the deposit, and cannot or will not provide a reason (context)
  - exhibits nervous behaviour (context)
- **Transactions to a business account with the following additional elements:**
  - deposits to the account are made by numerous parties that are not signing authorities or employees (fact)
  - the account activity involves wire transfers in and out of the country (fact), which do not fit the expected pattern for that business (context)
- **Transactions frequently being made on behalf of another person or entity:**
  - multiple payments made to an account by non-account holders (fact)
  - account is linked to seemingly unconnected parties (context)

What is a money laundering or terrorist activity financing indicator, or sanctions evasion characteristic Money laundering and terrorist activity financing indicators, and sanctions evasion characteristics are potential red flags that can initiate suspicion and indicate that something may be unusual without a reasonable explanation. Red flags typically stem from one or more facts, behaviours, patterns or other contextual factors that identify irregularities related to a client's transactions. These often present inconsistencies with what is expected or considered normal based on the facts and context you know

about your client and their transactional activities.

Criminal organizations often try to avoid the detection of money laundering or terrorist activity financing by using multiple concealment methods. Indicators of money laundering and terrorist activity financing can bring to light suspicious transactional activity, but it is your holistic assessment of facts, context and money laundering and terrorist activity financing indicators that will enable you to determine whether you have reached reasonable grounds to suspect that a transaction is related to the commission of a money laundering or terrorist activity financing offence. Indicators are also helpful to articulate your rationale for reaching the reasonable grounds to suspect threshold in a Suspicious Transaction Report. The explanation of how you reached your grounds for suspicion is extremely important for FINTRAC's development and disclosure of financial intelligence.

For more information and examples of money laundering and terrorist activity financing indicators applicable to your business sector:

- Consult money laundering and terrorist financing indicators under All FINTRAC guidance – Transaction reporting
- FINTRAC also publishes strategic intelligence products (for example, operational alerts and briefs) that focus on the identification of money laundering or terrorist activity financing related methods, techniques, and vulnerabilities

For information on the characteristics of financial transactions related to suspected sanctions evasion, consult FINTRAC's Special Bulletin on financial activity associated with suspected sanctions evasion.

What is "as soon as practicable" **As soon as practicable** means that you have completed the measures that have allowed you to determine that you reached the reasonable grounds to suspect threshold and as such the development and submission of that Suspicious Transaction Report must be treated as a priority. The greater the delay to submit a Suspicious Transaction Report, the greater the need for a suitable explanation. Suspicious Transaction Reports can be complex, yet you must treat them as a priority and ensure they are timely. You must also complete the measures that allowed you to conclude that you have reasonable grounds to suspect the transaction is related to the commission of a money laundering or terrorist activity financing offence **before** you submit the report to FINTRAC.

Failure to submit a Suspicious Transaction Report, or not submitting one in a timely manner, may impede FINTRAC's ability to carry out its mandate. FINTRAC expects that when you have completed your measures and determined that you have reasonable grounds to suspect that a transaction is related to the commission of a money laundering or terrorist activity financing offence, you will prioritize the submission of that Suspicious Transaction Report.

Note: In situations involving time-sensitive information, such as suspected terrorist financing and threats to national security, you are encouraged, as a best practice, to expedite the submission of your Suspicious Transaction Reports. We recommend that this be included in your compliance policies and procedures.

5. How to submit a report to FINTRAC

You must submit a suspicious transaction report to FINTRAC **electronically** using the following options:

- FINTRAC Web Reporting System (FWR) (geared towards reporting entities with lower reporting volumes)
- FINTRAC API report submission (secure system-to-system transfer of report information)

Paper reporting

If you do **not** have the technical capability to submit reports electronically, you must submit reports in paper form to FINTRAC. You can access and print the Suspicious Transaction Report in paper form on the Paper reporting forms web page, or request to have one faxed or mailed to you by calling 1-866-346-8722.

Changes to a Suspicious Transaction Report

Once you have submitted a Suspicious Transaction Report, it is possible to modify the report, for instance to add missing information or make corrections, but you must provide an explanation for the change.

If you submitted a Suspicious Transaction Report to FINTRAC and need to make a subsequent change to the report, you must make the change and submit the revised report to FINTRAC **within 20 days of the date in which you made the request for change**, based on system requirements.

6. The form for reporting suspicious transactions

Form structure

The form for reporting suspicious transactions has 6 sections:

- General information
- Transaction information
- Starting action
- Completing action
- Details of suspicion
- Action taken

Main sections of the form | Type of information for each section |
General information | - Reporting entity report reference number- Information about your business including contact details- Ministerial Directives |

Transaction information | - Transaction status (completed or attempted)- Reason transaction was not completed (if applicable) - Date and time of transaction - Method of transaction- Location where transaction was conducted or attempted - Purpose of the transaction- Reporting entity transaction reference number |
Starting action | - Direction of starting action (in or out)- Amount and type of funds, assets or virtual currency (in or out)- Currency or virtual currency type- Information about the source of funds, assets or virtual currency - Virtual currency address reference and/or account information - Information about how the funds or virtual currency were obtained- Conductor (person or entity that conducted or attempted the transaction and their associated information)- Third party (person or entity on whose behalf the transaction is conducted or attempted and their associated information) |
Completing action | - Details of disposition- Amount and currency or virtual currency type- Virtual currency address, reference and/or account information- Any other person or entity involved in the completing action and their associated information- Beneficiary (any person or entity that was the beneficiary of the transaction and their associated information) |
Details of suspicion | This is a free form text section where you can describe in clear, simple and concise language your grounds for suspicion of a money laundering, terrorist activity financing or sanctions evasion offence including the facts, context, and indicators that allowed you to reach reasonable grounds for suspicion.In this section, you can indicate:- whether the suspicious activity is related to a money laundering, terrorist activity financing or sanctions evasion offence.- the public-private partnership project name(s)- whether the report includes information about an individual who has been determined to be a politically exposed person- Report reference numbers of previously submitted reports that may relate to the suspicious activity mention in this report |
Action taken | - This is a free form text section where you can describe what action, if any, was or will be taken as a result of the suspicious transaction(s) |
NoteThis table shows the type of information for each section **but does not list every field** on the form.- To access most fields and their category (mandatory, mandatory for processing or reasonable efforts), refer to: - Annex A: Field instructions to complete a Suspicious Transaction Report (which provides instructions on completing the form) |

Structure of the Suspicious Transaction Report form: Main sections and types of information for each section

Form highlights

The structure of the form allows you to include **1 or more transactions** in a report.

- When **entering multiple transactions** into a report, you can enter transactions that have:
  - the same or different transaction status (for example, a report can

include completed transactions and attempted transactions), **and**
  - have taken place at the same or different locations

- For **each completed or attempted transaction**, you must provide all of these details:
  - information obtained about that transaction
  - the details of suspicion
  - the action you have taken in the fields provided in the Suspicious Transaction Report

For example, if you know or obtained the following information, you must provide it in the Suspicious Transaction Report:

- name of the person or entity who completed or attempted to complete the transaction
- type and amount of funds, assets or virtual currency involved in the completed transaction or attempted transaction
- how the funds, assets or virtual currency were used (details of disposition) for a completed transaction or going to be used in an attempted transaction
- whether the person or entity who conducted or attempted the transaction did so on anyone else's behalf
- account details of an account involved in a completed transaction or was going to be involved in an attempted transaction
- For a **completed transaction**, there should be at least **1 starting action** and **1 completing action**.
  - You must also provide the name of the beneficiary to the transaction if you know or obtained this information.
    - For instance, if this transaction had also been submitted to FINTRAC in a different report (LVCTR, LCTR, EFTR, CDR), you may have obtained beneficiary name at that time.
- A transaction can have **multiple starting actions and/or completing actions**—depending on the client's instructions.
  - Within each starting action, you can include multiple conductors, account holders, sources of funds or virtual currency, and third parties.
    - If the conductor or third party is an entity, you can also include information about the entity's director(s), beneficial owner(s), trustee(s), settlor(s), and beneficiary(s) as applicable.
  - Within **each completing action**, you can include multiple account holders, beneficiaries and other persons or entities involved in the completing action.

- **For each starting action, you will need to indicate the direction of the funds, asset or virtual currency** used to start the transaction as either **in** or **out**.
  - The direction of the starting action is **in** when a client physically brings in or electronically transfers in funds, assets or virtual currency to your business to start a transaction.
  - The direction of the starting action is **out** when your client requests to start a transaction with client funds, assets or virtual currency already held by or deposited at your business.

For example:

- The **direction of the starting action is in**, if a client brings cash to your business to purchase a bank draft.
- The **direction of the funds is out for the starting action**, if a client does not bring in any funds but requests to purchase a bank draft with the client's funds already held by or deposited at your business.

Important information about the number of transactions, starting actions and completing actions in a report

- You must complete the General Information section of the report and provide information for each transaction.
- Every transaction must have at least:
  - 1 starting action, and
  - 1 completing action (if available)
- A report can have multiple transactions and within each transaction, you can include multiple starting and completing actions.
- When completing the report, you must ensure that the information you provide reflects your client's instructions and is consistent with your policies and procedures.

Example 1

- On July 10, 2023, Ms. Green walks into branch 1 of Maple Credit Union and deposits $9,900 cash into her savings account.
- On July 11, 2023, Ms. Green walks into branch 2 of Maple Credit Union with a cheque for $20,000 and deposits $12,000 into her savings account and $8,000 into her chequing account.
- On July 12, 2023, Ms. Green walks into branch 1 of Maple Credit Union and instructs that $20,000 be withdrawn from her savings account and transferred to ABC Automotive Company's account at Hemlock Bank.

Based on a review of facts, context and indicators, as well as their procedures to assess suspicious transactions, Maple Credit Union establishes that there are **reasonable grounds to suspect** that the transactions are related to the commission of a money laundering or terrorist activity financing offence.

Therefore, Maple Credit Union submits a Suspicious Transaction Report.

The Suspicious Transaction Report provides general information about Maple Credit Union and indicates that Ms. Green conducted 3 transactions:

- The **first transaction** was conducted at branch 1 on July 10, 2023:
  - **1 starting action** involving $9,900 **cash coming in,** and
  - **1 completing action** where $9,900 is **deposited into a savings account**.
  - As Ms. Green is the **sole account holder**, she is the **beneficiary** of this transaction.
- The **second transaction** was conducted at branch 2 on July 11, 2023:
  - **1 starting action** involving a $20,000 **cheque coming in,** and
  - **2 completing actions** where $12,000 is **deposited into a savings account** and $8,000 is **deposited into a chequing account**.
  - Ms. Green is the **sole account holder** for both accounts and therefore the **beneficiary** of this transaction.
- The **third transaction** was conducted at branch 1 on July 12, 2023:
  - **1 starting action** involving $20,000 **funds withdrawal out,** and
  - **1 completing action**—an **outgoing domestic funds transfer** for $20,000 where ABC Automotive Company is the **beneficiary**.

In the **Details of suspicion section** of the Suspicious Transaction Report, Maple Credit Union provides the facts, context and indicators that allowed it to conclude that there are reasonable grounds to suspect that the transactions are related to the commission or attempted commission of a money laundering or terrorist activity financing offence.

In the **Action taken section**, Maple Credit Union describes the action it has taken.

7. Other requirements associated with suspicious transactions

Compliance program

Your compliance policies and procedures must outline your process and criteria on:

- how you identify and assess Suspicious Transactions Reports
- submitting reports to FINTRAC

If you have an automated or triggering system in place to detect suspicious transactions, a person may still assess the transaction(s), as a best practice, to determine whether there are reasonable grounds to suspect that a transaction is related to the commission of a money laundering or terrorist activity financing offence, and to ensure that, in these cases, the submission of a Suspicious Transaction Report.

Your compliance program must also include **training** on suspected money laundering and terrorist financing activities in relation to your business.

You must also assess the effectiveness of your compliance program as a part of your **two-year effectiveness review**. This includes assessing how effective you are in detecting, assessing and submitting Suspicious Transaction Reports. The following are examples of how this can be done:

- Review previously submitted Suspicious Transaction Reports to ensure that you are consistent in the detection, assessment and submission of these reports.
  - If certain money laundering or terrorist activity financing indicators have supported your suspicions of money laundering or terrorist activity financing, you can assess whether these indicators apply to other situations to ensure that you are not missing suspicious transactions that should be or should have been reported to FINTRAC. This approach can help you build consistency within your organization.
- Work with others in your business sector to learn how they are detecting, assessing and reaching the reasonable grounds to suspect threshold and to establish common ideas of what could be considered unusual or suspicious.

  For more information, consult FINTRAC's strategic intelligence products:
  - Strategic intelligence
- Review a sample of your Suspicious Transaction Reports to assess the timeliness of your reporting of suspicious transactions.
  - Specifically, you can review your business processes to ensure that you are submitting Suspicious Transaction Reports to FINTRAC as soon as practicable after you have completed measures that enable you to determine that there are reasonable grounds to suspect that the transaction or attempted transaction is related to the commission of a money laundering or terrorist activity financing offence.
- Review a sample of your Suspicious Transaction Reports to assess the quality of information reported.
  - This can include reviewing the integrity and consistency of know your client information held by your business and ensuring that all know your client information was included in the Suspicious Transaction Reports.

Large cash transactions

If the suspicious transaction involves a reportable large cash transaction, then you must submit a Large Cash Transaction Reports to FINTRAC **in addition to** a Suspicious Transaction Report.

Electronic funds transfers

If the suspicious transaction involved a reportable electronic funds transfer, then you must submit an Electronic Funds Transfer Report to FINTRAC **in addition to** a Suspicious Transaction Report.

Large virtual currency transactions

If the suspicious transaction involved a reportable large virtual currency transaction, then you must submit a Large Virtual Currency Transaction Report to FINTRAC **in addition to** a Suspicious Transaction Report.

Casino disbursements

If the suspicious transaction involved a reportable casino disbursement, then you must submit a Casino Disbursement Report to FINTRAC **in addition to** a Suspicious Transaction Report.

Terrorist property

In addition to reporting a suspicious transaction, you may also be required to submit a Terrorist Property Reports to FINTRAC if you are required to make a disclosure under the Criminal Code or the Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism.

Record keeping requirements

When you submit a Suspicious Transaction Report to FINTRAC, you must keep a copy of it for **at least 5 years** after the day the report is sent.

Verifying the identity of persons and entities

You are required to take reasonable measures to verify the identity of every person or entity that conducts or attempts to conduct a suspicious transaction. This means that you are expected to ask the client for this information unless you think doing so will tip them off to your suspicion.

Third party determination

There are requirements to determine whether a person or entity is acting on behalf of another person or entity for a financial activity or transaction.

Ministerial directives

You must consider all requirements issued under a ministerial directive along with your suspicious transaction reporting requirements.

Voluntary self-declaration of non-compliance

If you discover instances of non-compliance related to your suspicious transaction reporting requirements, FINTRAC strongly encourages you to report a voluntary self-declaration of non-compliance.

8. Reporting subsequent suspicious transactions

Once you have reached the reasonable grounds to suspect threshold, you must submit a Suspicious Transaction Report. If there are subsequent transactions, you must keep reporting the transactions as long as the suspicion remains.

You are expected to periodically re-assess the client to verify that the level of suspicion has not changed. This process may be part of your documented risk assessment or ongoing monitoring.

If you continue to report Suspicious Transaction Reports on the same person or entity, you can reference a previous Suspicious Transaction Report in the Related Report(s) section by providing all of the following information:

- the reporting entity report reference number and the reporting entity transaction reference number
- the reasonable grounds to suspect (facts, context and money laundering and terrorist financing indicators) that were included in the first Suspicious Transaction Report submission
- any new additional information

If you are reporting Suspicious Transaction Reports due to new facts, context, or money laundering or terrorist activity financing indicators revealed during your assessment of the client, you are expected to detail this new information in the Suspicious Transaction Reports.

- For example, through the course of your assessment, you may have identified new money laundering or terrorist activity financing indicators, or new people or entities transacting with your client. You may choose to include that information under a separate heading in the Details of suspicion section of the Suspicious Transaction Report so that it is properly labeled as new information.

9. FINTRAC's expectations for completing a Suspicious Transaction Report

It is your responsibility to ensure that the information provided in a Suspicious Transaction Report is complete and accurate. It is also important that you submit comprehensive and high quality Suspicious Transaction Report to facilitate FINTRAC's analysis process and disclosure to recipients.

In the narrative sections of the Suspicious Transaction Report: Details of suspicion and Action taken, it is important to **avoid jargon or non-public ref-**

erences, such as terms and acronyms that are specific to your organization. Please use clear, simple and concise language so that an outsider can easily understand the information that you provide.

A variety of information is often collected as part of an assessment to determine if you are required to submit a Suspicious Transaction Report and this information is valuable to include in your report to FINTRAC.

A well-completed Suspicious Transaction Report should consider the following questions:

- **Who** are the parties to the transaction?
  - Provide information on:
    - **conductor(s)**
    - **third party(ies)**
    - **beneficiary(ies)**
    - **account holder(s)**
    - **source(s) of funds or virtual currency**
    - **any other person or entity involved in the transaction(s)**
  - Provide **identifying information** on the parties involved in the transaction. This could include the information you recorded to identify the conductor, as well as any information you have on the other parties to the transaction or its recipients. See the Annexes of the Methods to verify the identity of persons and entities for a summary of information that must be recorded when verifying identity.
  - **When possible**, provide information on:
    - **owner(s)**
    - **director(s)**
    - **officer(s)**
    - **trustee(s)**
    - **settlor(s)**
    - **those with signing authority**
  - If the transaction involves an entity, you can include information on the ownership, control and structure of the business in the Suspicious Transaction Report.
  - Provide **clear information about each person or entity's role** in each of the financial transactions described. For example, it is important to know who is sending and receiving the funds and this can be elaborated in the Details of suspicion section of the Suspicious Transaction Report.
  - **Provide the relationships between the parties (if known).** This is very helpful to FINTRAC when trying to establish networks of persons or entities suspected of being involved in the commission

or attempted commission of a money laundering, terrorist activity financing or sanctions evasion offence.

- **When** was the transaction completed/attempted? If it was not completed, why not?
  - Provide the **facts, context and** money laundering and terrorist activity financing indicators, or sanctions evasion characteristics regarding the transaction
- **What** are the financial instruments or mechanisms used to conduct the transaction?
- **Where** did this transaction take place?
- **Why** are the transaction(s) or attempted transaction(s) related to the commission or attempted commission of a money laundering, terrorist activity financing or sanctions evasion offence?
  - State the money laundering or terrorist activity financing indicators, or sanctions evasion characteristics used to support your suspicion.
  - State the **suspected** criminal offence related to money laundering, terrorist activity financing or sanctions evasion, if known.
- **How** did the transaction take place?

Transactions and their details must be entered in the appropriate structured fields of the form.

- Transactions may be referenced in the narrative section if there are additional facts or context.
- Examples of structured fields where you can enter information include the following **:**
  - a person's alias
  - electronic transfers (such as email money transfers (EMTs) or wire transfers) including IP addresses and sender/recipient email addresses
  - location of automated teller machine (ATM) withdrawals
  - the ownership, control and structure of an entity
  - the source of funds or virtual currency
  - any related and previously submitted Suspicious Transaction Report report reference numbers and transaction reference numbers
  - credit card activity including details of purchases (dates, amounts, retailer (online or in-store) and details of payments (dates, amounts, conductor and source of payment)

If there are transaction details for which there is no structured field for this information, you can include this information in the narrative section of the Suspicious Transaction Report.

- Information provided in the narrative section of the Suspicious Transaction Report can contribute greatly to FINTRAC's analysis. This includes the following types of information:
  - the history the client has with you
  - links made to other people, businesses and accounts
  - information on the ownership, control and structure of an entity that is not already captured in the fields provided in the Suspicious Transaction Report form, particularly for any business entities that have a complex structure
  - the intended or expected use of an account versus the activity you may have observed
  - any other information about your interactions with the client
  - relationships between parties to the transaction
  - the money laundering or terrorist activity financing indicators or factors that assisted in forming the basis of your suspicion
  - any information, including publicly available information and/or information from law enforcement, that made you suspect that the transaction might be related to terrorist financing, money laundering, or both
  - the location where a transaction was conducted, when this location does not belong to your business—for example, the location of a white label ATM that you do not own
  - information on any politically exposed persons, including their names, role and involvement in the transactions being reported
  - any details surrounding why an attempted transaction was not completed
  - any context or clarification about the information that was reported in the structured sections

If there are multiple details for a field, provide the detail that is specific to the transaction.

This may occur for some fields such as the following:

- email address
- telephone number
- URL
- Username
- Device identifier number
- Internet protocol address

For example:

- Your client Billy Bird has three email addresses (Sky@example.ca, Sky22@example.ca and BlueSky@example.ca.); and sends email money transfers (EMTs) to Oscar Ocean who is also your client. Oscar has two email addresses (Starfish@example.ca and Whaleshark@example.ca).
- A recipient, who is not your client, has the email address, Fast-

Car@example.ca and goes by an alias name, “Smitty”.

The email addresses that you report in a Suspicious Transaction Report will depend on the transaction details.

The table below provides some transaction details and the expected email address that should be reported.

Transaction details	Email address to be reported in the Suspicious Transaction Report
Billy Bird sends an outgoing email money transfer (EMT) for $500 using Sky@example.ca to Oscar Ocean at Starfish@example.ca	- Sky@example.ca (conductor email address field) - Starfish@example.ca (beneficiary email address field).
Billy Bird sends an outgoing email money transfer (EMT) for $900 using Sky22@example.ca to Oscar Ocean at Whaleshark@example.ca.	- Sky22@example.ca (conductor email address field) - Whaleshark@example.ca (beneficiary email address field).
Billy Bird sends an outgoing email money transfer (EMT) for $1,000 using Sky22@example.ca to “Smitty” at FastCar@example.ca	- Sky22@example.ca (conductor email address field)- FastCar@example.ca (beneficiary email address field).

Any additional email addresses that you have on your client (and were not related to a specific transaction) can be reported in the Details of suspicion section of the Suspicious Transaction Report. In the example above, you can explain in this section that your client, Billy Bird, has a third email address (BlueSky@example.ca) that was not used in these transactions.

Note: If your client (conductor) is not sending an email money transfer (EMT), you should still report the client’s email address that you have on file in the conductor email address field. If your client has more than one email address, the additional email addresses can be provided in the narrative section of the Suspicious Transaction Report (Details of suspicion).

FINTRAC has been able to identify networks of suspected money launderers and terrorist financiers through pieces of information such as email addresses and secondary identifiers (nicknames) or phone numbers. This type of information may seem insignificant but can be very important to FINTRAC, as it may identify connections among persons, entities or crimes when compared against other FINTRAC intelligence.

The Suspicious Transaction Report structure is intended to encourage reporting even in situations where you may not have information because the client did not provide any or asking for details might “tip off” the client to your suspicions. It is FINTRAC’s expectation that if you have the information within your organization, that it be reported.

10. Common Suspicious Transaction Report deficiencies to avoid

The following are examples of deficiencies that FINTRAC has identified through its assessments and other compliance activities. FINTRAC is sharing these examples to illustrate common errors that you can avoid.

- **Using a higher threshold as your basis for reporting**
  - You are required to submit a Suspicious Transaction Report when you have completed the measures that enable you to establish that there are **reasonable grounds to suspect** that a transaction is related to the commission of a money laundering or terrorist activity financing offence as explained in section 3. Reasonable grounds to believe is a higher threshold than reasonable grounds to suspect and is beyond what is required to submit a Suspicious Transaction Report.
- **Failing to list all the transactions and accounts relevant to your suspicion in the specified fields**
  - You are required to report all the transactions and accounts that led to your determination that there are reasonable grounds to suspect that the transaction is related to the commission or attempted commission of a money laundering or terrorist activity financing offence in the specified fields of the report. Providing a summary of the transactions in the narrative section (Details of suspicion) is not enough.
- **Not providing or naming all parties to the transactions when the information is available**
  - All parties to the transaction, including their associated information, must be provided in their corresponding structured fields if this information is available. This includes any conductors, third parties, beneficiaries, account holders, sources of funds or virtual currency, and any other persons or entities involved in the transaction.
- If an entity is involved, then owners, directors, officers, trustees, settlors and those with signing authority should be provided as applicable. You should also specify whether the parties are known or unknown.
- This has been observed in transactions such as wire transfers that involve multiple parties.
  - For example, if you are reporting a wire transfer, you should include any information you have on both the ordering client and beneficiary. This could include, but is not limited to, their names, their account number and institution, their relationship, and any known identifiers. FINTRAC acknowledges that this information may not always be at your disposal, but when you know it, you should provide it.
- **The information provided in the narrative section of the Suspicious Transaction Report (Details of suspicion) does not elaborate on your grounds for suspicion or link to the transaction(s) in the report**

- You must explain the reason(s) for your determination that there are reasonable grounds to suspect that the transaction(s) is/(are) related to the commission or attempted commission of a money laundering or terrorist financing offence. This includes providing,in the narrative section of the Suspicious Transaction Report,all of the relevant facts, context and money laundering and terrorist activity financing indicators that are related to the transaction(s) in the report and support your suspicion.
- This deficiency has been observed when a reporting entity does not articulate the reasons for their suspicion or does not explain how or why certain information is relevant to their suspicion.

Annex A: Field instructions to complete a Suspicious Transaction Report

This annex contains instructions on how to complete the fields in a Suspicious Transaction Report.

Note:

- Some fields only become applicable on the completion of other fields.
- Some field instructions may only apply to the electronic report submissions and not paper submissions.
- Fields that are **not applicable** are to **be left blank**. When a field is not applicable:
  - **do not enter** "Not applicable", "N/A" or "n/a", or
  - **do not substitute** any other abbreviations, special characters ("x", "-"or "*") or words ("unknown") in the field
- **Failure to provide applicable reporting information** will result in non-compliance and may lead to criminal or administrative penalties.

Standardized field instructions

This section contains instructions for:

- the expected level of effort to obtain the prescribed information for the reporting fields
- completing some fields that appear in multiple sections of the form.

In this section

- Field categories
- Name fields
- Address fields
- Occupation/business fields

- Identification fields
- Telephone number fields

Field categories Fields are categorized as either:

- mandatory
- mandatory for processing
- mandatory if applicable, or
- reasonable measures

Field categories	Instructions
Mandatory	These fields are indicated with an asterisk symbol **(*)** and **must** be completed. However, **in the case of an attempted transaction**, these fields become "reasonable measures" fields and you must take reasonable measures, as indicated in the instructions below, to obtain the information for any mandatory field. Legal references- Proceed of Crime (Money Laundering) and Terrorist Financing Suspicious Transaction Reporting Regulations, SOR/2001-317 - section 11(2)
Mandatory for processing	These fields are indicated with a double dagger symbol **(‡)** and **must** be completed.
Mandatory if applicable	These fields are indicated with a dagger symbol **(†)** and **must** be completed if they are applicable to you or the transaction being reported.

Field categories	Instructions
Reasonable measures	You must take reasonable measures to obtain the information for all non-mandatory fields in the report, **if they are applicable**.Reasonable measures are the steps that you must take, as outlined in your policies and procedures, to obtain the information that can include asking the person or entity involved in the transaction for the information.If you obtain the information, you must report it. You must also provide the information if it is contained within your systems or records.For all fields, you are not required to obtain the information or take reasonable measures to obtain the information if you believe doing so will tip off the person or entity that you are submitting a Suspicious Transaction Report.**Note**: **Fields that are not applicable are to be left blank.**- When a field is not applicable, **do not enter** "Not applicable", "N/A" or "n/a" or substitute any other abbreviations, special characters ("x", "-" or "*") or words ("unknown") in these fields. Legal references- Proceed of Crime (Money Laundering) and Terrorist Financing Suspicious Transaction Reporting Regulations, SOR/2001-317 - section 11(1) - section 11(3)

Instructions for field categories

Name fields

Name fields	Instructions
Surname	Provide the last name of the person.

Name fields	Instructions
Given name	Provide the first name of the person.**Note:** If a person has only a single name, enter "XXX" in the "Given name" field and the person's single name in the "Surname" field.
Other/Initial	Provide the middle or other name(s) of the person, or their initial(s) if no other names apply.
Alias	Provide the name a person uses, or by which they are known, other than the name provided under surname, given name, or other/initial.
Name of entity	Provide the full name of the entity.

Instructions for the name fields

Address fields Provide the address details in the structured or unstructured fields (as applicable) as explained below.

Structured address fields Structured address fields include:

- Apartment/Room/Suite/Unit number
- House/Building number
- Street address
- City
- District
- Country
- Province or state (code) – For provinces or states in Canada, the United States or Mexico, select from the list of options.
- Province or state (name) – For provinces or states outside Canada, the United States or Mexico, provide the name of the province or state.
- Sub-province and/or sub-locality
- Postal or zip code

If you have the ability to separate the information

You must report it in the structured address fields.

For example, if a person lives at #10-123 Main Street, Richmond, British Columbia, Canada A1B 2C3, complete the address fields as follows:

Structured address fields	Information provided
Apartment/Room/Suite/Unit number	10
House/Building number	123

Structured address fields	Information provided
Street address	Main Street
City	Richmond
Country	Canada
Postal code	A1B 2C3

Example illustrating how to provide information if you have the ability to separate address information

If you are unable to separate the address information into the structured address fields

If, for example, your system groups the Apartment/Room/Suite/Unit number with the House/Building number and Street address, then provide:

- all the address information in the street address field
- the city, province, country and postal code in their respective fields

If there is no civic address

If a person or entity's address is in an area where there is **no civic address**, provide a description of the physical location.

For example, if a person lives in the third house to the right after the community center in Tinytown, Saskatchewan, Canada X1Y 2Z2, complete the address fields as follows:

Structured address fields	Information provided
Street address	Third house to the right after the community center
City	Tinytown
Province	SK
Country	Canada
Postal code	X1Y 2Z2

Example illustrating how to provide information if there is no civic address

Note: If you use the structured address fields, you **cannot** use the unstructured address fields to provide additional information.

Unstructured address field You should only use the unstructured address field when it is not possible to separate the address information. This typically occurs when you are uploading a large volume of reports and the data originates from outside your organization. For example, when you are in final receipt of an electronic funds transfer and the foreign address of the person who requested the transfer information cannot be easily populated into the structured address fields.

If possible, enter information about the country in the Country field and provide the unstructured address information in the following format:

- street address/city/province or state/postal code or zip code

Invalid addresses The following **are not valid addresses**, and **should not** be provided in either the structured or unstructured address fields:

- a post office box without a complete physical address (for example, PO Box 333)
- general delivery address
- only a suite number (for example, Suite 256) without additional address information

A **legal land description** can be acceptable as long as the land description is specific enough to pinpoint the physical location of the client's address. If the legal land description refers to an area or a parcel of land on which multiple properties are located, the legal land description would not be sufficient.

Persons who are transient or have no fixed address For **persons who are transient** (for example, travelling in a recreational vehicle or temporarily working in a camp) and have **no fixed address**, you are required to provide the following information:

Type of person	What to provide
Canadian residents	Their permanent Canadian address, even if that is not where they are currently residing
Foreign clients travelling in Canada for a short period of time	Their foreign residential address
Foreign clients living in Canada for a longer period of time (such as a student)	The person's temporary Canadian address

Address information to provide for persons who are transient or have no fixed address

Occupation/business fields

Occupational/business fields	Instructions
Occupation	When entering occupation information, you should be as descriptive as possible. For example, if the person is:- a manager, provide the area of management, such as "hotel reservations manager" or "retail clothing store manager"- a consultant, provide the type of consulting, such as "IT consultant" or "forestry consultant"- a professional, provide the type of profession, such as "petroleum engineer" or "family physician"- a labourer, provide the type of labour performed, such as "road construction worker" or "landscape labourer"- not working, you should still be as descriptive as possible, and indicate "student," "unemployed," "retired," etc. You can enter a numeric classification code and the code title in this field (for example, NOC – National Occupational Classification). However, a numeric code on its own is not sufficient as you need a written description of the occupation as explained above.**Note**: If your client indicates that they are the manager of Blue Moon Auto Parts Ltd., you would enter "manager of auto parts company" in the occupation field and "Blue Moon Auto Parts Ltd." in the name of employer field as explained below.

Occupational/business fields	Instructions
Name of employer	Enter the name of the person's employer.Do not provide the name of a supervisor or manager.This field is meant to capture the name of the business that employs the person.If the person has multiple employers, you only need to provide one but it should be the person's primary employer. Providing the name of employer can augment the description of a person's occupation. For example, "retail clothing store manager for ABC high-end clothing store" and "retail clothing store manager for XYZ discount clothing store" are more descriptive than "retail clothing store manager" on its own.
Nature of entity's principal business	You should be as descriptive as possible when entering the entity's principal business.If the entity's principal business is "sales," provide the type of sales, such as "pharmaceutical sales" or "retail clothing sales." You can enter a numeric classification code **and** the code title in this field (for example, NAICS – North American Industry Classification System). However, a numeric code on its own is not sufficient, as you need a written description of the nature of the entity's principal business as explained above.

Instructions for the occupation/business fields

Identification fields

Identification fields	Instructions
Identifier type	Select the identifier type for the person or entity as applicable.If the identifier type is not listed, select "Other" and provide details.If you use the dual process method to identify a person, you must provide details of both sources of information in the identifier type fields. **Note**: Don't report a Social Insurance Number (SIN) to FINTRAC. In addition, you cannot use documentation for identification purposes where it is prohibited by provincial legislation.For more information on how to identify persons and entities, refer to:- FINTRAC's guidance on Methods to verify the identity of persons and entities
Number associated with identifier type	This is the number indicated on the identifier type that was used to verify the identity of the person or entity. For example, on a driver's licence, the licence number is the identification number and on a Certificate of Incorporation, the incorporation number is the identification number.
Jurisdiction of issue (country, province or state)	Provide the country, province, or state that issued the documentation used to identify the person or entity.

Type of jurisdiction	What and how to provide
A country	Enter that country as the jurisdiction of issue.
A province or state in Canada, the United States or Mexico	Select the province or state **code** from the list of options.
A province or state outside Canada, the United States or Mexico	Provide:- that province or state **name** as the jurisdiction of issue, and- the corresponding country information

How to provide the jurisdiction that issued the documentation used for identification |

Instructions for the identification fields

Telephone number fields

Location of telephone number	Instructions
Canada or the United States	Enter the area code and local number (for example, 999-999-9999).
Outside Canada or the United States	Enter the:- country code- city code, and- local number using a dash (-) to separate each oneFor example, “99-999-9999-9999” would indicate:- a 2-digit country code- a 3-digit city code, and- an 8-digit local number

Instructions for the telephone number fields

Specific field instructions

This section contains instructions for the report fields and are laid out in the same order as they appear on the Suspicious Transaction Report form.

Note: For some fields, the instructions:

- have not been provided and are indicated as “Instructions not specified”
- refer to the Standardized field instructions section

In this section

- General information
- Transaction information
- Starting action
- Completing action
- Details of suspicion
- Action taken

General information

Fields	Instructions
* **Reporting entity number**	You must enroll in FINTRAC Web Reporting System (FWR) to submit reports electronically.Provide the 7-digit identifier number assigned to you by FINTRAC at enrolment.
‡ **Reporting entity report reference number**	A number assigned to each **report** by:- you (the reporting entity), or- the individual or organization submitting the report on your behalfThis number must be **unique to your business, meaning it can only be used once**.

Instructions for the fields under "General information"

Which one of the following types of reporting entities best describes you?

Field	Instructions
* **Activity sector**	Enter your business activity sector.If you are involved in more than 1 type of business activity, indicate the one applicable to the transaction being reported.If there is more than 1 business activity for 1 or more transactions on the report, select only 1 to indicate your principal type of business activity.

Instructions for the question related to the type of reporting entities best describing you

Whom can FINTRAC contact about this report? Enter the contact information of the person you would like FINTRAC to liaise with in the event that a follow up is required.

You must ensure that all of your contacts' information is up to date in FINTRAC Web Reporting System (FWR) prior to submitting your report(s).

Report information

Fields	Instructions
Ministerial directive	If a transaction is being reported to FINTRAC under a ministerial directive, then indicate this by selecting the ministerial directive in the report.Leave this field blank if the transaction(s) are not part of a ministerial directive.**Note**:- Only **one** Ministerial Directive (IR2020) is available for a Suspicious Transaction report. If you select Ministerial Directive, then the report can only contain one transaction. This transaction must be a completed transaction that includes a starting and completing action. In addition, you **must not** complete the "Details of suspicion" and "Action taken" sections of the Suspicious Transaction Report form.- If a transaction is being reported to FINTRAC under a Ministerial Directive **and the transaction also meets the reasonable grounds to suspect threshold**, then you must submit two reports to FINTRAC. In the first report, select Ministerial Directive and do not complete the "Details of suspicion" and "Action taken" sections of the Suspicious Transaction Report form. In the second report, do not select Ministerial Directive but complete all applicable fields of the form, including the "Details of suspicion" and "Action taken" sections.

Instructions for the fields under "Report information"

Transaction information: Transaction 1 of X

Information about the transaction

Fields	Instructions
*** Was the transaction attempted?**	- Select yes if the transaction was attempted. - Select no if the transaction was completed.
†Reason transaction was not completed	If the transaction was not completed, provide the reason.
† Date of transaction	Enter the date of the transaction or attempted transaction. It cannot be a future date and must be different from the posting date.This field is **mandatory**, unless you:- are a financial entity, and - indicate that the transaction was a night deposit or a quick drop.If you do not provide the date of transaction in this field, you **must** provide the date of posting **if** different from date of transaction. Refer to the field Date of posting for more information.
Time of transaction	Enter the time of the transaction or attempted transaction and provide the time zone (that is, UTC offset) based on the location where the transaction or attempted transaction took place (for example, the location of where the cash was received). The time must be entered in the following format: HH:MM:SS±ZZ:ZZ. - For example, 1:25:06 pm in Ottawa, ON would be reported as 13:25:06-05:00.A report can contain multiple transactions that took place in different time zones.If you do not know the time of an attempted transaction, but you are aware of the approximate time frame of when the attempted transaction occurred, you can indicate this in the narrative section of the report (Details of suspicion)—for example, afternoon, morning, between 3 to 4 pm.

Fields	Instructions
*** Method of transaction**	Select the method that describes how the transaction occurred (example, the method that describes how you received the cash, funds, or virtual currency).If the method is not listed, select "Other."**Note**:- "Night deposit" and "quick drop" are **only applicable to financial entities**.- If you select either of these methods of transaction, you **will not be required** to complete the conductor information fields.
† If "Other," please specify	Provide a brief description of the method of transaction.
Date of posting (if different from date of transaction)	Enter the date the transaction is posted, if this differs from the date of the transaction. It cannot be a future date and it must be different from the transaction date.This field is **mandatory if**:- the transaction was a night deposit or quick drop and the date of transaction was not provided, or- the posting date differs from the transaction dateIn all other cases, this is a reasonable efforts field.
Time of posting (if different from the time of transaction)	Enter the time of posting, if this differs from of the time of the transaction.The time must be entered in the following format: HH:MM:SS±ZZ:ZZ. - For example, 1:25:06 pm in Ottawa, ON would be reported as 13:25:06-05:00.
‡ Reporting entity transaction reference number	This is a unique number assigned to **each transaction** by:- you (the reporting entity), or- the individual or organization submitting the report on your behalf

Fields	Instructions
Purpose of transaction	This is the reason for the transaction. The **bolded text** below are examples of purpose of transaction:- A client brings cash tips from his job as a server for deposit into his bank account to **save for the purchase of a home**.- A client purchases jewellery that will be **a gift for a friend**.- A client exchanges Canadian dollars (CAD) to British pound sterlings (GBP) for **vacation purposes**.- A client brings purchases a bank draft in order to **buy a boat**.You may be able to determine the purpose of a transaction by asking the client.

Instructions for the fields under "Information about the transaction"

Information about where the transaction was conducted or attempted
Provide information about the physical location where the transaction took place or was attempted.

For example, if the transaction was conducted at:

- a branch, provide the reporting entity location number of that branch
- an automated teller machine (ATM), provide the reporting entity location number of that ATM

For the following situations, provide the **location number of where the transaction was processed** – this could be a branch location or a head office location, depending on your business process:

- There is no physical location (for instance, the transaction was conducted online).
- The location where the transaction occurred does not belong to your business (for instance the location of a white label ATM that you do not own).

Note:

- Information about a location that does not belong to your business can be provided in the narrative section of the Suspicious Transaction Report.

Field	Instructions
*** Reporting entity location number**	This represents information about where the transaction took place. For example, if the client deposited cash at Branch 1, then select the location number that is associated with Branch 1.If the client conducts a transaction online, then select the location number that is associated with the location that processes the client's online instructions – this could be a branch location or head office location, depending on your business process. The location number is:- created and assigned to you by FINTRAC during the enrolment process to FINTRAC Web Reporting System (FWR), and- maintained by your FWR administrator.For more information about this, contact your FWR administrator.

Instructions for the field under "Information about where the transaction was conducted or attempted"

Starting action Provide information about how the transaction was started.

Fields	Instructions
‡ Direction of Starting Action (In /Out)	Indicate the direction of the starting action as either **in** or **out** for the funds, assets or virtual currency involved. - The direction of the starting action is **in** when a client physically brings in or electronically transfers in funds, assets or virtual currency to your business to start a transaction. - The direction of the starting action is **out** when your client requests to start a transaction with funds, assets or virtual currency already held by or deposited at your business.

Fields	Instructions
‡ Type of funds, assets or virtual currency (In/Out	If the direction of the starting action is **in**, select one of the following based on what the client brought or transferred in to start the transaction:- **Bank draft** – To be used when the client brings in a bank draft to start a transaction. The term bank draft refers to a negotiable instrument that can be used as payment (similar to a cheque). Unlike a cheque though, a bank draft is guaranteed by the issuing bank.- **Cash** – To be used when the client brings in coins or bank notes that are intended for circulation in Canada or coins or bank notes of countries other than Canada to start a transaction.- **Casino product** – To be used when the client brings in chips, plaques, tokens or other casino products to start a transaction.- **Cheque** – To be used when the client brings in a cheque, including personal, certified and casino cheques, to start a transaction. - **Domestic funds transfer** – To be used when the starting action involves the final receipt of funds from within Canada. This includes transfers within the same organization where funds are transferred from one account to another account.- **Email money transfer (EMT)** – To be used when the starting action involves an incoming email transfer using the recipient's email address.- **International funds transfer** – To be used when the starting action involves the final receipt of funds from outside Canada. - **Investment product** – To be used when the starting action involves an incoming transfer of an investment product (for example, transfer of shares from one investment account to another).- **Jewellery** – To be used when the client brings in jewellery to start a transaction. Jewellery means objects made of precious metals, precious stones or pearls that are intended for personal adornment.- **Mobile money transfer** – To be used when the starting action involves an

Fields	Instructions
† If "Other," please specify	Provide a description of the type of funds, assets for virtual currency.
*** Amount**	Enter the total amount of funds, assets or virtual currency involved in the starting action.If this amount **was not** in Canadian dollars (CAD), do not convert it to CAD but provide the currency or virtual currency type in the next field.
† Currency / † Virtual currency type	Enter the fiat currency (including if it was in Canadian dollars) **or** virtual currency of the starting action. If the currency **or** virtual currency type is not in the lists provided, you must select "Other" and provide the full name of the currency.
† If "Other," please specify	If "Other", provide the full name of the currency or virtual currency type.
Exchange rate	Provide the rate of exchange that you used for the transaction. This can be an exchange rate for fiat currency or virtual currency.
† Virtual currency transaction identifier	This is a unique identifier.It is commonly represented by a hash consisting of mixed numerical and alphabetical characters.
† Sending virtual currency address	The sending virtual currency address is made up of a number of alpha-numeric characters. The address length is determined by the type of virtual currency used in the transaction. The sending virtual currency address is associated with whoever is sending the virtual currency (typically the conductor).

Fields	Instructions
† Receiving virtual currency address	The receiving virtual currency address is made up of a number of alpha-numeric characters.The address length is determined by the type of virtual currency used in the transaction.The receiving virtual currency address is associated with whoever is receiving the virtual currency (typically the beneficiary)
† Reference number	If the transaction involved a reference number, provide it in this field.If the transaction involves an account at a **financial entity**, **securities dealer** or **casino**, **do not** provide the account number information in this field **.** The account number must be provided in the Account number field.For all other reporting entities, if you have an internal account number that is used as a reference number, then provide the internal account number in this field.
Other number related to reference number	Provide any other number related to the reference number as applicable.
† Financial institution number	Provide the financial institution number of the account from which the transaction initiated.
† Branch number	Provide the branch number of the account from which the transaction is initiated.
† Account number	If the transaction involves an account at a **financial entity**, **securities dealer** or **casino**, provide the account number. If you are not an account-based reporting entity (for example, a money services business), but the transaction involves an account at an account-based reporting entity (for example, a financial entity), provide that account number in this field.

Fields	Instructions
† Account type	Provide the account typeIf the account type is not in the list provided, you must select "Other" and provide the account type.
† If "Other," please specify	If "Other" is selected, you must provide the account type.
† Account currency	Provide the account currency (fiat) type code.Currencies are represented both numerically and alphabetically, using either three digits or three letters.If the account currency type code can not be found, you must select "Other" and provide the currency (fiat) type.
† Account virtual currency type	Provide the account virtual currency type.If the account virtual currency type is not in the list provided, you must select "Other" and provide the account virtual currency type.
† If "Other," please specify	If "Other" is selected, you must provide the account currency (fiat) type or account virtual currency type.
Date account opened	Provide the date the account was opened.
Date account closed	Provide the date the account was closed.
† Status of account at time of transaction	Provide the status of the account at the time of the transaction (e.g. active, inactive, dormant, closed).
How were the funds or virtual currency obtained?	This is how the conductor initially acquired the funds or virtual currency used for the transaction, **not** where the funds or virtual currency may have been transferred from.For example, you can obtain funds or virtual currency from activities such as:- employment- sale of a large asset, and- giftsThis information must be reported if obtained.

Fields	Instructions
‡ Was information about the source (person/entity) of funds or virtual currency obtained?	This field is a "Yes/No" question.**Select "Yes"** if you have:- the name of any person or entity that is the source of the funds or virtual currency- their account number or policy number, or- an identifying number if there is no account number or policy numberOtherwise, **select "No"** to indicate that you do not have the information.

Instructions for the fields under "Starting action 1 of Y of transaction X"

Account holder Person

Fields	Instructions
† Surname	Refer to Name fields under "Standardized field instructions".
† Given name	Same instructions (Name fields)
Other/initial	Same instructions (Name fields)

Instructions for the fields under "Person 1 of N starting action Z"

Entity

Fields	Instructions
† Name of entity	Refer to Name fields under "Standardized field instructions".

Instructions for the fields under "Entity 1 of N starting action Z"

Source of funds or virtual currency If you have information on any source of funds or virtual currency involved in the transaction, you must report it.

If there are multiple sources, you must provide information for each source.

Person

Fields	Instructions
† Surname	Refer to Name fields under "Standardized field instructions".
† Given name	Same instructions (Name fields)
Other/initial	Same instructions (Name fields)
Account number	Provide the account number for the source of funds.It is acceptable to include the financial institution number and branch number as part of an account number.
Policy number	Instructions not specified
Identifying number	If there is no account or policy number, provide an identifying number if available.

Instructions for the fields under "Person 1 of N of starting action Y"

Entity

Fields	Instructions
† Name of entity	Refer to Name fields under "Standardized field instructions".
Account number	Provide the account number for the source of funds.It is acceptable to include the financial institution number and branch number as part of an account number.
Policy number	Instructions not specified
Identifying number	If there is no account or policy number, provide an identifying number if available.

Instructions for the fields under "Entity 1 of N of starting action Y"

Note about source of funds or virtual currency fields Although the following fields are about how the conductor obtained the funds or virtual currency, they are different:

- How were the funds or virtual currency obtained?
- Was information about the source (person/entity) of funds or virtual currency obtained?
- Source of funds or virtual currency – person or entity

The following example demonstrates the differences.

Example :

Vicky Violet brings in $12,000 cash for deposit into her bank account and tells the bank that she obtained this cash when she sold her car to Griffin Grey.

She was only able to provide Griffin Grey's name to the bank because she did not have information on his account number, policy number or identifying number.

As such, the source of funds or virtual currency fields would be completed as follows:

Source of funds fields	Information provided in t
How were the funds obtained?	**Sale of car**
Was information about the source (person / entity) of funds obtained?	**Yes**
Source of funds	**Griffin Grey**

How the source of funds fields would be completed for this example

Conductor information

Field	Instructions
‡ Have you obtained any conductor information related to this transaction or attempted transaction?	This field is a "Yes/No" question."No" should only be selected if the conductor is **not** your client, **and** after taking reasonable measures, you were not able to obtain **any** conductor details.

Instructions for the fields under "Conductor – indicator"

Fields	Instructions
Surname	Refer to Name fields under "Standardized field instructions".
Given name	Same instructions (Name fields)
Other/Initial	Same instructions (Name fields)
Alias	Same instructions (Name fields)
Client number	A unique identifying number assigned by the reporting entity to the person conducting the transaction.
Apartment/Room/Suite/Unit number	Refer to Address fields under "Standardized field instructions".
House/Building number	Same instructions (Address fields)
Street address	Same instructions (Address fields)

Fields	Instructions
City	Same instructions (Address fields)
District	Same instructions (Address fields)
Country	Same instructions (Address fields)
Province or state	Same instructions (Address fields)
Sub-province and/or sub-locality	Same instructions (Address fields)
Postal or zip code	Same instructions (Address fields)
Unstructured address details	Refer to Unstructured address field under "Standardized field instructions".
Telephone number	Refer to Telephone number fields under "Standardized field instructions".
Extension	Same instructions (Telephone number fields)
Email address	Instructions not specified
URL	Enter the uniform resource location, commonly known as the web address, for the conductor. This includes the URL for personal or business websites, blogs and any social media. If the conductor has more than one URL, provide the main URL in this field and the others in the Details of suspicion section. The URL does not include handles which can be included in the Details of suspicion section.
Date of birth	Instructions not specified
Country of residence	Enter the primary country of residence for the person.It can be the same or different from the country entered in the address section.
Country of citizenship	Enter the primary country of citizenship for the person. It can be same or different from the country entered into the address section.
Occupation	Refer to Occupation/business fields under "Standardized field instructions".
Name of employer	Same instructions (Occupation/business fields)

Instructions for the fields under “Person 1of A of starting action Y”

Fields	Instructions
Apartment/Room/Suite/Unit number	Refer to Address fields under “Standardized field instructions”.
House/Building number	Same instructions (Address fields)
Street address	Same instructions (Address fields)
City	Same instructions (Address fields)
District	Same instructions (Address fields)
Country	Same instructions (Address fields)
Province or state	Same instructions (Address fields)
Sub-province and/or sub-locality	Same instructions (Address fields)
Postal or zip code	Same instructions (Address fields)
Unstructured address details	Refer to Unstructured address field under “Standardized field instructions”.
Telephone number	Refer to Telephone number fields under “Standardized field instructions”.
Extension	Same instructions (Telephone number fields)

Instructions for the fields under “Information about the employer’s address”

Identification of the person

Fields	Instructions
Identifier type	Refer to Identification fields under “Standardized field instructions”.
† If “Other”, please specify	If “Other” identifier type is selected, you must specify the identifier type.
Number associated with identifier type	Same instructions (Identification fields)
Jurisdiction of issue (country)	Same instructions (Identification fields)
Jurisdiction of issue (province or state)	Same instructions (Identification fields)

Instructions for the fields under “Identification of 1 of N of person conductor A”

Fields	Instructions
Type of device used	Provide the type of device used.If "Other" type of device used is selected, you must specify the type of device used.
† If "Other", please specify	If "Other" type of device used is selected, you must specify the type of device used.
Username	A username is how a person or an entity refers to themselves online.
Device identifier number	The device identifier number is a number assigned to the device, such as a Media Access Control (MAC) address or International Mobile Equipment Identity (IMEI) number.
Internet protocol address	Provide the Internet Protocol (IP) address.It is the unique identifying number assigned to every device connected to the internet.
Date and time of online session in which request was made	This is the date and time the conductor accessed the online environment where the transaction was requested.

Instructions for the fields under "Information about conducting or attempting to conduct the transaction online"

Conductor – Entity Provide all the information you have on one, or multiple entities specified as the conductors of the transaction.

Fields	Instructions
Name of entity	Refer to Name fields under "Standardized field instructions".
Client number	A unique identifying number assigned by the reporting entity to the entity conducting the transaction.
Apartment/Room/Suite/Unit number	Refer to Address fields under "Standardized field instructions".
House/Building number	Same instructions (Address fields)
Street address	Same instructions (Address fields)
City	Same instructions (Address fields)
District	Same instructions (Address fields)

Fields	Instructions
Country	Same instructions (Address fields)
Province or state	Same instructions (Address fields)
Sub-province and/or sub-locality	Same instructions (Address fields)
Postal or zip code	Same instructions (Address fields)
Unstructured address details	Refer to Unstructured address field "Standardized field instructions".
Telephone number	Refer to Telephone number fields under "Standardized field instructions".
Extension	Same instructions (Telephone number fields)
Email address	Instructions not specified
URL	Enter the uniform resource location, commonly known as the web address, for the conductor. This includes the URL for personal or business websites, blogs and any social media. If the conductor has more than one URL, provide the main URL in this field and the others in the Details of suspicion section. The URL does not include handles which can be included in the Details of suspicion section.

Instructions for the fields under "Entity 1 of A starting action Y"

Fields	Instructions
Entity structure / type	Provide the entity ownership structure type:- Corporation- Trust- Widely held or publicly traded trust, or - Entity other than a corporation or trust
If "Entity other than a corporation or trust" is selected, please specify	If "Entity other than a corporation or trust" is selected, provide specification.
Nature of entity's principal business	Refer to Occupation/business fields under "Standardized field instructions".

Fields	Instructions
Is the entity registered or incorporated?	This field is a "Yes/No" question.Indicate whether entity is registered or incorporated

Information respecting the structure of Entity 1 of N of entity conductor A

Incorporation of the entity

Fields	Instructions
Incorporation number	Provide the incorporation number of the entity conducting the transaction for each jurisdiction where the entity is incorporated.
Jurisdiction of issue (country) of incorporation	Provide the country that issued the documentation used to identify the entity for each jurisdiction where the entity is incorporated.
Jurisdiction of issue (province or state) of incorporation	Provide the jurisdiction of issue (province or state) of incorporation for each jurisdiction where the entity is incorporatedIf the jurisdiction is a province or state **in** Canada, the United States or Mexico, **select the code from the list of options.**If the jurisdiction is **outside** Canada, the United States or Mexico, **provide the name of the province or state.**

Information under Incorporation 1 of N of entity conductor A

Registration of the entity

Fields	Instructions
Registration number	Provide the registration number of the entity conducting the transaction for each jurisdiction where the entity is registered.For Canadian entities, a registration number can include the 9-digit business number assigned to that entity by the Canadian Revenue Agency (CRA)
Jurisdiction of issue (country) of registration	Provide the country that issued the documentation for each jurisdiction where the entity is registered.
Jurisdiction of issue (province or state) of registration	Provide the jurisdiction of issue (province or state) for each jurisdiction where the entity is registeredIf the jurisdiction is a province or state **in** Canada, the United States or Mexico, **select the code from the list of options.**If the jurisdiction is **outside** Canada, the United States or Mexico, **provide the name of the province or state.**

Registration 1 of N of entity conductor A

Identification of the entity Provide the following information that was used to verify the identity of the entity. For some entities, this information may be the same as the registration or incorporation information.

Fields	Instructions
Identifier type	Refer to Identification fields under "Standardized field instructions".
† If "Other", please specify	If "Other" identifier type is selected, you must specify the identifier type.
Number associated with identifier type	Same instructions (Identification fields)
Jurisdiction of issue (country)	Same instructions (Identification fields)
Jurisdiction of issue (province or state)	Same instructions (Identification fields)

Instructions for the fields under "Identification 1 of N of entity conductor A"

Person authorized to bind the entity or act with respect to the account (maximum 3) If the conductor is an entity, you must provide the information for **up to 3 persons** who are authorized to:

- bind the entity, or
- act with respect to the account

Fields	Instructions
Surname	Refer to Name fields under "Standardized field instructions".
Given name	Same instructions (Name fields)
Other/Initial	Same instructions (Name fields)

Instructions for the fields under "Person 1 of N (max 3)"

Entity Structure/Type: Corporate Information

Director(s) of a corporation

Fields	Instructions
Surname	Refer to Name fields under "Standardized field instructions".
Given name	Same instructions (Name fields)
Other/Initial	Same instructions (Name fields)
Apartment/Room/Suite/Unit number	Refer to Address fields under "Standardized field instructions".
House/Building number	Same instructions (Address fields)
Street address	Same instructions (Address fields)
City	Same instructions (Address fields)
District	Same instructions (Address fields)
Country	Same instructions (Address fields)
Province or state	Same instructions (Address fields)
Sub-province and/or sub-locality	Same instructions (Address fields)
Postal or zip code	Same instructions (Address fields)
Unstructured address details	Refer to Unstructured address field under "Standardized field instructions".
Telephone number	Refer to Telephone number fields under "Standardized field instructions".
Extension	Same instructions (Telephone number fields)

Instructions for the fields under "Director 1 of N of starting action Y"

Person who directly or indirectly owns or controls 25% or more shares of the corporation

Fields	Instructions
Surname	Refer to Name fields under "Standardized field instructions".
Given name	Same instructions (Name fields)
Other/Initial	Same instructions (Name fields)

Instructions for the fields under "Person 1 of N of starting action Y"

Trust Information Trustee(s) of a trust

Fields	Instructions
Surname	Refer to Name fields under "Standardized field instructions".
Given name	Same instructions (Name fields)
Other/Initial	Same instructions (Name fields)
Apartment/Room/Suite/Unit number	Refer to Address fields under "Standardized field instructions".
House/Building number	Same instructions (Address fields)
Street address	Same instructions (Address fields)
City	Same instructions (Address fields)
District	Same instructions (Address fields)
Country	Same instructions (Address fields)
Province or state	Same instructions (Address fields)
Sub-province and/or sub-locality	Same instructions (Address fields)
Postal or zip code	Same instructions (Address fields)
Unstructured address details	Refer to Unstructured address field under "Standardized field instructions".
Telephone number	Refer to Telephone number fields under "Standardized field instructions".
Extension	Same instructions (Telephone number fields)

Instructions for the fields under "Trustee 1 of N of starting action Y"

Settlor(s) of a trust

Fields	Instructions
Surname	Refer to Name fields under "Standardized field instructions".
Given name	Same instructions (Name fields)
Other/Initial	Same instructions (Name fields)
Apartment/Room/Suite/Unit number	Refer to Address fields under "Standardized field instructions".
House/Building number	Same instructions (Address fields)
Street address	Same instructions (Address fields)
City	Same instructions (Address fields)
District	Same instructions (Address fields)
Country	Same instructions (Address fields)
Province or state	Same instructions (Address fields)
Sub-province and/or sub-locality	Same instructions (Address fields)
Postal or zip code	Same instructions (Address fields)
Unstructured address details	Refer to Unstructured address field under "Standardized field instructions".
Telephone number	Refer to Telephone number fields under "Standardized field instructions".
Extension	Same instructions (Telephone number fields)

Instructions for the fields under "Settlor 1 of N of starting action Y"

Widely held or publicly traded trust information Person who directly or indirectly owns or controls 25% or more units of a widely held or publicly traded trust

Fields	Instructions
Surname	Refer to Name fields under "Standardized field instructions".
Given name	Same instructions (Name fields)
Other/Initial	Same instructions (Name fields)
Apartment/Room/Suite/Unit number	Refer to Address fields under "Standardized field instructions".
House/Building number	Same instructions (Address fields)
Street address	Same instructions (Address fields)
City	Same instructions (Address fields)
District	Same instructions (Address fields)
Country	Same instructions (Address fields)

Fields	Instructions
Province or state	Same instructions (Address fields)
Sub-province and/or sub-locality	Same instructions (Address fields)
Postal or zip code	Same instructions (Address fields)
Unstructured address details	Refer to Unstructured address field under "Standardized field instructions".
Telephone number	Refer to Telephone number fields under "Standardized field instructions".
Extension	Same instructions (Telephone number fields)

Instructions for the fields under "Person 1 of N of starting action Y"

Beneficiary(ies) of a trust, other than a widely held or publicly traded trust

Fields	Instructions
Surname	Refer to Name fields under "Standardized field instructions".
Given name	Same instructions (Name fields)
Other/Initial	Same instructions (Name fields)
Apartment/Room/Suite/Unit number	Refer to Address fields under "Standardized field instructions".
House/Building number	Same instructions (Address fields)
Street address	Same instructions (Address fields)
City	Same instructions (Address fields)
District	Same instructions (Address fields)
Country	Same instructions (Address fields)
Province or state	Same instructions (Address fields)
Sub-province and/or sub-locality	Same instructions (Address fields)
Postal or zip code	Same instructions (Address fields)
Unstructured address details	Refer to Unstructured address field under "Standardized field instructions".
Telephone number	Refer to Telephone number fields under "Standardized field instructions".
Extension	Same instructions (Telephone number fields)

Instructions for the fields under “Beneficiary 1 of N of starting action Y”

Entity other than a corporation or trust information Person who directly or indirectly owns or controls 25% or more of an entity other than a corporation or trust

Fields	Instructions
Surname	Refer to Name fields under “Standardized field instructions”.
Given name	Same instructions (Name fields)
Other/Initial	Same instructions (Name fields)

Instructions for the fields under “Person 1 of N of starting action Y”

Fields	Instructions
Type of device used	Provide the type of device used.If “Other” type of device used is selected, you must specify the type of device used.
† If “Other”, please specify	If “Other” type of device used is selected, you must specify the type of device used.
Username	A username is how a person or an entity refers to themselves online.
Device identifier number	The device identifier number is a number assigned to the device, such as a Media Access Control (MAC) address or International Mobile Equipment Identity (IMEI) number.
Internet protocol address	Provide the Internet Protocol (IP) address.It is the unique identifying number assigned to every device connected to the internet.
Date and time of online session in which request was made	This is the date and time the conductor accessed the online environment where the transaction was requested.

Instructions for the fields under “Information about conducting or attempting to conduct the transaction online”

On behalf of On behalf of indicator

Field	Instructions
‡ Was this transaction conducted or attempted on behalf of another person or entity?	This field is a "Yes/No" question.Select "Yes" if the transaction was conducted on behalf of another person or entity.The "on behalf of" party is also known as:- the "third party", or- the party providing instructions for the transaction**If the transaction was conducted on behalf of another person, you must include the relevant information below.**

Instructions for the field under "On behalf of indicator"

Fields	Instructions
Surname	Refer to Name fields under "Standardized field instructions".
Given name	Same instructions (Name fields)
Other/Initial	Same instructions (Name fields)
Alias	Same instructions (Name fields)
Client number	Instructions not specified
Apartment/Room/Suite/Unit number	Refer to Address fields under "Standardized field instructions".
House/Building number	Same instructions (Address fields)
Street address	Same instructions (Address fields)
City	Same instructions (Address fields)
District	Same instructions (Address fields)
Country	Same instructions (Address fields)
Province or state	Same instructions (Address fields)
Sub-province and/or sub-locality	Same instructions (Address fields)
Postal or zip code	Same instructions (Address fields)
Unstructured address details	Refer to Unstructured address field under "Standardized field instructions".
Telephone number	Refer to Telephone number fields under "Standardized field instructions".
Extension	Same instructions (Telephone number fields)

Fields	Instructions
URL	Enter the uniform resource location, commonly known as the web address, for the conductor. This includes the URL for personal or business websites, blogs and any social media. If the conductor has more than one URL, provide the main URL in this field and the others in the Details of suspicion section. The URL does not include handles which can be included in the Details of suspicion section.
Email address	Instructions not specified
Date of birth	Instructions not specified
Country of residence	Enter the primary country of residence for the person.It can be the same or different from the country entered in the address section.
Country of citizenship	Enter the primary country of citizenship for the person. It can be same or different from the country entered into the address section.
Occupation	Refer to Occupation/business fields under "Standardized field instructions".
Name of employer	Same instructions (Occupation/business fields)

Instructions for the fields under "Person 1 of B of conductor A"

Fields	Instructions
Apartment/Room/Suite/Unit number	Refer to Address fields under "Standardized field instructions".
House/Building number	Same instructions (Address fields)
Street address	Same instructions (Address fields)
City	Same instructions (Address fields)
District	Same instructions (Address fields)
Country	Same instructions (Address fields)
Province or state	Same instructions (Address fields)
Sub-province and/or sub-locality	Same instructions (Address fields)
Postal or zip code	Same instructions (Address fields)

Fields	Instructions
Unstructured address details	Refer to Unstructured address field under "Standardized field instructions".
Telephone number	Refer to Telephone number fields under "Standardized field instructions".
Extension	Same instructions (Telephone number fields)

Instructions for the fields under "Information about the employer's address"

Identification of person on whose behalf the transaction was conducted

Fields	Instructions
Identifier type	Refer to Identification fields under "Standardized field instructions".
† If "Other", please specify	If "Other" identifier type is selected, you must specify the identifier type.
Number associated with identifier type	Same instructions (Identification fields)
Jurisdiction of issue (country)	Same instructions (Identification fields)
Jurisdiction of issue (province or state)	Same instructions (Identification fields)

Instructions for the fields under "Identification 1 of N on behalf of person B"

Fields	Instructions
Type of device used	Provide the type of device used.If "Other" type of device used is selected, you must specify the type of device used.
† If "Other". Please specify	If "Other" is selected, specify the type of device used.
Username	A username is how a person or an entity refers to themselves online.
Device identifier number	The device identifier number is a number assigned to the device, such as a Media Access Control (MAC) address or International Mobile Equipment Identity (IMEI) number.

Fields	Instructions
Internet protocol address	Provide the Internet Protocol (IP) address.It is the unique identifying number assigned to every device connected to the internet.
Date and time of online session in which request was made	This is the date and time the conductor accessed the online environment where the transaction was requested.

Instructions for the fields under "Information about conducting or attempting to conduct the transaction online"

Fields	Instructions
Relationship	Select the relationship of the "on behalf of" party to the person or entity conducting the transaction.The "on behalf of" party is understood to be the person or entity that instructs the person or entity conducting the transaction.
† If "Other", please specify	If "Other" is selected, specify the relationship of the "on behalf of" party to the person or entity conducting the transaction.

Instructions for the fields under "Relationship of the person named above to the person or entity conducting or attempting to conduct the transaction"

If the transaction was conducted on behalf of another entity, you must include the relevant information.

Fields	Instructions
Name of entity	Refer to Identification fields under "Standardized field instructions".
Client number	Instructions not specified
Apartment/Room/Suite/Unit number	Refer to Address fields under "Standardized field instructions".
House/Building number	Same instructions (Address fields)
Street address	Same instructions (Address fields)
City	Same instructions (Address fields)
District	Same instructions (Address fields)

Fields	Instructions
Country	Same instructions (Address fields)
Province or state	Same instructions (Address fields)
Sub-province and/or sub-locality	Same instructions (Address fields)
Postal or zip code	Same instructions (Address fields)
Unstructured address details	Refer to Unstructured address field under "Standardized field instructions".
Telephone number	Refer to Telephone number fields under "Standardized field instructions".
Extension	Same instructions (Telephone number fields)
Email address	Instructions not specified
URL	Enter the uniform resource location, commonly known as the web address, for the conductor. This includes the URL for personal or business websites, blogs and any social media. If the conductor has more than one URL, provide the main URL in this field and the others in the Details of suspicion section. The URL does not include handles which can be included in the Details of suspicion section.

Instructions for the fields under "Entity 1 of B of conductor A"

Fields	Instructions
Entity structure / type	Provide the entity ownership structure type:- Corporation- Trust- Widely held or publicly traded trust, or - Entity other than a corporation or trust
If "Entity other than a corporation or trust" is selected, please specify	If "Entity other than a corporation or trust" is selected, provide specification.
Nature of entity's principal business	Refer to Occupation/business fields under "Standardized field instructions".

Fields	Instructions
‡Do you have incorporation or registration information?	This field is a "Yes/No" question.Select "Yes" if you have the information.Select 'No' if you do not have the information.
Incorporated or registered?	Provide the incorporation or registration type:- Incorporated- Registered- Incorporated and registered, or - Unknown

Instructions for the fields under "Information respecting the structure of Entity 1 of B"

Incorporation of the entity

Fields	Instructions
Incorporation number	Provide the incorporation number of the entity conducting the transaction for each jurisdiction where the entity is incorporated.
Jurisdiction of issue (country) of incorporation	Provide the country that issued the documentation used to identify the entity for each jurisdiction where the entity is incorporated.
Jurisdiction of issue (province or state) of incorporation	Provide the jurisdiction of issue (province or state) of incorporation for each jurisdiction where the entity is incorporatedIf the jurisdiction is a province or state **in** Canada, the United States or Mexico, **select the code from the list of options.**If the jurisdiction is **outside** Canada, the United States or Mexico, **provide the name of the province or state.**

Instructions for fields under "Incorporation 1 of N of entity B"

Registration of the entity

Fields	Instructions
Registration number	Provide the registration of the entity conducting the transaction For Canadian entities, a registration number can include the 9-digit business number assigned to that entity by the Canada Revenue Agency (CRA).
Jurisdiction of issue (country) of registration	Provide the country that issued the documentation for each jurisdiction where the entity is registered.
Jurisdiction of issue (province or state) of registration	Provide the jurisdiction of issue (province or state) for each jurisdiction where the entity is registeredIf the jurisdiction is a province or state **in** Canada, the United States or Mexico, **select the code from the list of options.**If the jurisdiction is **outside** Canada, the United States or Mexico, **provide the name of the province or state.**

Instructions for fields under "Registration 1 of N of entity B"

Identification of the entity on whose behalf the transaction was conducted Provide the following information that was used to verify the identity of the entity on whose behalf the transaction was conducted.

For some entities, this information may be the same as the registration or incorporation information.

Fields	Instructions
Identifier type	Refer to Identification fields under "Standardized field instructions".
† If "Other", please specify	If "Other" identifier type is selected, you must specify the identifier type.
Number associated with identifier type	Same instructions (Identification fields)
Jurisdiction of issue (country)	Same instructions (Identification fields)
Jurisdiction of issue (province or state)	Same instructions (Identification fields)

Instructions for the fields under “Identification 1 of N on behalf of entity B”

Person authorized to bind the entity or act with respect to the account (maximum 3)

Fields	Instructions
Surname	Refer to Name fields under “Standardized field instructions”.
Given name	Same instructions (Name fields)
Other/Initial	Same instructions (Name fields)

Instructions for the fields under “Person 1 of N (max.3)”

Beneficial Ownership information (Entity structure / type) Corporate information: Directors of a corporation

Fields	Instructions
Surname	Refer to Identification fields under “Standardized field instructions”.
Given Name	Same instructions (Identification fields)
Other/Initial	Same instructions (Identification fields)
Apartment/Room/Suite/Unit number	Refer to Address fields under “Standardized field instructions”.
House/Building number	Same instructions (Address fields)
Street address	Same instructions (Address fields)
City	Same instructions (Address fields)
District	Same instructions (Address fields)
Country	Same instructions (Address fields)
Province or state	Same instructions (Address fields)
Sub-province and/or sub-locality	Same instructions (Address fields)
Postal or zip code	Same instructions (Address fields)
Unstructured address details	Refer to Unstructured address field under “Standardized field instructions”.
Telephone number	Refer to Telephone number fields under “Standardized field instructions”.
Extension	Same instructions (Telephone number fields)

Instructions for the fields under “Director 1 of N of starting action Y”

Person who directly or indirectly owns or controls 25% or more shares of the corporation

Fields	Instructions
Surname	Refer to Identification fields under "Standardized field instructions".
Given Name	Same instructions (Identification fields)
Other/Initial	Same instructions (Identification fields)

Instructions for the fields under "Person 1 of N of starting action Y"

Trust Information Trustee(s) of a trust

Fields	Instructions
Surname	Refer to Identification fields under "Standardized field instructions".
Given Name	Same instructions (Identification fields)
Other/Initial	Same instructions (Identification fields)
Apartment/Room/Suite/Unit number	Refer to Address fields under "Standardized field instructions".
House/Building number	Same instructions (Address fields)
Street address	Same instructions (Address fields)
City	Same instructions (Address fields)
District	Same instructions (Address fields)
Country	Same instructions (Address fields)
Province or state	Same instructions (Address fields)
Sub-province and/or sub-locality	Same instructions (Address fields)
Postal or zip code	Same instructions (Address fields)
Unstructured address details	Refer to Unstructured address field under "Standardized field instructions".
Telephone number	Refer to Telephone number fields under "Standardized field instructions".
Extension	Same instructions (Telephone number fields)

Instructions for the fields under "Trustee 1 of N of starting action Y"

Settlor(s) of a trust

Fields	Instructions
Surname	Refer to Identification fields under "Standardized field instructions".
Given Name	Same instructions (Identification fields)
Other/Initial	Same instructions (Identification fields)
Apartment/Room/Suite/Unit number	Refer to Address fields under "Standardized field instructions".
House/Building number	Same instructions (Address fields)
Street address	Same instructions (Address fields)
City	Same instructions (Address fields)
District	Same instructions (Address fields)
Country	Same instructions (Address fields)
Province or state	Same instructions (Address fields)
Sub-province and/or sub-locality	Same instructions (Address fields)
Postal or zip code	Same instructions (Address fields)
Unstructured address details	Refer to Unstructured address field under "Standardized field instructions".
Telephone number	Refer to Telephone number fields under "Standardized field instructions".
Extension	Same instructions (Telephone number fields)

Instructions for the fields under "Settlor 1 of N of starting action Y"

Widely held or publicly traded trust information Person who directly or indirectly owns or controls 25% or more units of a widely held or publicly traded trust.

Fields	Instructions
Surname	Refer to Identification fields under "Standardized field instructions".
Given Name	Same instructions (Identification fields)
Other/Initial	Same instructions (Identification fields)

Fields	Instructions
Apartment/Room/Suite/Unit number	Refer to Address fields under "Standardized field instructions".
House/Building number	Same instructions (Address fields)
Street address	Same instructions (Address fields)
City	Same instructions (Address fields)
District	Same instructions (Address fields)
Country	Same instructions (Address fields)
Province or state	Same instructions (Address fields)
Sub-province and/or sub-locality	Same instructions (Address fields)
Postal or zip code	Same instructions (Address fields)
Unstructured address details	Refer to Unstructured address field under "Standardized field instructions".
Telephone number	Refer to Telephone number fields under "Standardized field instructions".
Extension	Same instructions (Telephone number fields)

Instructions for the fields under "Person 1 of N of starting action Y"

Beneficiary(s) of a trust, other than a widely held or publicly traded trust

Fields	Instructions
Surname	Refer to Identification fields under "Standardized field instructions".
Given Name	Same instructions (Identification fields)
Other/Initial	Same instructions (Identification fields)
Apartment/Room/Suite/Unit number	Refer to Address fields under "Standardized field instructions".
House/Building number	Same instructions (Address fields)
Street address	Same instructions (Address fields)
City	Same instructions (Address fields)
District	Same instructions (Address fields)
Country	Same instructions (Address fields)
Province or state	Same instructions (Address fields)
Sub-province and/or sub-locality	Same instructions (Address fields)

Fields	Instructions
Postal or zip code	Same instructions (Address fields)
Unstructured address details	Refer to Unstructured address field under "Standardized field instructions".
Telephone number	Refer to Telephone number fields under "Standardized field instructions".
Extension	Same instructions (Telephone number fields)

Instructions for the fields under "Beneficiary 1 of N of starting action Y"

Entity other than a corporation or trust information Person who directly or indirectly owns or controls 25% or more of an entity other than a corporation or trust

Fields	Instructions
Surname	Refer to Identification fields under "Standardized field instructions".
Given Name	Same instructions (Identification fields)
Other/Initial	Same instructions (Identification fields)

Instructions for the fields under "Person 1 of N of starting action Y"

Fields	Instructions
Type of device used	Provide the type of device used.If "Other" type of device used is selected, you must specify the type of device used.
† If "Other". Please specify	If "Other" type of device used is selected, you must specify the type of device used.
Username	A username is how a person or an entity refers to themselves online.
Device identifier number	The device identifier number is a number assigned to the device, such as a Media Access Control (MAC) address or International Mobile Equipment Identity (IMEI) number.

Fields	Instructions
Internet protocol address	Provide the Internet Protocol (IP) address.It is the unique identifying number assigned to every device connected to the internet.
Date and time of online session in which request was made	This is the date and time the conductor accessed the online environment where the transaction was requested.

Instructions for the fields under "Information about conducting or attempting to conduct the transaction online"

Fields	Instructions
Relationship	Select the relationship of the "on behalf of" party to the person or entity conducting or attempting to conduct the transaction. The "on behalf of" party is understood to be the person or entity that instructs the person or entity conducting or attempting to conduct the transaction
† If "Other". Please specify	If "Other" is selected, specify the relationship of the "on behalf of" party to the person or entity conducting the transaction.

Instructions for the fields under "Relationship of the entity named above to the person or entity conducting or attempting to conduct the transaction"

Completing action Provide information about how the transaction was completed.

*** Details of disposition** This field describes what happened to the cash involved in the transaction.

Select the following disposition(s) based on the client's instructions.

Types of dispositions to select from	Instructions
Added to virtual currency wallet	Select when virtual currency is added to a virtual currency wallet.**This cannot be the first disposition**. For example, the cash received must be exchanged to virtual currency (first disposition) before it can be added to a virtual currency wallet (subsequent disposition).
Cash out	Select when cash is paid out by a non-account based reporting entity, such as a money services business.
Cash withdrawal (account based)	Select when cash is withdrawn from an account-based reporting entity, such as a bank or credit union.
Denomination exchange	Select when the cash received is exchanged from one unit value to another (for example, 20s to 100s) within the same currency.
Deposit to account	Select when cash is deposited into an account at an account-based reporting entity, such as a bank or credit union.
Exchange to fiat currency	Select for:- a fiat-to-fiat currency exchange (for example, Canadian dollars to US dollars), or- a virtual currency-to-fiat exchange (for example, bitcoin to Canadian dollars)**A virtual currency-to-fiat exchange cannot be the first disposition**. The cash received must be exchanged to virtual currency (first disposition) before the virtual currency can be exchanged to fiat (subsequent disposition).
Exchange to virtual currency	Select for:- a fiat-to-virtual currency exchange (for example, Canadian dollars to bitcoin), or- a virtual currency-to-virtual currency exchange (for example, bitcoin to ethereum (ETH))

Types of dispositions to select from	Instructions
Holding funds	Select when a non-account-based reporting entity (for example, a money services business) receives cash and holds these funds for a client for the purpose of a future transaction (for example, receipt of funds to buy virtual currency when it hits a certain threshold).
Investment product purchase or deposit	Select when a client buys or makes a deposit to a Guaranteed Investment Contract (GIC), RRSP, stock from an exchange (for example, Toronto Stock Exchange (TSX)), or any other such investments.
Issued cheque	Select for the issuance of:- a certified cheque or- a disbursement through a casino cheque, etc.
Life insurance policy purchase or deposit	Select when a client buys or puts a deposit down to purchase a life insurance policy.
Outgoing domestic funds transfer	Select when the transaction instructions are for the transfer of funds within Canada.
Outgoing email money transfer (EMT)	Select when the funds are transferred using a recipient's email address.
Outgoing international funds transfer	Select when the transaction instructions are for the transfer of funds outside of Canada.
Outgoing mobile money transfer	Select when the funds are transferred using a recipient's phone number.
Outgoing virtual currency transfer	Select when a reporting entity transfers virtual currency from a client's virtual currency wallet to another virtual currency wallet.**This cannot be the first disposition**. For example, the cash received must be exchanged to virtual currency (first disposition) before it can be added to a virtual currency wallet (second disposition) and then transferred to another virtual currency wallet.

Types of dispositions to select from	Instructions
Payment to account	Select when funds or virtual currency are used to pay down a loan, mortgage, line of credit or credit card account balance.
Purchase of bank draft	Select when a client purchases a bank draft from a financial entity.The term bank draft refers to a negotiable instrument that can be used as payment (similar to a cheque). Unlike a cheque, a bank draft is guaranteed by the issuing bank.
Purchase of casino product	Select when a client purchases a casino product.A casino product can include, but is not limited to:- chips- plaques, and- tokens
Purchase of jewellery	Select when a client purchases jewellery from a dealer in precious metals and precious stones.Jewellery means objects made of precious metals, precious stones or pearls that are intended for personal adornment.
Purchase of money order	Select when a client purchases a money order.A money order is a certificate, usually issued by a government or financial institution that allows the stated payee to receive cash on demand.A money order functions much like a cheque as the purchaser of the money order may stop the payment.
Purchase of precious metals	Select when a client purchases precious metals from a dealer in precious metals and precious stones.Precious metals means:- gold- silver- palladium, and- platinum in the form of:- coins- bars- ingots- granules, or- in other similar forms
Purchase of precious stones	Select when a client purchases precious stones from a dealer in precious metals and precious stones.Precious stones means:- diamonds- sapphires- emeralds- tanzanites- rubies, or- alexandrites

Types of dispositions to select from	Instructions
Purchase of prepaid payment product/card	Select when a client purchases a prepaid payment product.The product must be tied to a prepaid payment product account held by a financial entity.A prepaid payment product is a product that is issued by a financial entity that enables a person or entity to engage in a transaction by giving them electronic access to funds or to virtual currency paid into a prepaid payment product account held with the financial entity in advance of a transaction taking place.
Real estate purchase or deposit	Select when a client purchases or puts a deposit down on real estate.
Purchase of / Payment for goods	Select when a client purchases or pays for goods not already captured by any other disposition type included in the list above (for example, a car, yacht).
Purchase of / Payment of services	Select when a client purchases or pays for services not already captured by any other disposition type included in the list above (for example, cable, internet, hydro).

Types of dispositions to select from	Instructions
Other	Select when the disposition is not captured by any other disposition type included in the list above.Upon selecting "Other," you must provide a description of the disposition."Other" should not be used to combine multiple dispositions that are listed above. Specifically, if the completing action has multiple dispositions that are included in the list above, then each disposition should be selected and not combined under "Other".**Note: If the disposition is "Other", provide details that describe the disposition of the transaction in the field "† If"Other", please specify".**

Instructions for types of disposition to select for the field "* Details of disposition"

Number of dispositions in a completing action A completing action may have **1 or more dispositions**, depending on the client's instructions and your business process.

Example 1: A single disposition

Your client brings in $12,000 cash and instructs to deposit the entire amount into the client's savings account.

There is only 1 disposition:

- "deposit to account".

Example 2: Multiple dispositions

Your client brings in $12,000 cash and instructs to:

- deposit $5,000 into the client's savings account, and
- exchange $7,000 to bills in a larger denomination

There are 2 dispositions:

- "deposit to account", and
- "denomination exchange"

Example 3: A single disposition or multiple dispositions (depending on your business process)

Your client brings in $12,000 cash and instructs to transfer $12,000 to a friend outside Canada.

Financial entity

If your business process is to:

- deposit the cash into the client's account before the amount is sent to the client's friend, there are 2 dispositions:
  - "deposit to account", and
  - "outgoing international funds transfer"
- send the amount to the friend without depositing into an account, then there is 1 disposition:
  - "outgoing international funds transfer"

Money services business

If your business process is to:

- hold the funds until a later date on which you send the amount, there are 2 dispositions:
  - "holding funds", and
  - "outgoing international funds transfer"
- send the amount to the friend without holding the funds, then there is 1 disposition:
  - "outgoing international funds transfer"

Completing action fields

Fields	Instructions
† If 'Other', please specify	Select when the disposition is not captured by any other disposition type included in the list above.Upon selecting "Other," you must provide a description of the disposition."Other" should not be used to combine multiple dispositions that are listed above. Specifically, if the completing action has multiple dispositions that are included in the list above, then each disposition should be selected and not combined under "Other".**Note**: If the disposition is "Other", provide details that describe the disposition of the transaction in the field " **† If "Other", please specify**".
*** Amount**	Enter the amount involved in the completing action. For example, this may be the amount of:- virtual currency after an exchange to virtual currency- funds being initiated for an outgoing international funds transfer- funds indicated on the bank draft
† Currency	If the disposition involves a fiat currency, enter the currency even if it was in Canadian dollars.If the currency type is not in the list provided, you must select "Other" and provide the name of the currency.
† Virtual currency type	If the disposition involves virtual currency, select the virtual currency. If the currency type is not in the list provided, you must select "Other" and provide the name of the virtual currency.
† If "Other", please specify	If "Other" is selected, you must provide the name of the type of currency or virtual currency

Fields	Instructions
† Exchange rate	Provide the rate of exchange that you used for the transaction. This can be an exchange rate for fiat currency or virtual currency.
† Value in Canadian dollars	Provide the Canadian dollar value of the disposition if not in fiat or virtual currency. For example, provide the Canadian dollar value of the jewellery, precious metals or precious stones that were purchased. This may be the market, retail or other value that you would use in the ordinary course of your business at the time of transaction, and as detailed by and in accordance with your policies and procedures.
† Virtual currency transaction identifier	This is a unique identifier.It is commonly represented by a hash consisting of mixed numerical and alphabetical characters.
† Sending virtual currency address	The sending virtual currency address is made up of a number of alpha-numeric characters. The address length is determined by the type of virtual currency used in the transaction. The sending virtual currency address is associated with whoever is sending the virtual currency (typically the conductor).
† Receiving virtual currency address	The receiving virtual currency address is made up of a number of alpha-numeric characters.The address length is determined by the type of virtual currency used in the transaction.The receiving virtual currency address is associated with whoever is receiving the virtual currency (typically the beneficiary)

Fields	Instructions
† Reference number	If the transaction involved a reference number, provide it in this field.If the transaction involves an account at a financial entity, securities dealer or casino (account-based reporting entity), **do not provide the account number information in this field**—instead, provide that information in the account number field.For all other reporting entities, if you have an internal account number that is used as a reference number, then provide the internal account number in this field.
Other number related to reference number	Provide any other number related to the reference number as applicable.
† Financial institution number	Instructions not specified
† Branch number	Instructions not specified
† Account number	If the transaction involves an account at a **financial entity**, **securities dealer** or **casino**, provide the account number. If you are not an account-based reporting entity (for example, a money services business), but the transaction involves an account at an account-based reporting entity (for example, a financial entity), provide that account number in this field.
† Account type	Provide the account type.If the account type is not in the list provided, you must select "Other" and provide the account type.
† If "Other", please specify	If "Other" account type is selected, you must specify the account type.
† Account currency	Provide the account currency (fiat) type code.Currencies are represented both numerically and alphabetically, using either three digits or three letters.If the account currency type code can not be found, you must select "Other" and provide the currency (fiat) type.

Fields	Instructions
† Account virtual currency type	Provide the account virtual currency type.If the account virtual currency type is not in the list provided, you must select "Other" and provide the account virtual currency type.
† If "Other", please specify	If "Other", provide the full name of the currency or virtual currency type.
Date account opened	Provide the date the account was opened.
Date account closed	Provide the date the account was closed.
† Status of account at the time of transaction	Provide the status of the account at the time of the transaction (for example: active, inactive, dormant, closed).
‡ Was there any other person or entity involved in the completing action?	This field is a "Yes/No" question.See **Involved in the completing action,** below.

Instructions for the "Completing action fields"

Account holder – person

Fields	Instructions
† Surname	Refer to Name fields under "Standardized field instructions".
† Given name	Same instructions (Name fields)
Other/Initial	Same instructions (Name fields)

Instructions for the fields under "Person 1 of N completing action Z"

Account holder – entity

Field	Instructions
† Name of entity	Refer to Name fields under "Standardized field instructions".

Instructions for the field under "Entity 1 of N completing action Z"

Involved in the completing action Person involved in the completing action

If you have information about other persons involved in the completing action, you must include it.

Note: These persons **cannot be**:

- the conductor
- on behalf of party, or
- beneficiary of the transaction

Fields	Instructions
† Surname	Refer to Name fields under "Standardized field instructions".
† Given name	Same instructions (Name fields)
Other/initial	Same instructions (Name fields)
Account number	Provide the account number of the person involved in the completing action.If the transaction involves an account at a **financial entity**, **securities dealer** or **casino**, provide the account number. If you are not an account-based reporting entity (for example, a money services business), but the transaction involves an account at an account-based reporting entity (for example, a financial entity), provide that account number in this field.It is acceptable to include the financial institution number and branch number as part of an account number.
Policy number	Instructions not specified
Identifying number	Instructions not specified

Instructions for the fields under "Person 1 of N of completing action Z"

Entity involved in the completing action If you have information about other entities involved in the completing action, you must include it.

Note: These entities **cannot be**:

- the conductor
- on behalf of party, or
- beneficiary of the transaction

Fields	Instructions
† Name of entity	Refer to Name fields under "Standardized field instructions".
Account number	Provide the account number of the entity involved in the completing action.If the transaction involves an account at a **financial entity**, **securities dealer** or **casino**, provide the account number. If you are not an account-based reporting entity (for example, a money services business), but the transaction involves an account at an account-based reporting entity (for example, a financial entity), provide that account number in this field.It is acceptable to include the financial institution number and branch number as part of an account number.
Policy number	Instructions not specified
Identifying number	Instructions not specified

Instructions for the fields under "Entity 1 of N of completing action Z"

Beneficiary

Fields	Instructions
‡ Have you obtained any beneficiary information related to this transaction or attempted transaction? (Only select No if the beneficiary is **not** your client **and**, after taking reasonable measures, you were not able to obtain any beneficiary details.)	This field is a "Yes/No" question.Only select No if the beneficiary is **not** your client **and**, after taking reasonable measures, you were not able to obtain any beneficiary details.

Instructions for the fields under "Beneficiary Indicator"

Provide beneficiary information for each completing action.

A beneficiary, for example, can be:

- the person who receives the virtual currency

- the person named on a money order, or
- the person who receives the jewellery

The beneficiary **can be** the **same person or entity** that conducts the transaction or someone else.

The beneficiary **cannot be** the reporting entity.

Person beneficiary

Fields	Instructions
† Surname	Refer to Name fields under "Standardized field instructions".
† Given name	Same instructions (Name fields)
Other/Initial	Same instructions (Name fields)
Alias	Same instructions (Name fields)
Username	A username is how a person or an entity refers to themselves online.
Client number	Instructions not specified
Apartment/Room/Suite/Unit number	Refer to Address fields under "Standardized field instructions".
House/Building number	Same instructions (Address fields)
Street address	Same instructions (Address fields)
City	Same instructions (Address fields)
District	Same instructions (Address fields)
Country	Same instructions (Address fields)
Province or state	Same instructions (Address fields)
Sub-province and/or sub-locality	Same instructions (Address fields)
Postal or zip code	Same instructions (Address fields)
Unstructured address details	Refer to Unstructured address field under "Standardized field instructions".
Telephone number	Refer to Telephone number fields under "Standardized field instructions".
Extension	Same instructions (Telephone number fields)
Email address	Instructions not specified
Date of birth	Instructions not specified
Country of residence	Enter the primary country of residence for the person.It can be the same or different from the country entered in the address section.

Fields	Instructions
Occupation	Refer to Occupation/business fields under "Standardized field instructions".
Name of employer	Same instructions (Occupation/business fields)

Instructions for the fields under "Person 1 of C completing action Z"

Identification of the person beneficiary

Fields	Instructions
Identifier type	Refer to Identification fields under "Standardized field instructions".
† If "Other", please specify	If "Other" identifier type is selected, you must specify the identifier type.
Number associated with identifier type	Same instructions (Identification fields)
Jurisdiction of issue (country)	Same instructions (Identification fields)
Jurisdiction of issue (province or state)	Same instructions (Identification fields)

Instructions for the fields under "Identification 1 of N of the person beneficiary C"

Identification of the entity beneficiary

Fields	Instructions
† Name of entity	Refer to Identification fields under "Standardized field instructions".
Username	A username is how a person or an entity refers to themselves online.
Client number	Instructions not specified
Apartment/Room/Suite/Unit number	Refer to Address fields under "Standardized field instructions".
House/Building number	Same instructions (Address fields)
Street address	Same instructions (Address fields)
City	Same instructions (Address fields)
District	Same instructions (Address fields)
Country	Same instructions (Address fields)

Fields	Instructions
Province or state	Same instructions (Address fields)
Sub-province and/or sub-locality	Same instructions (Address fields)
Postal or zip code	Same instructions (Address fields)
Unstructured address details	Refer to Unstructured address field under "Standardized field instructions".
Telephone number	Refer to Telephone number fields under "Standardized field instructions".
Extension	Same instructions (Telephone number fields)
Email address	Instructions not specified
Nature of entity's principal business	Refer to Occupation/business fields under "Standardized field instructions".
Is the entity incorporated or registered?	This field is a "Yes/No" question.

Instructions for the fields under "Entity 1 of C of completing action Z"

Incorporation of the entity

Fields	Instructions
Incorporation number	Provide the incorporation number of the entity conducting the transaction for each jurisdiction where the entity is incorporated.
Jurisdiction of issue (country) of incorporation	Provide the jurisdiction of issue (country) of incorporation for each jurisdiction where the entity is incorporated

Fields	Instructions
Jurisdiction of issue (province or state) of incorporation	Provide the jurisdiction of issue (province or state) of incorporation for each jurisdiction where the entity is incorporatedIf the jurisdiction is a province or state **in** Canada, the United States or Mexico, **select the code from the list of options.**If the jurisdiction is **outside** Canada, the United States or Mexico, **provide the name of the province or state.**

Instructions for the fields under "Incorporation 1 of N of entity beneficiary A"

Registration of the entity

Fields	Instructions
Registration number	Provide the registration number of the entity conducting the transaction for each jurisdiction where the entity is registeredFor Canadian entities, a registration number can include the 9-digit business number assigned to that entity by the Canada Revenue Agency (CRA).
Jurisdiction of issue (country) of registration	Provide the country that issued the documentation used to identify the entity for each jurisdiction where the entity is registered.
Jurisdiction of issue (province or state) of registration	Provide the jurisdiction of issue (province or state) for each jurisdiction where the entity is registeredIf the jurisdiction is a province or state **in** Canada, the United States or Mexico, **select the code from the list of options.**If the jurisdiction is **outside** Canada, the United States or Mexico, **provide the name of the province or state.**

Instructions for the fields under "Registration 1 of N of entity beneficiary A"

Identification of the entity Provide the following information that was used to verify the identity of the entity that is a beneficiary.

For some entities, this information may be the same as the registration or incorporation information.

Fields	Instructions
Identifier type	Refer to Identification fields under "Standardized field instructions".
† If "Other", please specify	If "Other" is selected, you must specify the identifier type.
Number associated with identifier type	Same instructions (Identification fields)
Jurisdiction of issue (country)	Same instructions (Identification fields)
Jurisdiction of issue (province or state)	Same instructions (Identification fields)

Instructions for the fields under "Identification 1 of N of entity beneficiary C"

Fields	Instructions
Surname	Refer to Name fields under "Standardized field instructions".
Given name	Same instructions (Name fields)
Other/Initial	Same instructions (Name fields)

Instructions for the fields under "Person authorized to bind the entity beneficiary or act with respect to the account (maximum 3)"

Details of suspicion **Note:** The "Details of suspicion" section of the Suspicious Transaction Report form **must not be completed** if the transaction is being reported to FINTRAC under a Ministerial Directive.

***Description of suspicious activity** This section is the narrative that explains your grounds for suspicion that led to your decision to submit a Suspicious Transaction Report to FINTRAC.

You must describe in clear, simple and concise language your grounds for suspicion of a money laundering or terrorist financing offence – including the facts, context, and indicators that allowed you to reach reasonable grounds for suspicion.

The narrative should:

- **not assume** that the reader will be familiar with acronyms or terminology specific to your business.

- focus on the question: "Why do you think the transaction is suspicious of money laundering or terrorist financing?"
- **not refer** to any internal files or documents since FINTRAC cannot have access to these internal files or documents for its analysis.
- not include graphics, underlined, italicized or bolded text since they cannot be viewed in the Suspicious Transaction Report form
- be consistent with the information in the structured fields of the Suspicious Transaction Report form
  - For example, if you are referring to specific account activity in this section, the details of those accounts and transactions should be entered in the structured fields.

Detailed and high quality Suspicious Transaction Reports provide valuable and actionable intelligence for FINTRAC and this section is shared with law enforcement and intelligence agencies in FINTRAC disclosures.

Instructions for the fields under "details of suspicion"

Fields	Instructions
Suspicion type	Select:- money laundering- terrorist financing- money laundering and terrorist financing- sanctions evasion- money laundering and sanctions evasion- terrorist financing and sanctions evasion- money laundering, terrorist financing and sanctions evasionIf your primary suspicion type is sanctions evasion, and you do not have the system capability at this time to select the new sanctions evasion option, you must select "money laundering" as suspicion type from the drop down list and add #SANCTIONS as part of the grounds for suspicion in the Description of suspicious activity section.
Public-Private partnership name	Select the public-private partnership project name that the Suspicious Transaction Report is associated with, if applicable.

Fields	Instructions
Does this report include information about an individual you have determined to be a politically exposed person (PEP)?	This field is a "Yes/No" question.

Related Reports Are there previously submitted reports that may relate to the suspicious activity mentioned in this report?

Fields	Instructions
Reporting entity report reference number (1 of N)	Provide the reporting entity report reference number(s) of the previously submitted report(s) that may relate to the suspicious activity mentioned in this Suspicious Transaction Report.
Reporting entity transaction reference number (1 of Z of report N)	Provide the reporting entity transaction reference number(s) of the previously submitted report(s) that may relate to the suspicious activity mentioned in this Suspicious Transaction Report.

Instructions for the fields under "Report 1 of X"

Action taken **Note:** The "Action taken" section of the Suspicious Transaction Report form **must not be completed** if the transaction is being reported to FINTRAC under a Ministerial Directive.

*** Description of action taken** Describe the action(s) that you have taken or will be taking as a result of the suspicious transaction(s).

The following are examples of actions taken:

- reporting the information directly to law enforcement;
- initiating enhanced transaction monitoring;
- closing the account(s) in question or exiting the business relationship; and/or
- cancelling, reversing or rejecting the transaction.

Reporting a Suspicious Transaction Report to FINTRAC **does not** prevent you from contacting law enforcement directly.

However, even if you do contact law enforcement directly about your suspicions of money laundering or terrorist financing, you must still submit a Suspicious Transaction Report to FINTRAC.

Some **Suspicious Transaction Reports** have included the law enforcement agency's contact information in this part of the **Suspicious Transaction Report** when the suspicion was also reported directly to law enforcement and this information can be helpful.

Annex B - Scenarios

The following scenarios demonstrate form completion and the expected field information in a Suspicious Transaction Report based on the client's instructions and transaction(s) in each scenario.

Notes about these scenarios

- Specific money laundering and terrorist financing indicators and a full narrative of the reasonable grounds to suspect has not been provided.
  - For information on reasonable grounds to suspect and indicators for your sector, refer to 4. When to submit a Suspicious Transaction Report above, and the money laundering and terrorist financing indicators under All FINTRAC guidance – Transaction reporting.
  - Not all fields of the Suspicious Transaction Report form are displayed—only fields with completed information are displayed.
- Not all fields of the Suspicious Transaction Report form are displayed.
- Only fields with completed information are displayed.
- Some fields have been combined for the purpose of brevity. For example, conductor name, address, telephone number and other conductor fields have been combined as conductor information.
- Because some fields are mandatory and some are not, it has been assumed that the reporting entity had the information if a field has been completed.

In this annex

Scenario B.1: Person deposits cheque and sends an email money transfer (EMT)

- On July 6, 2022, Gordie Gold deposited a $1,500 cheque from Iron Construction Ltd. into a joint account (with Gemma Gold) at Moon Rays Financial by using his access card at an automated teller machine (ATM).
  - The cheque, which was payable to Gordie Gold, included the following memo line: Pay cheque—Job # 5.
- On the same evening, Gordie logged into online banking using his access card and sent an email money transfer (EMT) in the amount of $2,500 from his joint account with Gemma to Sunny Silver's account at Solar Bank.
  - Sunny is not a client of Moon Rays Financial.
  - The EMT message indicates the following: July 2022 rent.
- Moon Rays Financial is submitting the following Suspicious Transaction Report as it identified multiple indicators and determined that there are reasonable grounds to suspect the transactions are related to the commission of a money laundering offence.

Expected field information in the report

General information – Scenario B.1

Fields	Information provided by Moon Rays Financial
Reporting entity number	The reporting entity number assigned to Moon Rays Financial when it enrolled with FINTRAC Web Reporting System (FWR)
Reporting entity report reference number	The unique number for this report that was assigned by:- Moon Rays Financial, or- its service provider
Activity sector	Bank
Contact information for this report	Information about the person at Moon Rays Financial that FINTRAC can liaise with in the event that a follow up is required

General information about Moon Rays Financial

Transaction information – Scenario B.1

Fields	Information provided for transaction 1 of 2	Information provided for transaction 2 of 2
Transaction Status	Completed	Completed
Date of transaction	The date the cheque was deposited at Moon Rays Financial (July, 6, 2022)	The date the online transaction was conducted (July 6, 2022)
Time of transaction	The time the cheque was deposited at Moon Rays Financial	The time the online transaction was conducted on July 6, 2022
Method of transaction	Automated teller machine (ATM)	Online
Reporting entity transaction reference number	The unique number for this transaction that was assigned by:- Moon Rays Financial Bank, or- its service provider	The unique number for this transaction that was assigned by:- Moon Rays Financial, or- its service provider
Reporting entity location number	Information about where the transaction took place (ATM location)	Information about where the transaction took place -specifically, the location number that is associated with the location that receives and initiates the client's online instructions

"Transaction information" provided by Moon Rays Financial

Starting action – Scenario B.1

Fields	Information provided for starting action 1 of transaction 1	Information provided for starting action 1 of transaction 2
Direction of starting action	In	Out
Type of funds, assets or virtual currency (in/out)	Cheque	Funds withdrawal
Amount	1,500	2,500
Currency	CAD	CAD

Fields	Information provided for starting action 1 of transaction 1	Information provided for starting action 1 of transaction 2
Financial Institution and branch number	The financial institution and branch number which issued the cheque	The financial institution and branch number for Moon Rays Financial
Account number	The account number indicated on the cheque	The account number for the joint account of Gordie and Gemma Gold at Moon Rays Financial
Was information about the source (person/entity) of funds or virtual currency obtained?	No	No
Account holder	Iron Construction Ltd. (as indicated on the cheque)	Gordie and Gemma Gold
Conductor information	Information that Moon Rays Financial has on Gordie Gold which may include: - name- alias- client number- address- telephone number- email address- URL- date of birth- country of residence- country of citizenship- occupation- name and address of employer, and- identification details	Information that Moon Rays Financial has on Gordie Gold which may include:- name- alias- client number- address- telephone number- email address- URL- date of birth- country of residence- country of citizenship- occupation- name and address of employer, and- identification details
Information about conducting or attempting to conduct the transaction online	[Field left blank because not applicable]	Information including:- type of device used- username- device identifier number- internet protocol address- date and time of online session in which request was made

Fields	Information provided for starting action 1 of transaction 1	Information provided for starting action 1 of transaction 2
Was this transaction conducted or attempted on behalf of another person or entity?	No	No

"Starting action" information provided by Moon Rays Financial

Completing action – Scenario B.1

Fields	Information provided for completing action 1 of transaction 1	Information provided for completing action 1 of transaction 2
Details of disposition	Deposit to account	Outgoing email money transfer (EMT)
Amount	1,500	2,500
Currency	CAD	CAD
Financial institution number and branch number (if available for EMT)	The financial institution and branch number for Moon Rays Financial	The financial institution and branch number for Solar Bank
Account number (if available for EMT)	The account number for the joint account of Gordie and Gemma Gold at Moon Rays Financial	The account number of Sunny Silver at Solar Bank
Account holder (if available for EMT)	Gordie and Gemma Gold	Sunny Silver
Was there any other person or entity involved in the completing action?	No	No

Fields	Information provided for completing action 1 of transaction 1	Information provided for completing action 1 of transaction 2
Beneficiary information	Information that Moon Rays Financial has on Gordie and Gemma Gold as they are the account holders on the joint account in which the cheque was deposited. This may include; - name- alias- username- client number- address- telephone number- email address- date of birth- country of residence- occupation- name of employer, and- identification details	Sunny Silver's nameAlso, if obtained, information about Sunny Silver including:- name- alias- client number- address- telephone number- email address- date of birth- country of residence- occupation- name of employer, and- identification details

"Completing action" information provided by Moon Rays Financial

Details of suspicion – Scenario B.1

Details of Suspicion
The description of the facts, context and indicators that allowed Moon Rays Financial to establish that there are reasonable grounds to suspect that the transaction(s) are related to the commission of a money laundering offence.In this scenario, this could include the information from the cheque memo line (Pay cheque—Job # 5) and the EMT message (July 2022 rent).

"Details of Suspicion" information provided by Moon Rays Financial

Details of action taken – Scenario B.1

Action Taken
The action that Moon Rays Financial has taken as a result of the suspicious transaction(s).

"Details of Action Taken" information provided by Moon Rays Financial

Note:

- If the conductor (Gordie Gold) has multiple email addresses, provide the email address that the conductor used to send the EMT in the email address field for the conductor.
- Gordie's other email addresses can be provided in the narrative section of the report (Details of suspicion).
- The beneficiary email address field should be the email address that was used by the beneficiary to receive the email money transfer (EMT).

Scenario B.2: Entity exchanges cash to virtual currency and transfers to wallet

- On July 7, 2022, Gordie Gold walked into Cosmic Virtual Currency Money Service Business (Cosmic VC MSB) with $9,997 CAD cash.
  - Gordie advised Cosmic VC MSB that he is representing Gordie's Painting Inc. A company in which he is the CEO and sole director and shareholder.
  - Gordie also advised Cosmic VC MSB that the cash was payment from a recently sold painting to a client, Sunny Silver.
  - Gordie requested that the cash be exchanged to Ethereum (ETH) so that it could be added to Cosmic VC MSB's custodial virtual currency wallet. The virtual currency exchange rate was 0.0007.
  - Gordie then requested the ETH be transferred to his personal external virtual currency wallet.
- Cosmic VC MSB is submitting this Suspicious Transaction Report as it identified multiple indicators and determined that there are reasonable grounds to suspect the transaction is related to the commission of a money laundering offence.

Expected field information in the report

General information – Scenario B.2

Fields	Information provided by Cosmic VC MSB
Reporting entity number	The reporting entity number assigned to Cosmic VC MSB when it enrolled with FINTRAC Web Reporting System (FWR)
Reporting entity report reference number	The unique number for this report that was assigned by:- Cosmic VC MSB, or- its service provider
Activity sector	Money services business

Fields	Information provided by Cosmic VC MSB
Contact information for this report	Information about the person at Cosmic VC MSB that FINTRAC can liaise with in the event that a follow up is required

General information about Cosmic VC MSB

Transaction information – Scenario B.2

Fields	Information provided for transaction 1 of 1
Transaction Status	Completed
Date of transaction	The date the cash was received by Cosmic VC MSB (July, 7, 2022)
Time of transaction	The time the cash was received by Cosmic VC MSB on July 7, 2022
Method of transaction	In person
Reporting entity transaction reference number	The unique number for this transaction that was assigned by:- Cosmic VC MSB, or- its service provider
Reporting entity location number	Information about where the transaction took place

"Transaction information" provided by Cosmic VC MSB

Starting action – Scenario B.2

Fields	Information provided for starting action 1 of transaction 1
Direction of starting action	In
Type of funds, assets or virtual currency (in/out)	Cash
Amount	9,997
Currency	CAD
How were the funds or virtual currency obtained?	Gordie Gold advised that he received the cash when he sold a painting to his client, Sunny Silver

Fields	Information provided for starting action 1 of transaction 1
Was information about the source (person/entity) of funds or virtual currency obtained?	Yes
Source of funds or virtual currency	Sunny Silver
Conductor information	Information that Cosmic VC MSB has on Gordie's Painting Inc. which may include: - name- alias- client number- address- telephone number- email address- URL, and- identification details
Additional information about the conductor if it is an entity	- Person(s) authorized to bind the entity (Gordie Gold),- Type of entity (corporation) - Nature of entity's principal business (painting/contracting) - Incorporation and/or registration information - Director(s) of the corporation (Gordie Gold)- Person(s) who directly or indirectly owns or controls 25% or more shares of the corporation (Gordie Gold)
Was this transaction conducted or attempted on behalf of another person or entity?	No

"Starting action" information provided by Cosmic VC MSB

Completing action – Scenario B.2

Fields	Information provided for completing action 1 of transaction 1	Information provided for completing action 2 of transaction 1	Information provided for completing action 3 of transaction 1
Details of disposition	Exchange to virtual currency	Added to virtual currency wallet	Outgoing virtual currency transfer
Amount	7	7	7
Virtual Currency type	ETH	ETH	ETH

Fields	Information provided for completing action 1 of transaction 1	Information provided for completing action 2 of transaction 1	Information provided for completing action 3 of transaction 1
Exchange rate	.0007	[Field left blank because not applicable]	[Field left blank because not applicable]
Virtual Currency transaction identifier	[Field left blank because not applicable]	The unique identifier for this transaction (completing action 2) that is commonly represented by a hash consisting of mixed numerical and alphabetical characters	The unique identifier for this transaction (completing action 3) that is commonly represented by a hash consisting of mixed numerical and alphabetical characters
Receiving Virtual currency address	[Field left blank because not applicable]	The virtual currency address for Cosmic VC MSB as it received the virtual currency	The virtual currency address for Gordie Gold as he received the virtual currency in his personal wallet
Was there any other person or entity involved in the completing action?	No	No	No

Fields	Information provided for completing action 1 of transaction 1	Information provided for completing action 2 of transaction 1	Information provided for completing action 3 of transaction 1
Beneficiary information	Information that Cosmic VC MSB has on Gordie's Painting Inc. which may include:- name- username- client number- address- telephone number- email address- nature of entity's principal business (painting/ contracting) - incorporation and/or registration information- identification details, and- person(s) authorized to bind the entity (Gordie Gold)	Information that Cosmic VC MSB has on Gordie's Painting which may include: - name- username - client number - address - telephone number - email address - nature of entity's principal business (painting/ contracting) - incorporation and/or registration information- identification details, and- person(s) authorized to bind the entity (Gordie Gold)	Information that Cosmic VC MSB has on Gordie Gold which may include: - name - alias - username- client number - address - telephone number - email address - date of birth - country of residence - occupation,- name of employer, and - identification details

"Completing action" information provided by Cosmic VC MSB

Details of suspicion – Scenario B.2

Details of Suspicion
The description of the facts, context and indicators that allowed Cosmic VC MSB to establish that there are reasonable grounds to suspect that the transaction(s) is/are related to the commission of a money laundering offence.

"Details of Suspicion" information provided by Cosmic VC MSB

Details of action taken – Scenario B.2

Action Taken
The action that Cosmic VC MSB has taken because of the suspicious transaction(s).

"Details of Action Taken" information provided by Cosmic VC MSB

Scenario B.3: Person deposits on behalf of another person who later purchases casino chips and then redeems these chips

- On July 8th, 2022, Gordie Gold came into Vega Casino to deposit $9,000 cash on behalf of Sunny Silver.
  - The cash was deposited into Sunny's account and Gordie advised the casino that he and Sunny were friends.
  - The casino was not able to obtain information about the purpose of the transaction or the source of funds.
- On July 9th, 2022, Sunny purchased casino chips at Vega Casino using funds in her casino account totaling $9,000.
  - After leaving the front desk, Sunny was seen passing the chips to Chuck who is an individual known to the casino.
  - Within an hour, Sunny returned to the front desk to redeem the remaining casino chips and requested a cheque payable to herself totaling $5,000.
- Vega Casino is submitting this Suspicious Transaction Report as it identified multiple indicators and determined that there are reasonable grounds to suspect the transactions are related to the commission of a money laundering offence.

Expected field information in the report

General information – Scenario B.3

Fields	Information provided by Vega Casino
Reporting entity number	The reporting entity number assigned to Vega Casino when it enrolled with FINTRAC Web Reporting System (FWR)
Reporting entity report reference number	The unique number for this report that was assigned by:- Vega Casino, or- its service provider
Activity sector	Casino

Fields	Information provided by Vega Casino
Contact information for this report	Information about the person at Vega Casino that FINTRAC can liaise with in the event that a follow up is required

General information about Vega Casino

Transaction information – Scenario B.3

Fields	Information provided for transaction 1 of 3	Information provided for transaction 2 of 3	Information provided for transaction 3 of 3
Transaction Status	Completed	Completed	Completed
Date of transaction	The date Vega Casino received the cash from Gordie Gold (July 8, 2022)	The date casino chips were purchased (July 9, 2022)	The date casino chips were redeemed (July 9, 2022)
Time of transaction	The time Vega Casino received the cash on July 8, 2022	The time the casino chips were purchased on July 9, 2022	The time the casino chips were redeemed on July 9, 2022
Method of transaction	In person	In person	In person
Reporting entity transaction reference number	The unique number for this transaction that was assigned by:- Vega Casino, or- its service provider	The unique number for this transaction that was assigned by:- Vega Casino, or- its service provider	The unique number for this transaction that was assigned by:- Vega Casino, or- its service provider
Reporting entity location number	Information about where the transaction took place	Information about where the transaction took place	Information about where the transaction took place

Starting action – Scenario B.3

Fields	Information provided for starting action 1 of transaction 1	Information provided for starting action 1 of transaction 2	Information provided for starting action 1 of transaction 3
Direction of starting action	In	Out	In
Type of funds, assets or virtual currency (in/out)	Cash	Funds withdrawal	Casino product
Amount	9,000	9,000	5,000
Currency	CAD	CAD	CAD
Account number	[Field left blank because not applicable]	Sunny Silver's account number at Vega Casino	[Field left blank because not applicable]
Was information about the source (person /entity) of funds or virtual currency obtained?	No	No	No
Account holder	[Field left blank because not applicable]	Sunny Silver	[Field left blank because not applicable]

Fields	Information provided for starting action 1 of transaction 1	Information provided for starting action 1 of transaction 2	Information provided for starting action 1 of transaction 3
Conductor information	Information that Vega Casino has on Gordie Gold which may include: - name- alias- client number- address- telephone number- email address- URL- date of birth- country of residence- country of citizenship- occupation- name and address of employer, and- identification details	Information that Vega Casino has on Sunny Silver which may include:- name- alias- client number- address- telephone number- email address- URL- date of birth- country of residence- country of citizenship- occupation- name and address of employer, and- identification details	Information that Vega Casino has on Sunny Silver which may include:- name- alias- client number- address- telephone number- email address- URL- date of birth- country of residence- country of citizenship- occupation- name and address of employer, and- identification details
Was this transaction conducted or attempted on behalf of another person or entity?	Yes	No	No
Relationship of the person named above to the person or entity conducting or attempting to conduct the transaction	Friend	[Field left blank because not applicable]	[Field left blank because not applicable]

Scenario B.4: Person transfers funds between accounts and pays utility bill and credit card

- On July 9th, 2022, Gordie Gold logged into online banking at Moon Rays Financial using his access card and does the following:
  - transfers $1,500 from his joint account with Gemma Gold to his own personal account—and both accounts are held at Moon Rays Financial
  - pays an electric bill to ABC Electric Company (billing account reference number 12345-678) for $500 using funds from his own personal account, and
  - pays a credit card account balance of $1,000 to ABC Credit Card Company (credit card number 1234-5678-1234-5678) using funds from his personal account.
- Moon Rays Financial is submitting this Suspicious Transaction Report as it identified multiple indicators and determined that there are reasonable grounds to suspect the transactions are related to the commission of a money laundering offence.

Expected field information in the report

General information – Scenario B.4

Fields	Information provided by Moon Rays Financial
Reporting entity number	The reporting entity number assigned to Moon Rays Financial when it enrolled with FINTRAC Web Reporting System (FWR)
Reporting entity report reference number	The unique number for this report that was assigned by:- Moon Rays Financial, or- its service provider
Activity sector	Bank
Contact information for this report	Information about the person at Moon Rays Financial that FINTRAC can liaise with in the event that a follow up is required

General information about Moon Rays Financial

Transaction information – Scenario B.4

Fields	Information provided for transaction 1 of 3	Information provided for transaction 2 of 3	Information provided for transaction 3 of 3
Transaction Status	Completed	Completed	Completed
Date of transaction	The date the online transaction was conducted (July 9, 2022)	The date the online transaction was conducted (July 9, 2022)	The date the online transaction was conducted (July 9, 2022)
Time of transaction	The time the online transaction was conducted on July 9, 2022	The time the online transaction was conducted on July 9, 2022	The time the online transaction was conducted on July 9, 2022
Method of transaction	Online	Online	Online
Reporting entity transaction reference number	The unique number for this transaction that was assigned by:- Moon Rays Financial, or- its service provider	The unique number for this transaction that was assigned by:- Moon Rays Financial, or- its service provider	The unique number for this transaction that was assigned by:- Moon Rays Financial, or- its service provider
Reporting entity location number	Information about where the transaction took place – specifically the location number that is associated with the location that receives and initiates the client's online instructions	Information about where the transaction took place – specifically the location number that is associated with the location that receives and initiates the client's online instructions	Information about where the transaction took place – specifically the location number that is associated with the location that receives and initiates the client's online instructions

Starting action – Scenario B.4

Fields	Information provided for starting action 1 of transaction 1	Information provided for starting action 1 of transaction 2	Information provided for starting action 1 of transaction 3
Direction of starting action	Out	Out	Out
Type of funds, assets or virtual currency (in/out)	Funds withdrawal	Funds withdrawal	Funds withdrawal
Amount	1,500	500	1,000
Currency	CAD	CAD	CAD
Financial institution and branch number	The financial institution and branch number for Moon Rays Financial	The financial institution and branch number for Moon Rays Financial	The financial institution and branch number for Moon Rays Financial
Account number	The account number for the joint account of Gordie and Gemma Gold at Moon Rays Financial	The account number for Gordie Gold's personal account at Moon Rays Financial	The account number for Gordie Gold's personal account at Moon Rays Financial
Was information about the source (person /entity) of funds or virtual currency obtained?	No	No	No
Account holder	Gordie and Gemma Gold	Gordie Gold	Gordie Gold

Fields	Information provided for starting action 1 of transaction 1	Information provided for starting action 1 of transaction 2	Information provided for starting action 1 of transaction 3
Conductor information	Information that Moon Rays Financial has on Gordie Gold which may include: - name- alias- client number- address- telephone number- email address- URL- date of birth- country of residence- country of citizenship- occupation- name and address of employer, and- identification details	Information that Moon Rays Financial has on Gordie Gold which may include:- name- alias- client number- address- telephone number- email address- URL- date of birth- country of residence- country of citizenship- occupation- name and address of employer, and- identification details	Information that Moon Rays Financial has on Gordie Gold which may include:- name- alias- client number- address- telephone number- email address- URL- date of birth- country of residence- country of citizenship- occupation- name and address of employer, and- identification details
Information about conducting or attempting to conduct the transaction online	Information including:- type of device used- username- device identifier number- internet protocol address- date and time of online session	Information including:- type of device used- username- device identifier number- internet protocol address- date and time of online session	Information including:- type of device used- username- device identifier number- internet protocol address- date and time of online session in which the request was made
Was this transaction conducted or attempted on behalf of another person or entity?	No	No	No

Completing action – Scenario B.4

Fields	Information provided for completing action 1 of transaction 1	Information provided for completing action 1 of transaction 2	Information provided for completing action 1 of transaction 2
Details of disposition	Outgoing domestic funds transfer	Purchase of /Payment of services	Payment to account
Amount	1,500	500	1,000
Currency	CAD	CAD	CAD
Reference number	[Field left blank because not applicable]	12345-678 (the reference number associated with the bill payment)	[Field left blank because not applicable]
Financial institution and branch number	The financial institution and branch number which sent the outgoing domestic funds transfer	[Field left blank because not applicable]	[Field left blank because not applicable]
Account number	The account number for the personal account of Gordie Gold at Moon Rays Financial	[Field left blank because not applicable]	1234-5678-1234-5678 (the credit card account in which payment was made)
Account holder	Gordie Gold	[Field left blank because not applicable]	[Field left blank because not applicable]
Was there any other person or entity involved in the completing action?	No	No	No

Fields	Information provided for completing action 1 of transaction 1	Information provided for completing action 1 of transaction 2	Information provided for completing action 1 of transaction 2
Beneficiary information	Information that Moon Rays Financial has on Gordie Gold. This may include; - name- alias- username- client number- address- telephone number- email address- date of birth- country of residence- occupation- name of employer, and- identification details	Information that Moon Rays Financial has on ABC Electric Company. This may include:- name- username - client number - address - telephone number - email address - nature of entity's principal business (utility) - incorporation and/or registration information- identification details, and- person(s) authorized to bind the entity	Information that Moon Rays Financial has on ABC Credit Card Company. This may include:- name- username - client number - address - telephone number - email address - nature of entity's principal business (credit card company) - incorporation and/or registration information- identification details, and- person(s) authorized to bind the entity

"Completing action" information provided by Moon Rays Financial

Details of suspicion – Scenario B.4

Details of Suspicion
The description of the facts, context and indicators that allowed Moon Rays Financial to establish that there are reasonable grounds to suspect that the transaction(s) are related to the commission of a money laundering offence.

"Details of Suspicion" information provided by Moon Rays Financial

Details of action taken – Scenario B.4

Action Taken
The action that Moon Rays Financial has taken as a result of the suspicious transaction(s).

"Details of Action Taken" information provided by Moon Rays Financial

Guide on harm done assessment for record keeping violations

1. Introduction

This page presents how we assess the harm done and calculate the base penalty amount applied to record keeping violations.

1.1 Purpose of the guide

This guide presents how FINTRAC approaches the harm done criterion and the base penalty amount for violations under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (the Act) and its regulations. According to section 73.11 of the Act, FINTRAC must consider the harm done by a violation, that the purpose of an administrative monetary penalty (AMP) is to encourage compliance rather than to punish, and all other criteria prescribed in the regulations, including a reporting entity's (RE) history of compliance, when determining the amount of a penalty. Considerations for the non-punitive nature of an AMP and an REs' compliance history are assessed in another step in the penalty calculation and are outlined separately in FINTRAC's AMP policy.

1.2 Definition of harm

FINTRAC defines "harm" as the degree to which a violation interferes with achieving the objectives of the ActFootnote 1 or with FINTRAC's ability to carry out its mandateFootnote 2. Therefore, the consequences of non-compliance, when an AMP is imposed, are linked to its effects on Canada's efforts to combat money laundering and terrorist activity financing (ML/TF).

Compliance enforcement activities are undertaken to prevent and correct the harm that comes from non-compliance with the Act and regulations. REs' adherence to requirements such as record keeping and verifying client identity assists in the deterrence of ML/TF and supports investigations and criminal prosecutions. The requirements related to reporting ensure that FINTRAC is supplied with the high-quality, timely financial transaction reports it needs to produce the financial intelligence that helps with the investigation and prosecution of ML/TF offences.

1.3 Considering harm in AMP Calculations

When determining a penalty, FINTRAC considers the harm caused, that is, the degree to which the non-compliance interferes with the purpose of the Act and/or with FINTRAC's mandate. Non-compliance and harm are measured using the standards described in this guide, which outline the benchmark amounts for the corresponding levels of harm for a specific violation. FINTRAC considers the specific circumstances of each case, including the extent of the non-compliance and mitigating factors, which may further reduce the actual amounts applied.

2. Violations related to keeping prescribed records

Record keeping violations directly affect the objective set out in subparagraph 3(a)(i) of the PCMLTFA. Record keeping requirements are important to Canada's anti-money laundering and anti-terrorist financing (AML/ATF) regime because they compel the preservation of the information that is needed to achieve the objectives of the PCMLTFA and FINTRAC's mandate. The information that is required to be kept serves to identify individuals and entities that own or control funds, or conduct, direct or are beneficiaries to transactions. The required information also helps clarify financial transactions and activities for the purposes of following the flow of funds (such as transaction amounts, dates, currency types, etc.); of understanding clients (such as the nature of their business, occupation, intended use of accounts, etc.); of identifying relationships (such as third party information); of providing evidence for law enforcement investigations and prosecutions, and complying with the legislation.

Records that businesses are required to keep serve many purposes for your business as an RE, law enforcement and FINTRAC. Records with missing, incomplete, incorrect or inadequate information may affect your ability to submit high-quality and timely transaction reports to FINTRAC and to conduct effective risk assessments. They may also interfere with law enforcement investigations, and with FINTRAC's ability to ensure compliance with the Act and its regulations.

2.13 Harm done in the case of violations related to keeping prescribed records

Accurate and complete record keeping is fundamental to the detection, prevention, deterrence, investigation and prosecution of ML/TF offences. Without the prescribed records, REs and government agencies would not be able to identify the individual or entity that owns or controls the funds, or conducts, directs or is a beneficiary of the financial transactions. Information could be lacking on individuals or entities involved in the financial transactions, on their relationships, and on the flow of funds. Failing to comply with record keeping requirements could lead to being non-compliant with transaction reporting requirements and having inadequate risk assessments. This could result in FINTRAC missing

key information for its analysis. This could also lead to situations where law enforcement would not be able to collect critical evidence in their investigations and prosecutions of ML/TF offences.

When a record is not kept, or if the information contained in a record is missing, unclear, incomplete or inaccurate, REs, FINTRAC and law enforcement agencies may be prevented from performing their functions effectively and contributing to the objectives of the PCMLTFA.

2.14 Penalty determination for violations related to keeping prescribed records

The Proceeds of Crime (Money Laundering) and Terrorist Activity Financing Administrative Monetary Penalties Regulations (AMP Regulations) allow a penalty ranging from $1 to $1,000 for violations related to record keeping.

FINTRAC has identified four levels of harm related to these violations by considering the intended purpose of the information that must be kept and the consequences of not complying with the requirements on Canada's AML/ATF regime. Levels of harm are also based on our ability to use the information to identify individuals, entities, transactions and the flow of funds, to understand ML/TF risks, and to ensure compliance as described below. The penalty range of $1 to $1,000 is divided into four even intervals. Each level of harm incurs a maximum penalty of either: $1,000, $750, $500 or $250.

The highest level of harm (Level 1), which incurs a penalty of $1,000, is for violations that would have the greatest negative impact on the achievement of the objectives of the PCMLTFA and on FINTRAC's mandate. The lowest of the four levels of harm (Level 4) incurs a penalty of $250. Penalty amounts may be reduced if there are mitigating factors. All factors that may reduce a penalty will be considered, potentially lowering the penalty to the $1 minimum set out in the AMP Regulations.

The information that must be kept under the Act and its regulations can serve one or more purposes. Therefore, non-compliance with one record keeping requirement can cause various harm to the achievement of the objectives of the Act and FINTRAC's mandate. The table below lists the levels of harm, the types of non-compliance and the descriptions of harm along with their corresponding penalty.

Level of harm	Type of non-compliance	Description of harm	Penalty (not considering mitigating factors)
Level 1	Information that identifies individuals or entities that conduct, own, direct, control or benefit from funds and transactions; OR information that identifies the flow of funds/transactions is non-compliant	Prevents the identification of individuals or entities that conduct, own, direct, control, or benefit from funds or financial transactions; OR prevents FINTRAC from iden- tifying the flow of funds/transactions	$1,000
Level 2	Information that identifies relationships or other parties to a transaction is non-compliant	Prevents the identification of relationships	$750
Level 3	Information that can be used to assess ML/TF risks posed by individuals and entities is non-compliant	Prevents the understanding of an individual or entity, including the expected activity, in order to assess ML/TF risk	$500
Level 4	Information to ensure compliance and efficiency in use of records is non-compliant	Reduces the ability to analyze or use the information for risk assessment, intelligence, compliance and investigation purposes in a timely manner	$250

Table 14—Levels of harm and penalties for violations related to keeping pre-

scribed records

2.14.1 Level 1 harm: Information that identifies individuals/entities or the flow of funds/transactions is non-compliant When there is no information on the flow of funds or transactions, it is not possible to pursue ML/TF offences. Those who are responsible for these offences must be held accountable or prevented from committing the crime, so it is equally important to have the information identifying the individuals and entities that conduct, own, direct, control, or benefit from the funds or transactions.

The records that are required for purposes of identifying individuals and entities, transactions and the flow of funds may be the only proof that a transaction was conducted and may be the only way to confirm the involvement of individuals and entities. Without this information, there can be no meaningful risk assessment, no transaction reporting, no analysis, and no investigation and prosecution. If the record is insufficient for use by law enforcement as evidence, the investigation or prosecution of an ML/TF offence may be dropped. Because this poses the highest level of harm, when records that contain information identifying individuals, entities or transactions are not kept, or if the information in the records is unclear, incomplete or inaccurate, the penalty is determined at the maximum of $1,000 per record.

2.14.2 Level 2 harm: Information that identifies relationships or other parties to a transaction is non-compliant The information that identifies the relationships between the individuals and entities that conduct, own, direct, control, or benefit from the funds or transactions can be used for risk assessment, transaction reporting, analysis, and investigations and prosecutions of ML/TF offences. This information indicates to FINTRAC the type and level of involvement of individuals and entities in transactions and is used to prioritize analysis work. When relationship information is missing, FINTRAC's ability to follow the flow of funds can be significantly limited. When the information that serves to identify relationships is not kept, or when the information is unclear, incomplete or inaccurate to the point of being useless, the penalty is $750 per record.

2.14.3 Level 3 harm: Information that can be used to assess ML/TF risks posed by individuals/entities is non-compliant The Act and its regulations require that information on the background of individuals and entities be kept on record. This information helps understand individuals or entities by supplementing identity information, transaction and relationship information. It gives REs more in-depth knowledge of clients which lets them conduct comprehensive assessments of ML/TF risks that go beyond the client identity, transaction and relationship information that must be kept. While this information may not be required in prescribed transaction reports (Large Cash Transaction Reports, Electronic Funds Transfer Reports, Casino Disbursement Reports), it may support the detection of suspicious transactions that must be

reported to FINTRAC, or the identification of activities and areas of higher risk that require enhanced monitoring. If a suspicious transaction report (STR) is submitted, this information could form part of the grounds for suspicion, be included in the report, analyzed by FINTRAC, and disclosed to law enforcement. Therefore, when a record containing this information is not kept, or when the information is unclear, incomplete or inaccurate to the point of being useless, the penalty is $500 per record.

2.14.4 Level 4 harm: Information to ensure compliance and the efficient use of records is non-compliant Certain records are used to verify compliance or to enhance efficiency. They may help support law enforcement investigations, but are not critical for risk assessment or financial analysis. For example, the requirement to record a date could confirm that an RE has carried out a regulatory requirement within the prescribed period. Although this type of information is not critical, it is useful to assess compliance and consequently, the penalty for non-compliance is $250 per record.

2.15 Mitigating factors

In all the cases described above, mitigating factors will be considered and may reduce the penalty. For example, a financial entity that opens an account is required to keep a signature card for each account holder. Failure to keep a signature card poses harm at the highest level (Level 1) because the information that identifies a person is non-compliant. The penalty is $1,000 in this case. However, if the non-compliance is discovered and corrected before transactions are conducted, the penalty could be reduced to $250 (consistent with Level 4), if, considering the circumstances, the non-compliance's only impact is to the use of the record (or the information) for its intended purpose.

2.16 Non-compliance in the case of records that serve more than one purpose

Most of the required records can be useful for more than one of the purposes described above. For this reason, when determining the penalty amount for non-compliant record keeping that results in more than one level of harm, the penalty is determined at the amount corresponding to the highest level of harm. When assessing the level of harm and determining a penalty, FINTRAC takes the entire record into consideration.

3.1 Harm done in the case of violations related to the retention period for prescribed records

Accurate and complete records are fundamental when it comes to supporting the detection, deterrence and prevention of ML/TF offences. Therefore, records must be available when required to assess compliance, or in support of investigations and prosecutions of ML/TF offences. Not keeping a record for the

prescribed retention period poses the same harm as not having kept the record at all. If records are not retained for the required five-year period, they cannot be accessed to conduct risk assessments, reporting and to ensure compliance. Most importantly, missing records may impact law enforcement investigations of ML/TF offences negatively due to lack of evidence.

3.2 Penalty determination for violations related to the retention period for prescribed records

Since not keeping a record for the required five years poses the same harm as not keeping a record, the penalty is the same, $1,000 per instance. Penalty amounts may be reduced if there are mitigating factors.

4.1 Harm done in the case of a violation related to the requirement to provide a record to an authorized person

The Act and its regulations require records to be kept in a format that can be produced within 30 days when FINTRAC requests to examine it.Footnote 5 Failing to comply with this requirement interferes with FINTRAC's ability to efficiently and effectively ensure compliance with Parts 1 and 1.1 of the PCMLTFA, in accordance with paragraph 40(e) of the PCMLTFA.

4.2 Penalty determination for a violation related to the requirement to provide a record to an authorized person

As failing to comply with this obligation would impact FINTRAC's ability to verify compliance with regulatory requirements in a timely manner, the penalty is set at $250 per record produced after the prescribed period. This is consistent with the amount corresponding to "Information to ensure compliance and efficiency in use of records is non-compliant" (Level 4), as shown in Table 14. When a record is not produced after an extensive delay beyond the prescribed 30-day period, FINTRAC may consider that there is a violation for failing to keep a prescribed record. Penalty amounts may be reduced if there are mitigating factors.

5. Repeated instances of a given violation

When a particular violation occurs multiple times, FINTRAC will consider its underlying cause, its type and other relevant facts to assess whether the level of harm should be reduced for the subsequent instances of that violation. For example, should repeated instances of a given violation affect only the efficiency of FINTRAC's analysis, it may be appropriate to assess its recurring instances at the base penalty of $250 each (Level 4 harm), regardless of the level of harm of the first occurrence.

Guide on harm done assessment for "Know your client" requirements violations

1. Introduction

This page presents how we assess the harm done and calculate the base penalty amount applied to "Know your client" violations.

1.1 Purpose of the guide

This guide presents how FINTRAC approaches the harm done criterion and the base penalty amount for violations under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (the Act) and its regulations. According to section 73.11 of the Act, FINTRAC must consider the harm done by a violation, that the purpose of an administrative monetary penalty (AMP) is to encourage compliance rather than to punish, and all other criteria prescribed in the regulations, including a reporting entity's (RE) history of compliance, when determining the amount of a penalty. Considerations for the non-punitive nature of an AMP and an REs' compliance history are assessed in another step in the penalty calculation and are outlined separately in FINTRAC's AMP policy.

1.2 Definition of harm

FINTRAC defines "harm" as the degree to which a violation interferes with achieving the objectives of the Act Footnote 1 or with FINTRAC's ability to carry out its mandateFootnote 2. Therefore, the consequences of non-compliance, when an AMP is imposed, are linked to its effects on Canada's efforts to combat money laundering and terrorist activity financing (ML/TF).

Compliance enforcement activities are undertaken to prevent and correct the harm that comes from non-compliance with the Act and regulations. REs' adherence to requirements such as record keeping and verifying client identity assists in the deterrence of ML/TF and supports investigations and criminal prosecutions. The requirements related to reporting ensure that FINTRAC is supplied with the high-quality, timely financial transaction reports it needs to produce the financial intelligence that helps with the investigation and prosecution of ML/TF offences.

1.3 Considering harm in AMP calculations

When determining a penalty, FINTRAC considers the harm caused, that is, the degree to which the non-compliance interferes with the purpose of the Act and/or with FINTRAC's mandate. Non-compliance and harm are measured using the standards described in this guide, which outline the benchmark amounts for the corresponding levels of harm for a specific violation. FINTRAC considers the specific circumstances of each case, including the extent of the non-compliance and mitigating factors, which may further reduce the actual amounts

applied.

2. Violations related to "Know your client" (KYC) requirements

One of the most important things we can do to protect our financial system from being exploited for ML/TF activities is to remove anonymity from financial transactions.

Criminals convert, conceal and transfer their assets without detection by hiding their identities when conducting financial transactions.

Therefore, requirements such as verifying the identity of individuals, confirming the existence of entities, determining whether a person is acting on behalf of a third party or if an account will be used by a third party, and determining the beneficial ownership of an entity have been put in place to make our financial system less anonymous. As a consequence of these requirements, those who are conducting transactions, and those that are directly or indirectly in control of, or benefit from funds and transactions, will be known and this information will be documented. These measures are of utmost importance to detect, prevent and deter the exploitation of Canada's financial system. Violations related to these requirements interfere with the achievement of subparagraph 3(a)(i) of the Act and result in vulnerabilities in Canada's anti-money laundering and anti-terrorist financing (AML/ATF) regime, particularly when it comes to detecting ML/TF activities and deterring those criminals who would use our financial system for these purposes.

3. Violation related to opening an account when client identity cannot be established

3.1 Harm done in the case of a violation related to opening an account when client identity cannot be established

If an account is knowingly opened but the identity of the account holder cannot be verified, then the account holder can control the funds without being directly associated to the funds, and without being detected. Anonymous financial transactions and activities allow criminals to accumulate, transfer, convert and conceal assets from the authorities. In order to protect Canada's financial system from abuse, financial entities, securities dealers and casinos are prohibited from opening an account for a client whose identity cannot be ascertained.

Verifying the identity of the parties to financial transactions and activities removes the anonymity behind the transactions. This requirement deters those who would launder the proceeds of crime or finance terrorist activities, and when combined with record keeping requirements, it also serves as a tool for law enforcement to investigate and prosecute ML/TF-related offences.

3.2 Penalty determination for a violation related to opening an account when client identity cannot be established

When an account has been opened for client and their identity cannot be verified in accordance with the Act and its regulations, and at least one financial transaction has been conducted on the account, the maximum prescribed penalty of $100,000 is applied. If no transaction has been conducted, FINTRAC may consider this to be a mitigating factor and reduce the penalty.

4. Violations related to verifying client identity

This section outlines FINTRAC's approach to the violations related to the requirement to verify client identity in prescribed circumstances, including the harm assessment and penalty calculation.

4.1 Harm done in the case of violations related to verifying client identity

Verifying the identity of the parties to financial transactions and activities removes the anonymity behind them by identifying the individuals and entities responsible for the movement of the funds. The information collected during the process of verifying identity of an individual, or confirming the existence of an entity, must be recorded so that it can later be used to report to FINTRAC, in the RE's risk assessments and ongoing monitoring of business relationships. Verifying identity is necessary not only to meet client identification requirements, but also to meet record keeping requirements.

Verifying the identity of the parties to financial transactions and activities deters those who would launder the proceeds of crime or finance terrorist activities. When combined with the associated record keeping requirements, client identity verification also provides records and evidence for the ML/TF investigations and prosecutions of ML/TF offences.

Ultimately, without knowing the identity of the individuals involved in financial transactions potentially related to ML/TF offences, REs cannot conduct appropriate risk assessments, ongoing monitoring of business relationships or put in place mitigation measures. Furthermore, FINTRAC and its law enforcement partners cannot follow the flow of funds to combat these illegal activities, prevent future illegal activities, and protect the integrity of Canada's financial system and the safety of Canadians.

4.2 Penalty determination for violations related to verifying client identity

The PCMLTFR set out the ways by which individuals must be identified, and the existence of entities confirmed, as well as the timelines for making these verifications. The requirements were developed to make sure that the verification

of identity is done with methods that are accurate and timely, in support of FINTRAC and law enforcement agencies' purposes.

Given the importance of removing anonymity in financial transactions and activities conducted, when an RE has not taken measures to verify client identity, the maximum penalty of $1,000 per instance will apply, as this constitutes a complete violation or disregard for the requirement.

When the methods used to verify identity are not in accordance with the methods set out in the PCMLTFR, the client's identity is considered not to have been verified, therefore the harm to achieving the objectives of the PCMLTFA and FINTRAC's mandate is the same as with not taking steps to verify client identity and the same penalty ($1,000 per instance) will apply. Relevant mitigating factors of each case will be considered and may reduce the actual penalty amount. For example, if the RE did not verify the identity of the client within the prescribed period, but did so subsequently.

When an account is knowingly opened for a client without verifying client identity or confirming the existence of an entity, this is a violation of the prohibition under section 9.2 of the Act, which is a "serious" violation and carries a maximum penalty of $100,000. See *Violation related to opening an account when client identity cannot be established*.

4.3 Violations related to client identification information records

See the guide on harm done assessment for record keeping violations for the harm rationale and penalty calculation for the violations below.

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
6	64.2	Failure of a person or entity that is required to ascertain a person's identity to keep prescribed information	Minor$1-$1,000

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
6	65(3)	Failure of a person or entity who ascertains information in respect of a corporation by referring to an electronic version of a record to keep a prescribed record	Minor$1-$1,000
6	65(4)	Failure of a person or entity who ascertains information in respect of a corporation by referring to a paper copy of a record to retain the record or a copy of it	Minor$1-$1,000
6	66(3)	Failure of a person or entity who ascertains information in respect of an entity by referring to an electronic version of a record to keep a prescribed record	Minor$1-$1,000

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
6	66(4)	Failure of a person or entity who ascertains information in respect of an entity by referring to a paper copy of a record to retain the record or a copy of it	Minor$1-$1,000

Table 4—Violations related to client identification information records

5. Violations related to third party determination

This section outlines FINTRAC's approach to the violations related to the requirement to make a third party determination, including the harm assessment and penalty calculation.

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
6	8(1)	Failure to take reasonable measures to determine if an individual giving cash is acting on behalf of a third party	Minor$1-$1,000
6	9(1)	Failure to take reasonable measures when opening an account to determine if the account is to be used by or on behalf of a third party	Minor$1-$1,000

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
6	10(1)	Failure to take reasonable measures when client information record is created to determine whether the client is acting on behalf of a third party	Minor$1-$1,000
6	44(1)	Failure of a casino to take reasonable measures to determine if a person who receives a prescribed disbursement is acting on behalf of a third party	Minor$1-$1,000

Table 5—Violations related to third party determination

5.1 Harm done in the case of violations related to third party determination

Criminals who would launder the proceeds of crime or finance terrorist activities often resort to third parties to hide their identity. By doing so, they mask their involvement in the financial transactions and activities, maintain their anonymity while giving instructions for the funds and while retaining the benefits of the funds. The PCMLTFR require RE to take reasonable measures to determine whether a transaction is being conducted on behalf of a third party, whether a client is acting on behalf of a third party or whether an account will be used for the benefit of a third party. Failing to make a third party determination may result in financial transactions and activities being directed by unknown individuals and entities. When this occurs, REs cannot properly assess the risks posed by the transactions/activities, or report on all the parties involved in the transactions conducted. The information on third parties involved in transactions is required to be reported so that FINTRAC can properly conduct analysis to establish relationships, determine the individuals or entities directing transactions and the flow of funds, and law enforcement can effectively investigate

and prosecute ML and TF offences.

5.2 Penalty determination for violations related to third party determination

The PCMLTFR require that reasonable measures be taken to make a third party determination. The reasonable measures taken must be in line with those described in FINTRAC's guidance and documented in the RE's compliance policies and procedures. As reasonable measures include simply asking the client if they are acting on someone else's behalf or retrieving information from existing records, an RE who does not take any measures to make a third party determination has fully interfered with the purpose of the requirement, which is to eliminate anonymity and identify the individuals/entities that are giving instructions on transactions/activities conducted. Given the importance of removing anonymity in financial transactions and activities, the maximum prescribed penalty of $1,000 applies. This amount may be reduced in consideration of the relevant mitigating factors of each situation.

5.3 Violations related to third party information records

See the guide on harm done assessment for record keeping violations for the harm rationale and penalty calculation for the violations below.

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
6	8(2)	Failure to keep a record of prescribed information respecting third parties	Minor$1-$1,000
6	9(2)	Failure to keep a record of prescribed information respecting third parties	Minor$1-$1,000
6	10(2)	Failure to keep a record of prescribed information when it is determined that the client is acting on behalf of a third party	Minor$1-$1,000

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
6	44(2)	Failure of a casino to keep a record of prescribed information when it is determined that the client is acting on behalf of a third party	Minor$1-$1,000

Table 6—Violations related to third party information records

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
6	8(3)	Failure to keep a record of prescribed information respecting suspected third parties	Minor$1-$1,000
6	9(3)	Failure to keep a record of prescribed information in respect of suspected third parties	Minor$1-$1,000
6	10(3)	Failure to keep a record of prescribed information when there are reasonable grounds to suspect that the client is acting on behalf of a third party	Minor$1-$1,000

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
6	44(3)	Failure of a casino to keep a record of prescribed information when there are reasonable grounds to suspect that the client is acting on behalf of a third party	Minor$1-$1,000

Table 7—Violations related to suspected third party information records

6. Violation related to inter vivos trust information records

See the guide for harm done assessment for record keeping violations for the harm rationale and penalty calculation for the following violation.

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
6	11	Failure of a trust company to keep a record of prescribed information concerning inter vivos trusts	Minor$1-$1,000

Table 8—Violation related to inter vivos trust information records

7. Violation related to beneficial ownership

7.1 Harm done in the case of a violation related to beneficial ownership

Removing anonymity and identifying the **natural** persons behind transactions and account activities is a key component of Canada's AML/ATF regime. Beneficial owners hiding behind entities, including corporations is a technique used in many ML/TF schemes. An important step in the detection, prevention and deterrence of ML/TF is the collection and verification of beneficial ownership

information, which also support ML/TF investigations, and ultimately protect the integrity of Canada's financial system and the safety of Canadians.

If measures are not taken to obtain this information, there is a risk that transactions and account activities will be conducted without knowing the individuals controlling, benefitting from, or giving the instructions for the transactions. This could completely interfere with the objective of subparagraph 3(a)(i) of the PCMLTFA. This also prevents the RE from properly assessing the risks associated, law enforcement from effectively investigating and prosecuting ML and TF offences, and FINTRAC from using the information in support of its mandate, particularly in cases where the information helps establish reasonable grounds to suspect that a transaction is related to an ML/TF offence.

7.2 Penalty determination for a violation related to beneficial ownership

If an RE fails to obtain the prescribed information on the persons controlling an entity, the detection, prevention and deterrence purpose of this requirement, as described above, is completely impeded. Given the importance of removing anonymity in financial transactions and activities, the prescribed maximum penalty of $1,000 applies. This amount may be reduced in consideration of mitigating factors for each situation.

8. Violation related to confirming the accuracy of information on the control of an entity

8.1 Harm done in the case of a violation related to confirming the accuracy of information on the control of an entity

The requirement to take reasonable measures to confirm the accuracy of the prescribed information is not only to ensure the reliability of the information obtained, but also to deter clients from providing false information regarding the control, ownership or structure of entities. Removing anonymity from transactions is a key component of the detection, prevention and deterrence of ML and TF. Failing to take reasonable measures to confirm the accuracy of the prescribed information may result in unreliable information and in the true identity of the individuals behind transactions remaining unknown. In such situations, law enforcement cannot rely on the information to investigate or prosecute ML/TF offences, the RE cannot conduct proper risk assessments and ongoing monitoring of business relationships. In a worst case scenario, should the accuracy of beneficial ownership information be the only fact for establishing reasonable grounds to suspect that a transaction or attempted transaction is related to an ML/TF offence, it could result in an unreported suspicious transaction as that relevant suspicion would be missing. In the case where a suspicious transaction report (STR) was submitted containing beneficial ownership information in Part G that was not confirmed for accuracy, it could result in FINTRAC analyzing incomplete or inaccurate information and therefore the

true flow of funds or individuals behind suspicious transactions could not be established.

8.2 Penalty determination for a violation related to confirming the accuracy of information on the control of an entity

Given the importance of removing anonymity in financial transactions and account activities, the maximum prescribed penalty of $1,000 applies. This amount may be reduced in consideration of relevant mitigating factors of each situation.

9. Violation related to records on beneficial ownership information

See the guide on harm done assessment for record keeping violations for the harm rationale and penalty calculation for the violation below.

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
6	11.1(3)	Failure to keep a record of the prescribed information and the measures taken to confirm its accuracy	Minor$1-$1,000

Table 11— Violation related to records on beneficial ownership information

10. Violation related to ascertaining the identity of an entity's most senior managing officer

10.1 Harm done in the case of a violation related to ascertaining the identity of an entity's most senior managing officer

One of the most important things we can do to protect our financial system from being exploited for ML/TF purposes is to remove anonymity from financial transactions. It is important, not only to confirm the existence of an entity, but to also take reasonable measures to identify the individuals who are in control of it. When an RE is unable to obtain or confirm the accuracy of beneficial ownership information, individuals could be controlling an entity anonymously. This poses a higher risk for ML/TF offences, as individuals with criminal intent may remain undetected while potentially higher-risk activities are overlooked. Therefore, when the beneficial ownership information of an entity is not clear or cannot be established, an RE must verify the identity of the most senior person

who can control the financial transactions of the entity, and treat the activities of the entity as high risk. Failing to take these additional measures could leave Canada's financial system vulnerable to ML and TF caused by individuals criminally utilizing the entities they control anonymously.

10.2 Penalty determination for a violation related to ascertaining the identity of an entity's most senior managing officer

Failing to take reasonable measures to verify the identity of the most senior managing officer and treat the activities of the entity as high risk will result in the prescribed maximum penalty of $100,000. This amount may be reduced in consideration of relevant mitigating factors each situation.

11. Violations related to politically exposed persons (PEP) and heads of international organizations (HIO) determination

11.1 Harm done in the case of violations related to PEP and HIO determination

A PEP or HIO is a person entrusted with a prominent position that typically comes with the opportunity to influence decisions and the ability to control resources. The influence and control a PEP or HIO puts them in a position to impact policy decisions, institutions and rules of procedure in the allocation of resources and finances, which can make them vulnerable to corruption. It is important to understand that the possibility for corruption exists, and that PEPs and HIOs can be vulnerable to carrying out, or being used for, ML/TF offences.

The requirements concerning PEPs, HIOs and their family members and close associates have been put in place because of concerns about their higher vulnerability to corruption, and related higher risk of money laundering. Canada and the Financial Action Task Force (FATF) attach a great deal of importance to the fight against corruption as it has the potential to bring great harm to economic development, the fight against organized crime and the respect for law and effective governanceFootnote 5.

Therefore, under prescribed circumstances, financial entities; securities dealers; life insurance companies, brokers, and agents; and money services businesses are required to take reasonable measures to identify PEPs, HIOs, family members and persons closely related to them so that prescribed measures can be taken to mitigate risks. If REs fail to make the determination, risk mitigation measures cannot be applied.

11.2 Penalty determination for violations related to PEP and HIO determination

The determination of PEPs, HIOs and their family members and close associates, is the pre-requisite to taking the prescribed measures to mitigate risks. Without first making the determination, no mitigating measures can be applied and potentially higher-risk clients and their activities could remain undetected. As such, this type of violation carries the maximum penalty of $1,000. This amount may be reduced in consideration of the relevant mitigating factors of each situation. For example, should FINTRAC become aware of the violation prior to any transaction being conducted, the penalty may be reduced to the lower end of the penalty range to an amount that is sufficient to encourage compliance with the requirement, while recognizing that the potential harm is reduced considering that no transactions have been conducted.

12. Violations related to source of funds determination

12.1 Harm done in the case of violations related to source of funds determination

Once it has been determined that an individual is a PEP, a HIO, a family member or close associate, REs are required to determine the source of the funds that have been, will be or are expected to be deposited into an account; or to establish the source of the funds used in a prescribed transaction. The requirements concerning PEPs, HIOs, their family members and close associates have been put in place because of concerns over these individuals' higher vulnerability to corruption and related higher risk of money laundering. These requirements mitigate the inherent risks by allowing REs to know their clients, which deters criminal elements, by allowing REs to assess the ML/TF risk through the identification of the source of the funds, and through the detection of transactions that must be reported. Not complying may result in the improper assessment of ML/TF risks, which potentially leads to not applying the required mitigation measures and not reporting to FINTRAC.

12.2 Penalty determination for violations related to source of funds determination

Once it has been determined that a client is a PEP, HIO, family member or close associate, a higher risk situation has been identified. Not taking reasonable measures to determine the source of funds for these higher-risk clients will result in the prescribed maximum penalty of $1,000 per instance. This amount may be reduced in consideration of the relevant mitigating factors of each situation. For example, should FINTRAC become aware of the violation prior to any transaction being conducted, the penalty may be reduced to the lower end of the penalty range to an amount that is sufficient to encourage compliance with the requirement, while recognizing that the potential harm is reduced considering no transactions have been conducted.

13. Violations related to obtaining senior management approval to keep an account open or reviewing a prescribed transaction

13.1 Harm done in the case of violations related to obtaining senior management approval to keep an account open or reviewing a prescribed transaction

The requirements concerning PEPs, HIOs, their family members and close associates have been put in place because of concerns over these individuals' higher vulnerability to corruption and related higher risk of money laundering. Canada and the FATF attach a great deal of importance to the fight against corruption because corruption can harm economic development; interfere with the fight against organized crime, and with respect for the law and effective governance-Footnote 6. When the approval to keep an account open is not obtained, or when a transaction is not reviewed by senior management, higher ML/TF risks may not be properly assessed and understood sufficiently to conduct effective risk assessments and to ensure that the proper mitigation measures are applied.

13.2 Penalty determination for violations related to obtaining senior management approval to keep an account open or reviewing a prescribed transaction

Once it has been determined that a client is a PEP, HIO, family member or close associate, a higher-risk situation has been identified. Failing to obtain senior management's approval to keep the account open or failing to ensure that senior management reviews prescribed transactions in these higher-risk situations will result in the maximum penalty of $1,000 per instance. This amount may be reduced in consideration of the relevant mitigating factors of each situation. For example, should FINTRAC become aware of the violation prior to any transaction being conducted, the penalty may be reduced to the lower end of the penalty range to an amount that is sufficient to encourage compliance with the requirement, while recognizing that the potential harm is reduced considering that no transactions have been conducted.

14. Violations related to records for PEPs and HIOs

14.1 Violation related to enhanced ongoing monitoring of activities in respect of a PEP or HIO's account

This section outlines FINTRAC's approach to the violation related to enhanced ongoing monitoring of the activity on PEP and HIO's accounts, including the harm assessment and penalty calculation.

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
9.3(2)	67.1(1)(c) and (2)	Failure of a financial entity or securities dealer to conduct enhanced ongoing monitoring of the activities in respect of an account	Minor$1-$1,000

14.2 Harm done in the case of a violation related to enhanced ongoing monitoring of activities in respect of a PEP or HIO's account

When there is the potential for an increased risk of ML/TF offence, such as when a client is a politically exposed foreign person, or their family member or close associate, enhanced ongoing monitoring the client's account is a key measure that supports the detection, prevention and deterrence of ML/TF. Without enhanced ongoing monitoring, the level of scrutiny may not be appropriate to detect the transactions that would raise concern, which could result in the failure to detect the suspicious transactions or attempted suspicious transactions that are required to be reported to FINTRAC.

Ongoing monitoring must be conducted for the purposes of 1) detecting suspicious transactions that are required to be reported, 2) keeping client information up to date, 3) reassessing the level of risk, and 4) determining whether the transactions and activities are consistent with the information and risk level associated to a given client. Enhanced ongoing monitoring means that the above listed measures are conducted more frequently. When only some of the prescribed enhanced ongoing monitoring measures are conducted, or when all measures are conducted but not more frequently than for a lower risk situation, the ML/TF risks are only partially mitigated. Therefore, the penalty amount may be reduced based on the circumstances. When not performing enhanced ongoing monitoring results in the failure to report an STR, a separate violation and penalty can be imposed.

14.3 Penalty determination for a violation related to enhanced ongoing monitoring of activities in respect of a PEP or HIO's account

The penalty is set at the prescribed maximum amount of $1,000 for each account where enhanced ongoing monitoring is not conducted. This violation poses a high level of harm to the achievement of the objectives of the PCMLTFA and of FINTRAC's mandate, since the activity on an account held by an individual identified as being vulnerable to ML/TF offences could remain overlooked;

in some cases, this may also result in the failure to report suspicious transactions. This amount may be reduced in consideration of mitigating factors for each situation. For example, if no activity was conducted within the PEP or HIO's accounts prior to FINTRAC identifying the violation.

15. Violation related to ongoing monitoring of business relationships

15.1 Harm done in the case of a violation related to ongoing monitoring of business relationships

The requirement to conduct ongoing monitoring of a business relationship is in place to protect REs and Canada's financial system from ML/TF.

Failing to comply with the ongoing monitoring requirement can impact the objectives of the PCMLTFA which are to detect, prevent and deter ML/TF. When an RE fails to conduct ongoing monitoring of business relationships, it is unaware of changes to the client's transactions, activities, and circumstances; especially those that may pose a higher risk of ML/TF. When the RE is unaware, the client's information and risk assessment are not updated to reflect the true level of risk. This can potentially result in ineffective risk mitigation, and unreported transactions. When a high-risk client or business relationship is undetected because of a lack of ongoing monitoring, the RE's operations and Canada's financial system could be at risk. Should a lack of ongoing monitoring result in the failure to submit STRs, there is also an impact on FINTRAC's mandate which is to analyze and disclose information to assist in the detection, prevention and deterrence of ML/TF.

In addition, the requirement to record the measures taken and the information obtained demonstrates compliance with continuously assessing ML/TF risks, applying appropriate mitigation measures and detecting information that is required to be reported to FINTRAC. These reports support FINTRAC's analysis and disclosure mandate, which provides valuable financial intelligence to law enforcement agencies. Not keeping a record of the information obtained would not only interfere with the purposes listed above, but could also affect law enforcement investigations and prosecutions of ML/TF if client information is not up to date.

15.2 Penalty determination for a violation related to ongoing monitoring of business relationships

The Proceeds of Crime (Money Laundering) and Terrorist Financing Administrative Monetary Penalties Regulations (AMP Regulations) allow for a penalty ranging from $1 to $1,000 for violations of ongoing monitoring requirements.

FINTRAC has identified four levels of harm related to these violations by considering their impact on the objectives of the PCMLTFA or on FINTRAC's mandate. To create a penalty scale based on harm done, the above-mentioned

penalty range is divided in four to correspond with the identified levels of harm: $1,000, $750, $500 and $250.

The highest harm category (Level 1) is assigned the maximum amount of $1,000 as it would have the greatest effect on the objectives of the PCMLTFA or on FINTRAC's mandate. The lowest of the four harm levels (Level 4) has a penalty of $250. Penalty amounts may be reduced if there are mitigating factors, but must be enough to encourage a change in compliance behaviour.

We consider all factors that may reduce a penalty to the $1 minimum set out in the AMP Regulations.

15.2.1 Level 1 harm—No ongoing monitoring measures conducted In situations where no ongoing monitoring measures are taken, the potential impact on the objectives of the PCMLTFA and on FINTRAC's mandate is the greatest; therefore the harm posed is highest. As such, the penalty is determined at the prescribed maximum of $1,000.

15.2.2 Level 2 harm—Reassessment of risk levels and transaction monitoring not conducted In cases where some ongoing monitoring measures are taken and the non-compliance relates to the risk assessment or transaction monitoring, the harm is somewhat reduced compared to Level 1. However, this type of non-compliance could lead to the ineffective mitigation of ML/TF risks posed by the business relationship, or to the ineffective detection of suspicious transactions that need to be reported. This would pose high harm to the achievement of the objectives of the PCMLTFA and FINTRAC's mandate, therefore the penalty is set at $750.

15.2.3 Level 3 harm—Client information not kept up to date In cases where some ongoing monitoring measures are conducted and the non-compliance relates to keeping client information up to date, the harm on the objectives of the PCMLTFA and on FINTRAC's mandate is significant, but less important when non-compliance can affect ML/TF risk mitigation. While incomplete or outdated client information can be used in transaction reports or in law enforcement investigations, higher risk transactions may still be detected, mitigated, and reported to FINTRAC for analysis. As such, the penalty is set at $500.

15.2.4 Level 4 harm—Minor record keeping non-compliance When ongoing monitoring measures are taken and the non-compliance relates to record keeping requirements that do not prevent the use of the information for risk assessments, risk mitigation, transaction reporting, intelligence analysis, compliance and investigations in a timely manner, the harm to the achievement of the objectives of the PCMLTFA and FINTRAC's mandate is reduced. As such, the penalty is set at $250.

16. Violations related to treating the activities of a person or an entity as high-risk

16.1 Harm done in the case of violations related to treating the activities of a person or an entity as high-risk

The PCMLTFR set out specific circumstances under which an RE must treat the activities of clients as high-risk and apply the prescribed special measures to mitigate the heightened risks. The prescribed special measures that are required to be taken are the development and application of written policies and procedures for taking enhanced measures, based on the risk assessment undertaken, to ascertain the identify of clients, and taking any other enhanced measures to mitigate risks including keeping client information up to date and conducting ongoing monitoring of business relationships for the purpose of detecting suspicious transactions that are required to be reported to FINTRAC. Failure to do so would mean that the necessary controls, policies and processes are not in place to for high risk situations and consequently, high-risk transactions and activities could be allowed to proceed without mitigation and reporting. This could result in STRs not being submitted to FINTRAC, and information not being available for analysis and disclosure to police and law enforcement. Ultimately, this could leave Canada's financial system and Canadians vulnerable to abuse for ML/TF purposes.

16.2 Penalty determination for violations related to treating the activities of a person or an entity as high-risk

The AMP Regulations allow for a penalty ranging from $1 to $100,000 for failing to treat prescribed client activities as high-risk and taking the prescribed special measures. FINTRAC has identified five levels of harm related to these violations by considering their impact on the objectives of the PCMLTFA or on FINTRAC's mandate. To create a penalty scale based on harm done, the above-mentioned penalty range is divided in five to correspond with the identified levels of harm: $100,000, $75,000, $50,000, $25,000 and $10,000.

The highest harm category (Level 1) is assigned the prescribed maximum amount of $100,000 as it would have the greatest effect on the objectives of the PCMLTFA or on FINTRAC's mandate. The lowest of the five harm levels (Level 5) has a penalty of $10,000. The rationale for setting this amount as the lowest is based on the notion set out in subsection 4(2) of the AMP Regulations which establishes that a series of "minor" violations amounting to a total penalty of $10,000 or more is considered a "serious" violation.

Penalty amounts may be reduced if there are mitigating factors, but the amount must be enough to encourage a change in compliance behaviour with respect to high-risk activities. We consider all factors that may reduce a penalty to the $1 minimum set out in the AMP Regulations.

16.2.1 Level 1 harm—Specified client activities are not treated as high-risk and there are no policies and procedures on prescribed special measures When an RE fails to treat prescribed activities as high-risk and there are no policies and procedures for taking enhanced measures to mitigate the risks, there is a weakness at the compliance program level which poses the most harm. If there is no system in place to ensure that enhanced measures are applied to mitigate the high risk posed by certain activities, it is more likely that the objectives of the PCMLTFA which are to detect, prevent and deter ML/TF would be hindered. This could leave both the RE's operations and Canada's financial system more vulnerable to ML/TF. An RE in this situation would not have set out the concrete steps to take in order to reduce or prevent those risks. High-risk clients, transactions and activities could go undetected while suspicious transactions are not reported to FINTRAC. Unreported suspicious transactions lead to a loss of intelligence for investigations of ML/TF offences. Therefore the maximum penalty of $100,000 applies under these circumstances.

16.2.2 Level 2 harm—Policies and procedures for taking enhanced measures are developed but not applied The second highest level of harm relates to cases where policies and procedures related to taking enhanced measures for high-risk exist, but they are not being applied in practice. As mitigating measures are not taken, the prescribed activities are in fact not being treated as high-risk according to the requirements set out in the PCMLTFR. Therefore, the impact is nearly the same as in Level 1. However, an RE in this situation could more readily apply the procedures that it has developed in order to mitigate high-risk activities; therefore the harm done is potentially reduced. The penalty is $75,000 which remains at the higher end of the prescribed range but is less than that of Level 1 harm.

16.2.3 Level 3 harm—Enhanced ongoing monitoring, for purposes of detecting suspicious transactions, not conducted In cases where some enhanced measures are taken but the non-compliance relates to the requirement to conduct enhanced ongoing monitoring for the purpose of detecting suspicious transactions to be reported, the harm done is less than in the two previous circumstances. While other prescribed special measures are taken that could mitigate some risks, the potential unreported suspicious transactions can have a significant impact on FINTRAC's intelligence mandate, the investigation or prosecution of ML/TF offences, and other objectives of the PCMLTFA. Therefore, the penalty is set at mid-range, which is $50,000.

16.2.4 Level 4 harm—Enhanced measures are not taken to verify client identification or keep client information, including beneficial ownership information, up to date REs are required to take enhanced measures to ascertain the identity of clients whose activities are deemed high risk. Taking enhanced measures means doing more than what is set out in regular identity verification procedures, to ensure that the identity of the client is

verified and that transactions and activities are not conducted anonymously. If an RE fails to apply these enhanced measures, some risks would not be mitigated and it could leave the RE's operations and Canada's financial system vulnerable to ML/TF. Similarly, if an RE does not take enhanced measures to keep client information up to date in situations of high-risk, outdated or incomplete information could be used in risk assessments, transaction reports, or investigations. The harm posed is less than in Level 3, as some client information is still available although not necessarily complete or up to date. As such, the penalty is set at $25,000.

16.2.5 Level 5 harm—Other enhanced measures not taken to mitigate risks identified When the non-compliance relates to the failure to develop and apply policies and procedures to take any other enhanced measures to mitigate the risks identified (i.e., other than performing enhanced measures to verify client identification, conduct ongoing monitoring and keep client information up to date), effective risk assessment and mitigation, and the timely and efficient availability of information for transaction reporting, analysis, compliance and investigations ML/TF are diminished. The penalty is set at $10,000.

17. Repeated instances of a given violation

When a particular violation occurs multiple times, FINTRAC will consider its underlying cause, its type and other relevant facts to assess whether the level of harm should be reduced for the subsequent instances of that violation. For example, should repeated instances of a given violation only affect the efficiency of FINTRAC's analysis, it may be appropriate to assess its recurring instances at the base penalty of $250 (level 4 harm), regardless of the level of harm of the first occurrence.

Politically exposed persons and heads of international organizations guidance

Overview

All reporting entities (REs) have politically exposed persons (PEPs) and heads of international organizations (HIOs) requirements under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and associated Regulations. However, some requirements and the examples given in this guidance may only apply to certain REs.

References to PEPs in this guidance include both foreign and domestic PEPs, unless otherwise specified.

The access, influence and control that PEPs and HIOs have can make them vulnerable to corruption and the potential targets of criminals who could exploit their status and use them, knowingly or unknowingly, to carry out money

laundering (ML) or terrorist activity financing (TF) offences.Footnote 1 The family members and close associates of PEPs and HIOs are potential targets as well because they can more easily avoid detection.

This guidance explains your obligations under the PCMLTFA and associated Regulations in relation to determining who are PEPs, HIOs, and persons related or closely associated to them. It also provides clarity on related terminology and considerations.

1. Who is a domestic PEP?

A **domestic PEP** is a person who currently holds, or has held within the last 5 years, a specific office or position in or on behalf of the Canadian federal government, a Canadian provincial (or territorial) government, or a Canadian municipal government. Specifically, the person has held the office or position of:Footnote 2

- Governor General, lieutenant governor or head of government;
- member of the Senate or House of Commons or member of a legislature;
- deputy minister or equivalent rank;
- ambassador, or attaché or counsellor of an ambassador;
- military officer with a rank of general or above;
- president of a corporation that is wholly owned directly by His Majesty in right of Canada or a province;
- head of a government agency;
- judge of an appellate court in a province, the Federal Court of Appeal or the Supreme Court of Canada;
- leader or president of a political party represented in a legislature; or
- mayor, reeve or other similar chief officer of a municipal or local government**.

****Note**: In line with legislation across Canada, municipal governments include cities, towns, villages and rural (county) or metropolitan municipalities. As such, a mayor is the head of a city, town, village and rural or metropolitan municipality, regardless of the size of the population.

A person **ceases** to be a domestic PEP **5 years** after they have left office or **5 years** after they are deceased.Footnote 3 You must continue to mitigate the risks associated with domestic PEPs until they cease to be domestic PEPs.

2. Who is a foreign PEP?

A **foreign PEP** is a person who holds or has held one of the following offices or positions in or on behalf of a foreign state:Footnote 4

- head of state or head of government;
- member of the executive council of government or member of a legislature;
- deputy minister or equivalent rank;

- ambassador, or attaché or counsellor of an ambassador;
- military officer with a rank of general or above;
- president of a state-owned company or a state-owned bank;
- head of a government agency;
- judge of a supreme court, constitutional court or other court of last resort; or
- leader or president of a political party represented in a legislature.

These persons are foreign PEPs regardless of citizenship, residence status or birthplace.

Once you determine that a person is a foreign PEP, they remain a foreign PEP **forever**(including deceased foreign PEPs). You are not required to determine whether they are a foreign PEP again.Footnote 5

3. Who is a HIO?

A HIO is a person who currently holds or has held within the last 5 years the specific office or position of head of an international organization and the international organization that they head or were head of is either:Footnote 6

1. an international organization established by the governments of states;
2. an institution of an organization referred to in 1 above; or
3. an international sports organization.

An institution established by an international organization does not have to operate internationally and it is possible that an institution only operates domestically, or in one jurisdiction.

The HIO is the primary person who leads the organization. For example, the HIO could be a president or CEO.

A person **ceases** to be a HIO **5 years** after they are no longer the head of the organization or institution or **5 years** after they are deceased.Footnote 7 You must continue to mitigate the risks associated with HIOs until they cease to be HIOs.

4. What is an international organization?

To determine whether a person is a HIO, you must first determine whether you are dealing with an international organization. An international organization is set up by the governments of more than one member country, has activities in several countries, and is bound by a formal agreement among member countries. An international organization has its own legal status, and it is an entity that is distinct from the member countries.

Looking at how an organization was established will help you to determine if it is an international organization. For example, if the organization was established by a formally signed agreement between the governments of more than one

country, then it is likely an international organization, and the head of that organization is a HIO.

International organizations are recognized by their member countries, but they are not resident organizations of any country. For examples of international organizations and institutions established by international organizations, see Annex 1.

5. Who is a family member of a PEP or HIO?

If a person is a PEP or HIO, some of their family members are considered family members of PEPs or HIOs under the PCMLTFA and associated Regulations. These family members are:Footnote 8

- their spouse or common-law partner;
- their biological or adoptive child(ren);
- their mother(s) or father(s);
- the mother(s) or father(s) of their spouse or common-law partner (mother-in-law or father-in-law); and
- the child(ren) of their mother or father (sibling(s)).

Once you determine that a person is a family member of a foreign PEP (including a deceased foreign PEP), they remain a family member of a foreign PEP forever and you are not required to make this determination again.Footnote 9

Once you determine that a person is a family member of a domestic PEP or HIO, they remain a family member of a domestic PEP or HIO until five years after the domestic PEP or HIO has left office.Footnote 10 In the case of a deceased domestic PEP or HIO, persons that are their family members remain a family member of a domestic PEP or HIO for five years after the domestic PEP or HIO ceases to be a domestic PEP or HIO. So, you must continue to mitigate the risks associated with the family members of domestic PEPs or HIOs during that time.

Is a PEP or HIO's ex-spouse or partner considered a family member?

An ex-spouse or partner may continue to have access to a PEP or HIO's funds even when a divorce has taken place or a relationship has ended. Therefore, in the case of:

- the ex-spouse or partner of a **foreign PEP**, they are considered a family member of a foreign PEP forever; and
- the ex-spouse or partner of a **domestic PEP or HIO**, they are considered a family member of a domestic PEP or HIO until the domestic PEP or HIO ceases to be a domestic PEP or HIO.

Is a PEP or HIO's stepchild or step-sibling considered a family member?

A step family relationship does not fall under the definition of a family member unless a child is legally adopted. For example, if Helen is a domestic PEP, and she has legally adopted her stepdaughter, then her stepdaughter is her child under the law and is considered to be the family member of a domestic PEP.

Similarly, if a marriage includes step-siblings, these step-siblings are not considered family members if they are not legally adopted by the stepparent. However, you may want to consider the step family members as close associates of the PEP or HIO, depending on their relationship.

Is the niece or nephew of a PEP or HIO considered a family member?

No. Only the family members of a PEP or HIO listed in this guidance must be regarded as family members of PEPs or HIOs. For example, if John is a PEP, then John's brother, Sam, is considered a family member of a PEP, however, Sam's daughter (John's niece) is not considered a family member of a PEP. However, you may want to consider extended family members as close associates of the PEP or HIO, depending on their relationship.

6. Who is considered a close associate of a PEP or a HIO?

A close associate can be a person who is connected to a PEP or HIO for personal or business reasons. Examples of relationships that could indicate that someone is a close associate (personal or business) could include, but are not limited to, persons who:

- are the business partners of, or who beneficially own or control a business with, a PEP or HIO;
- are in a romantic relationship with a PEP or HIO;
- are involved in financial transactions with a PEP or a HIO;
- serve as prominent members of the same political party or union as a PEP or HIO;
- serve as a member of the same board as a PEP or HIO;
- carry out charitable works closely with a PEP or HIO; or
- are listed as joint on a policy where one of the holders may be a PEP or HIO.

Once you determine that a person is the close associate of a PEP or HIO, they remain a close associate until they lose that connection.

7. What does it mean to "detect a fact" about a PEP or HIO?

Detecting a fact about a PEP or HIO is to discover (proactively or not) information about a person that could lead you to make a PEP or HIO determination or

to update information about a known PEP or HIO. You detect a fact when you discover PEP or HIO related information about a person that has an account-based business relationship **or** a non-account-based business relationship with you, outside of your periodic review of existing clients. The information that you detect must be a fact that constitutes **reasonable grounds to suspect** that a person is a PEP, HIO, or family member or close associate of a PEP or HIO.

There is no requirement for you to have proactive processes in place to detect facts about existing clients, but if you do detect information related to a PEP or HIO determination, then you must act on that information. For example, you might detect a fact that would require further action based on information obtained from an existing client, monitoring efforts you may already have in place, knowledge of domestic and world events, or a search run against an open source or third party database.

While a name match is a fact, it is not necessarily a fact that constitutes reasonable grounds to suspect that an existing client is a PEP, HIO, or family member or close associate of a PEP or HIO. As a best practice, you could apply additional criteria (for example, address, date of birth, age, transaction activities, etc.) to a name match, to meet the reasonable grounds to suspect threshold.

8. How do I establish the source of funds, source of virtual currency (VC), or source of a person's wealth?

Once you have determined that a person is a PEP, HIO, or a family member or close associate of a PEP or HIO (in certain circumstances, as applicable), you must take reasonable measures to establish the source of the funds or source of VC used for a transaction or that is expected to be deposited into an account, and the source of a person's wealth. To do this you could take measures such as:

- asking the person; or
- referring to open source information available about the person.

If a transaction or the account activity is inconsistent with the information you have about the source of funds or source of VC, or the source of the person's wealth, then you may want to follow up with the client for clarification. If the information remains inconsistent with what you know about the person, or you are not satisfied with their response and have reasonable grounds to suspect that a transaction or deposit is related to the commission or the attempted commission of an ML or TF offence, you must file a suspicious transaction report.

9. Who can review a transaction or allow an account to stay open?

A member of senior management must review transactions and allow certain accounts to stay open. A member of senior management is a person who has:

- the authority to make management decisions about transactions or accounts and is accountable for them;
- awareness of the ML or TF risks to which you are exposed; and
- awareness and understanding of your obligations related to PEPs, HIOs, and their family members and close associates.

If you are a sole proprietor with no employees, agents or other persons authorized to act on your behalf, you are considered to be the senior manager.

10. Should I treat a PEP or HIO as a high-risk client?

You must treat all persons that you determine to be **foreign PEPs** or **family members or close associates of foreign PEPs** as posing a high risk.

Persons that you determine to be **domestic PEPs**, **HIOs**, or **family members or close associates of domestic PEPs or HIOs** must, be treated as high-risk if you consider, based on your risk assessment, that there is a **high-risk** of an ML or TF offence being committed.

Once you determine that there is a high risk of an ML or TF offence being committed, you must take the measures prescribed in the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations. These measures should be detailed in your written compliance policies and procedures for high-risk clients. For more information about risk assessment considerations for PEPs or HIOs see FINTRAC's Risk assessment guidance.

Methods to verify the identity of persons and entities

From: Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)

Overview

This guidance came into effect on June 1, 2021.

This guidance explains the methods that can be used by reporting entities (REs) to verify the identity of a person or an entity.

Note: For specific information on when to verify the identity of a person or an entity (the timing requirement) for your business sector, refer to the related guidance by business sectors.

Who is this guidance for

The requirement to verify the identity of a person or an entity under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and associated Regulations applies to all reporting entities

1. Meaning of verifying the identity of a person or an entity

It means to use the methods described in this guidance to ensure that the information in an identification document or from other informational sources matches the information that the person or entity provided.

Verifying identity is a foundational element of Canada's anti-money laundering and anti-terrorist financing regime and a key component of an RE's relationship with clients. It helps you to know your clients and to understand and assess any risk that may be associated to their transactions or activities.

2. How to verify the identity of a person

You can use any of the 5 methods described below to identify a person:

1. 2.1 Government-issued photo identification method
2. 2.2 Credit file method
3. 2.3 Dual-process method
4. 2.4 Affiliate or member method
5. 2.5 Reliance method

2.1 Government-issued photo identification method

You may verify the identity of a person by referring to a government-issued photo identification document.Footnote 1 To do so, the document must:

- be **authentic**, **valid and current**;Footnote 2
- be issued by a federal, provincial or territorial government (or by a foreign government if it is equivalent to a Canadian document);
- indicate the person's name;
- include a photo of the person;
- include a unique identifying number; and
- match the name and appearance of the person being identified.

Photo identification documents issued by municipal governments, Canadian or foreign, are not acceptable. See Annex 4 for examples of acceptable government-issued photo identification documents.

You can determine whether a government-issued photo identification document is **authentic, valid and current** by viewing it **in person**, and by looking at the characteristics of the original physical document and its security features (or markers, as applicable) **in the presence of the person being identified**. This will allow you to be satisfied that the identification document is authentic,

as issued by the competent authority (federal, provincial, or territorial government), valid (unaltered, not counterfeit) and current (not expired).

Using the government-issued photo identification method if a person is not physically present You may use the government-issued photo identification method if a person is **not physically present**, but you must have a **process in place to authenticate** the government-issued photo identification document. For instance, you could assess a document by using a technology capable of determining the document's authenticity. For example, you could:

- ask a person to scan their government-issued photo identification document using the camera on their mobile phone or electronic device; and
- use a technology to compare the features of the government-issued photo identification document against known characteristics (for example, size, texture, character spacing, raised lettering, format, design), security features (for example, holograms, barcodes, magnetic strips, watermarks, embedded electronic chips) or markers (for example, logos, symbols) to be satisfied that it is an authentic document as issued by the competent authority (federal, provincial, or territorial government).

When a person **is not physically present,** you must still determine whether the authenticated government-issued photo identification document is **valid** and **current,** and that the name and photo are those of the person providing the document. For example, you could:

- participate in a live video chat session with the person and compare the name and the features of the live video image to the name and photo on the authentic government-issued photo identification document; or
- ask the person to take a "selfie" photo using the camera on their mobile phone or electronic device, and use an application to apply facial recognition technology to compare the features of that "selfie" to the photo on the authentic government-issued photo identification document. You would also need a process to compare the name on the government-issued photo identification document with the name provided by the person.

Note: It is not enough to only view a person and their government-issued photo identification document through a video conference or another type of virtual application.

Your compliance program's policies and procedures must describe the processes you follow to determine whether a government-issued photo identification document is authentic, whether the client is present or not, and how you will confirm that it is valid and current. Your policies and procedures must also describe the steps you use to confirm that the name and photograph are those of the person. Your processes to determine that a government-issued photo identification document is authentic, valid, and current, **and** the verification step (ensuring that the name and photo match the name and appearance of the person), do **not**

need to happen at the same time. It is up to you to determine the timing, but you must complete both steps.

Record keeping requirements for the government-issued photo identification method If you use the government-issued photo identification method, you must record:Footnote 3

- the person's name;
- the date on which you verified the person's identity;
- the type of document used (for example, driver's licence, passport, etc.);
- the unique identifying number of the document used;
- the jurisdiction (province or state) and country of issue of the document; and
- the expiry date of the document, if available (if this information appears on the document or card, you must record it).

2.2 Credit file method

You may verify the identity of a person by referring to information that is in their credit file.Footnote 4 To do so, the credit file must:

- contain information that is **valid and current**;Footnote 5
- be from a Canadian credit bureau (credit files from foreign credit bureaus are not acceptable);
- have been in existence for at least three years;
- contain information that is derived from more than one source (i.e. more than one tradeline); and
- match the name, address and date of birth of the person being identified.

A credit file provides a rating on a person's ability to repay loans; however, it is possible to request a credit file to verify a person's identifying information that does not include a credit assessment. You do not need a credit assessment to verify the identity of a person. Equifax Canada and TransUnion Canada are Canadian credit bureaus that provide credit file information for identification purposes.

To use the credit file method, you must conduct the search **at the time** you are verifying the person's identity. A person cannot provide you with a copy of their credit file, nor can a previously obtained credit file be used.

It is acceptable to use an automated system to match the person's information with the information in the person's credit file. You may also refer to a third party vendor to provide you with valid and current information from the person's credit file. A third party vendor is a business that is authorized by a Canadian credit bureau to provide access to Canadian credit information.

If any of the information provided by the person (name, address or date of birth) does not match the information in the credit file, you cannot use that credit file to verify the identity of the person. You will need to use another credit file

from a different provider (credit bureau or third party vendor) or use a different method (for example, the government-issued photo identification method or the dual-process method) to verify the person's identity.

On occasion, information found in the credit file may contain a variation on the name or a discrepancy in the address that was provided to you by the person. In these instances, you must determine whether the information in the credit file matches the information provided by the person. For example:

- If there is a slight typo in the address or name, you may determine that the information still matches what the person provided.
- If there is a discrepancy in their date of birth, it is more likely that you will determine that the information does not match.
  - In this case, if this is your determination, you cannot rely on the information in the credit file for identification purposes. You will need to use another credit file from a different provider (credit bureau or third party vendor) or use a different method (for example, the government-issued photo identification method or the dual-process method) to verify the person's identity.
- If there are multiple addresses in the credit file, it is possible that the address the person provided to you is not the primary address in the credit file but it does appear in the credit file as a secondary address. If this is the case, you can still meet your requirements for ensuring that the information matches what the person provided.

Record keeping requirements for the credit file method If you use the credit file method, you must record:Footnote 6

- the person's name;
- the date you consulted or searched the credit file;
- the name of the Canadian credit bureau or third party vendor as the source holding the credit file; and
- the person's credit file number.

Your compliance program's policies and procedures must describe the processes you will follow to verify a person's identity using the credit file method **and** how you will ensure that the information is valid and current. It should also include the steps you will take if the information is not valid and current (for example, search a different credit file, use another method, stop the transaction, etc.).

2.3 Dual-process method

You may verify the identity of a person by using the dual-process method, which consists of doing any **two** of the following:Footnote 7

- referring to information from a reliable source that includes the **person's name and address** and confirming that the name and address are those of the person;

- referring to information from a reliable source that includes the person's **name and date of birth**, and confirming that the name and date of birth are those of the person; or
- referring to information that includes the person's **name and confirms that they have a deposit account, a prepaid payment product account , or a credit card or other loan account with a financial entity**, and confirming that information.

The information you refer to **must** be valid and currentFootnote 8 **and** come from two different reliable sources. This information could be found in **statements, letters, certificates, forms or other information sources** that can be provided through an original version or by another version of the information's original format such as a fax, a photocopy, a scan, or an electronic image. For example, you can rely on a fax, photocopy, scan or electronic image of a government-issued photo identification document as one of the two pieces of information required to verify a person's identity.

You **cannot** use the same source for the two categories of information you choose to verify a person's identity.Footnote 9 For example, you cannot rely on a bank statement from Bank A that includes the person's name and address and another bank statement from Bank A that includes the person's name and confirms that the person holds a deposit account, as Bank A would be the same source of both categories of information. You can, however, refer to a bank statement from Bank A that contains the person's name and confirms that the person holds a deposit account, and rely on an electronic image of a driver's licence to confirm the person's name and address.

For further precision, the possible combinations for this method include:

Referring to information from one reliable source that includes the person's **name** and **address** and confirming that this matches the information provided by the person, **and** referring to information from a different reliable source that includes the person's **name** and **date of birth** and confirming that this matches the information provided by the person.

OR

Referring to information from one reliable source that includes the person's **name** and **address** and confirming that this matches the information provided by the person, **and** referring to information from a different reliable source that includes the person's **name** and a **financial account**(specifically, a deposit account, a prepaid payment product account, a credit card account or a loan account) and confirming this information.

OR

Referring to information from one reliable source that includes the person's **name** and **date of birth** and confirming that this matches the information provided by the person, **and** referring to information from a different reliable source that includes the person's **name** and a **financial account**(specifically,

a deposit account, a prepaid payment product account, a credit card account or a loan account) and confirming this information.

Note: If the information does not match the information provided by the person, you cannot rely on it. For example, it is **not acceptable** to rely on information if the account number or number that is associated with the information is truncated or redacted. On occasion, information from a source may contain a variation on the name of the client or a typo in the client's address. In these instances, you must determine whether the information matches the information provided by the person. If it is a slight typo in the address or a misspelled name, you may determine that the information still matches what the person provided. However, in the case of an incorrect date of birth, it is more likely that you will determine that the information does not match. In this case, you cannot rely on the information from this source for identification purposes. You must obtain information from a different source under the dual-process method or use a different method (for example, the government-issued photo identification method or the credit file method) to verify the person's identity.

Reliable source of information A reliable source of information is an originator or issuer of information that you trust. To be considered reliable, the source should be well known and considered reputable. For example, a reliable source could be the federal, provincial, territorial or municipal levels of government, Crown corporations, federally regulated financial institutions, or utility providers. Social media is **not** an acceptable source of information to verify a person's identity. Also, the source **cannot** be the person whose identity is being verified, nor you, the RE who is verifying identity.Footnote 10 See Annex 5 for a table of examples of reliable sources of information for the dual-process method.

How to use a credit file under the dual-process method A Canadian credit file can be used as one of the two pieces of information required to verify the identity of a person under the dual-process method. Specifically, it can be used to confirm the person's name and address, name and date of birth, or to confirm the person's name and confirm that the person has a credit card account or a loan account. If you use a credit file as one of the information pieces for the dual-process method, it must have existed for at least six months.Footnote 11

Information from a second source, for example, a property tax assessment, must be used to confirm the second category of information. In this instance, the two reliable sources are the Canadian credit bureau that provided the credit file information and the municipal government that issued the property tax assessment. The information from these two sources must match the information provided by the person.

You can also refer to information from a Canadian credit bureau if it acts as an aggregator that compiles information from different reliable sources (often

referred to as tradelines). In this instance, the Canadian credit bureau must provide you with information from **two** independent tradelines where each tradeline confirms one of the two categories of information required to verify the identity of a person under this method. In this instance, **each tradeline is a distinct source; the credit bureau is not the source**.

The tradelines cannot be your own, as the RE verifying the person's identity, and each tradeline must originate from a different reliable source (for example, a federally regulated financial institution, a utility service provider, etc.).

Record keeping requirements for the dual-process method If you use the dual-process method to verify a person's identity, you must record:Footnote 12

- the person's name;
- the date you verified the information;
- the name of the two different reliable sources that were used to verify the identity of the person;
- the type of information referred to (for example, a utility statement, a bank statement, a marriage licence); and
- the number associated with the information (for example, account number or if there is no account number, a number that is associated with the information, which could be a reference number or certificate number, etc.). If you use information aggregated by a Canadian credit bureau and receive information from two distinct sources (tradelines), you must record the account number or number associated to each tradeline, not the aggregator (credit bureau) number.

Your compliance program's policies and procedures must describe the processes you follow when using the dual-process method to verify a person's identity and how you will ensure that the information is valid and current.

2.4 Affiliate or member method

You may verify the identity of a person by confirming that one of the following entities previously verified the person's identity:

- an **affiliate** of yours that is an RE referred to in any of paragraphs 5(a) to (g) of the PCMLTFA;Footnote 13
- a **foreign affiliate** of yours that carries out activities outside of Canada that are similar to the activities of an RE referred to in any of paragraphs 5(a) to (g) of the PCMLTFA;Footnote 14 **or**
- a financial entity that is subject to the PCMLTFA and isa **member** of yourfinancial services cooperative or credit union central.Footnote 15

You must confirm that the name, address, and date of birth in the affiliate or member's records match the information provided by the person whose identity is being verified.Footnote 16

The affiliate or member must have previously verified the person's identity by using the government-issued photo identification method, the credit file method or the dual-process method presented in this Guidance. If the affiliate or member verified the identity of the person prior to June 1, 2021, they must have done so in accordance with the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFR), by using the methods that were in place **at the time**.Footnote 17

If you have any concerns about the methods or information that the affiliate or member used to verify the person's identity, you should re-verify their identity,Footnote 18 as you have the responsibility for ensuring the person's identity has been verified.

Note: Financial services cooperatives or credit union centrals act on behalf of a membership composed of certain financial entities and can provide financial services to that group.

Record keeping requirements for the affiliate or member method
When you verify the identity of a person by confirming that an **affiliate** or a financial entity that is a **member** of **your** financial services cooperative or credit union central previously verified their identity, you must record:Footnote 19

- the person's name;
- the date on which you verified the identity of the person;
- the name of the affiliate or the member that previously verified the person's identity;
- the method (government-issued photo identification, credit file or dual-process) that the affiliate or the member used to verify the person's identity; and
- the information that the affiliate or the member recorded based on the method used (this includes the name of the person, the date the affiliate or member verified identity, and all the other information required to be kept by them for the method used).

Note: If the affiliate or the member verified the identity of the person in accordance with the methods that were in place prior to June 1, 2021, you must still record the information listed above, but include the method they used in accordance with the PCMLTFR as it read at the time, and the information that was required to be recorded for that method.Footnote 20

Your compliance program's policies and procedures must describe the processes you follow when using the affiliate or member method to verify a person's identity.

2.5 Reliance method

You may verify the identity of a person by relying on measures that were previously taken by:

- **another RE**(person or entity that is referred to in section 5 of the PCMLTFA);Footnote 21 **or**
- an entity that is affiliated with you or with another RE **and** carries out activities outside of Canada that are similar to those of a person or entity referred to in any of paragraphs 5(a) to (g) of the PCMLTFA(an **affiliated foreign entity**).Footnote 22

To rely on measures previously taken by an **affiliated foreign entity**, you must be satisfied, after considering the risk of a money laundering or terrorist activity financing offence in the foreign state in which it carries out its activities, that:Footnote 23

- the **affiliated foreign entity** has policies in place similar to the record keeping, verifying identity, and compliance program requirements under the PCMLTFA, including the requirement to develop and apply policies to assess, in the course of their activities, the risk of a money laundering offence or a terrorist activity financing offence, and the requirement to take enhanced measures where the risk has been identified as high; **and**
- the **affiliated foreign entity's** compliance with those policies is subject to the supervision of a competent authority under the legislation of that foreign state.

To rely on measures previously taken by **another RE** or an **affiliated foreign entity** to verify the identity of a person, you must:Footnote 24

- as soon as feasible, obtain from the **other RE** or **affiliated foreign entity** the information that was confirmed as being that of the person, and be satisfied that:
  - the information is valid and current; and
  - the **other RE** or **affiliated foreign entity** verified the person's identity using the government-issued photo identification method, the credit file method or the dual-process method, or if the **other RE** or **affiliated foreign entity** verified the person's identity prior to June 1, 2021, that they did so in accordance with the PCMLTFR, by using the methods that were in place at the time; **and**
- have a written agreement or arrangement with the **other RE** or **affiliated foreign entity** that upon request requires them to provide you, as soon as feasible, with all of the information that they referred to in order to verify the person's identity.

Record keeping requirements for the reliance method If you rely on **another RE** or an **affiliated foreign entity** to verify the identity of a person,

you must keep a record of:Footnote 25

- the person's name;
- the written agreement or arrangement with the **other RE** or **affiliated foreign entity** for the purpose of verifying a person's identity; and
- the information that the **other RE** or **affiliated foreign entity** referred to in order to verify the identity the person.

Your compliance program's policies and procedures must describe the processes you follow when using the reliance method to verify a person's identity and how you will ensure that the information is valid and current.

3. Using an agent or a mandatary to verify the identity of a person on your behalf

You may verify the identity of a person by using an agent or mandatary to carry out the verification on your behalf, in accordance with the government-issued photo identification method, the credit file method, or the dual-process method.Footnote 26

You may rely on the measures that were previously taken by an agent or mandatary to verify the person's identity, if the agent or mandatary was:Footnote 27

- acting in their own capacity at the time, whether or not they were required to use the methods in accordance with the PCMLTFR; or
- acting as an agent or mandatary under a written agreement or arrangement that was entered into with another RE, for the purposes of verifying a person's identity using either the government-issued photo identification method, the credit file method or the dual-process method, or if the measures were taken prior to June 1, 2021, using the methods in accordance with the PCMLTFR that were in place at the time.

To use an agent or mandatary to verify the identity of a person you must:Footnote 28

- have a written agreement or arrangement in place with the agent or mandatary **before** you use them;Footnote 29
- obtain, as soon as feasible, all of the information that the agent or mandatary referred to in order to verify the person's identity, and the information that the agent or mandatory confirmed as being that of the person;Footnote 30 and
- be satisfied that:
  - the information that the agent or mandatary confirmed as being that of the person is valid and current, and
  - the person's identity was verified using the government-issued photo identification method, the credit file method or the dual-process method, or, if the person's identity was verified prior to June 1, 2021,

using the methods in accordance with the PCMLTFR in place at the time.Footnote 31

Example 1 — Acceptable

Jane Smith would like to open an account with you. Your agent—with whom you have a written agreement for this purpose—verified Jane Smith's identity in 2019 using the government-issued photo identification method, by referring to her driver's licence, which expired in February 2021. In 2019, Jane Smith's name and appearance matched the name and photograph on the driver's licence, and the document was determined to be authentic, valid and current, therefore, her identity was verified by the agent in accordance with the method. Jane's name and appearance have not changed. When you obtain the information from the agent, you are satisfied that the information the agent confirmed as being Jane's (her name and photo) is still valid and current and is therefore acceptable. It does not matter that her licence (the identification document used by the agent) has expired, as it is the information that you must be satisfied is valid and current, not the document.

Example 2 — Not acceptable

Jane Smith (maiden name — Jane Rogers) would like to carry out a transaction for which you must verify her identity. Your agent—with whom you have a written agreement for this purpose—verified Jane Rogers' identity in 2019 using the government-issued photo identification method, by referring to her driver's licence, which has not yet expired. In 2019, **Jane Rogers'** name and appearance matched the name and photograph on the driver's licence, and the document was determined to be authentic, valid and current, therefore, her identity was verified by the agent in accordance with the method. However, although the licence has not yet expired, it is not acceptable to rely on the information from the agent now because the agent's information is about Jane Rogers, and this does not match the name of your client who is now Jane Smith, so the information provided by the agent is not valid and current.

Example 3 — Not acceptable

Jane Smith would like to carry out a transaction for which you must verify her identity. Your agent—with whom you have a written agreement for this purpose—verified Jane Smith's identity in 2019 by referring to her driver's licence, which expired in 2018. In 2019, because **Jane Smith's** driver's licence had expired, her identity **was not** verified in accordance with the government-issued photo identification method. As such, it is not acceptable to rely on the information from the agent.

Record keeping requirements when using an agent or a mandatary
When you verify the identity of a person by using an agent or mandatary, you must keep a record of:Footnote 32

- the person's name;

- the written agreement or arrangement with the agent or mandatary for verifying a person's identity; and
- all of the information the agent or mandatary referred to in order to verify the identity of the person, and the information that the agent or mandatary confirmed as being that of the person (this includes, as applicable, information that is required to be kept in the record for the method used).

Note: As an RE it is your responsibility to meet your client identification requirements under the PCMLTFA and associated Regulations, even when you use an agent or mandatary to verify the identity of a person on your behalf, or when you rely on the measures previously taken by an agent or mandatary to verify a person's identity.

For example, if your agent verifies the identity of a person using the government-issued photo identification method but they don't refer to an authentic, valid and current photo identification document issued by a federal, provincial or territorial government, or keep the required records after verifying the person's identity, you are still responsible. Specifically, it is your responsibility to ensure that the agent is verifying client identity and keeping the required records in accordance with the PCMLTFA and associated Regulations.

Your compliance program's policies and procedures must describe the processes you follow when you rely on an agent or mandatary to verify a person's identity and how you will ensure that the information is valid and current.

4. Verifying a person's identity if it has been previously verified

You do **not** need to verify a person's identity for subsequent transactions or activities, as required, **if** you have already verified the identity of the person using:Footnote 33

- one of the methods explained in this guidance; or
- the methods specified in the PCMLTFR prior to June 1, 2021 as it read at the time, and have kept the required record.

You must not have doubts about the information that was previously used to verify the person's identity. If you have doubts, you must verify their identity again using the methods explained in this guidance.Footnote 34

Note: In the context of a business merger or acquisition, you are not required to re-identify the acquired clients if their identities were verified in accordance with the methods in the PCMLTFR at the time the verification took place. As a best practice, you are encouraged to review and update client information (for example, name, address, occupation, etc.), in accordance with your risk assessment process. The acquired clients become the responsibility of the acquiring entity which must ensure compliance with the PCMLTFA and associated Regulations. This includes reviewing any money laundering or terrorist financing risks that may be associated with these clients.

5. How to identify a child

If a child is under 12 years of age, you must verify the identity of one parent, guardian or tutor **and** record the parent, guardian or tutor's information.Footnote 35 You can rely on the information provided by the parent, guardian or tutor in order to record the child's identification details.

If a child is between 12 and 15 years of age, you can verify their identity by using any of the methods. If this is not possible due to a lack of identification information, you may use a variation of the dual-process method that allows you to:

- Refer to one reliable source of information that includes the name and address of the child's parent, guardian, or tutor;Footnote 36 and
- Refer to a second reliable source that includes the child's name and date of birth.

For example, if the child has a passport you may be able to use it to verify their identity under the government-issued photo identification method. If not, you could rely on the parent's driver's licence to verify the parent's name and their common address, and the child's birth certificate to verify the child's name and date of birth.

6. How to verify the identity of a person who does not have any identity verification documentation or information for a retail deposit account Added on February 22, 2023

In the case of opening a retail deposit account, if a bank cannot verify a person's identity in accordance with one of the methods outlined above, they would still be in compliance with their anti-money laudering/anti-terrorist financing obligations if they opened the account in a way that meets the conditions set out in subsections 627.17(1) and (3) of the Bank Act.

Note: The Bank Act applies to banks, authorized foreign banks and federal credit unions, which are defined as banks under the Act.

For reasons beyond a person's control, they may face barriers in meeting requirements where they must provide proper identification documentation or information. This may be the case for vulnerable populations with barriers to obtaining proper identification such as survivors of human trafficking or victims of domestic abuse.

In specific circumstances, where a person does not have the proper identification documentation or information, a bank must:

- follow the measures as defined by the Bank Act and any bulletins published by the Financial Consumer Agency of Canada that further define the measures to be taken

- document in their compliance policies and procedures the types of circumstances where their organization would follow the Bank Act for verification of identification
- ensure that the banking products provided to the individual opening the account are limited to a basic retail deposit account until which time the account holder returns with the proper form of identification as specified in paragraphs 105(1)(a) to (e) of the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations
- verify the person's identity using the appropriate form of identification as specified in paragraphs 105(1)(a) to (e) of the Regulations, within 6 to 12 months, or as described in their risk-based approach and keep appropriate records
- continue to follow their customer due diligence and "know your client" processes, ensure ongoing monitoring activities are conducted as per the bank's risk assessment of the client and monitor transactions to ensure that the financial activity and use of associated products/services aligns with what is known about the person.

Note: The risk-based approach must reflect what is known about the client (i.e., their profile and individual circumstances including the fact that alternate identification was accepted), and that ongoing monitoring should then be commensurate to the risk profile of the client.

When FINTRAC undertakes compliance activities to ensure reporting entities are meeting their obligations, and observes that this process is used, we will:

- verify that you have documented policies and procedures that articulate the steps your organization takes to ensure that they are meeting this requirement
- ensure that the procedures are also followed in practice
- verify that your risk assessment takes into account these circumstances, ensures that these individuals are identified within a reasonable timeframe (i.e., 6 to 12 months) and that you are able to demonstrate that you are fulfilling these requirements.

7. How to verify the identity of an entity

You can use any of the 3 methods described below to verify the identity of an entity:

1. 7.1 Confirmation of existing method
2. 7.2 Reliance method
3. 7.3 Simplified identification method

While an entity can be a corporation, a trust, a partnership, a fund, or an unincorporated association or organization, corporations are subject to different requirements than other entities (as explained below).

7.1 Confirmation of existence method

Corporation To verify the identity of **a corporation**, you may refer to:Footnote 37

- a certificate of incorporation;
- a record that has to be filed annually under provincial securities legislation; **or**
- the most recent version of any other record that confirms the corporation's existence and contains its name and address and the names of its directors, such as a certificate of active corporate status, the corporation's published annual report signed by an audit firm, or a letter or notice of assessment for the corporation from a municipal, provincial, territorial or federal government.

The record you refer to must be authentic, valid and current.Footnote 38

You may obtain a corporation's name and address and the names of its directors from a publicly accessible database, such as a provincial or federal database like the Corporations Canada database, or a corporation search and registration service through subscription.

When a corporation is a securities dealer, you do not need to confirm the names of its directors when you confirm its existence.Footnote 39

Entity To verify the identity of an **entity other than a corporation,** you may refer to:Footnote 40

- a partnership agreement;
- articles of association; **or**
- the most recent version of any other record that confirms its existence and contains its name and address.

The record you refer to must be authentic, valid and current.Footnote 41

Record keeping requirements when verifying the identity of a corporation or other entity If you refer to a paper record or an electronic version of a record, you must keep the record or a copy of it.

If the electronic version of the record that you refer to is contained in a database that is accessible to the public, you must keep a record that includes the corporation or other entity's registration number, the type of record referred to and the source of the electronic version of the record.Footnote 42

Your compliance program's policies and procedures must describe the processes you follow when using the confirmation of existence method to verify the identity of corporations and other entities, and how you will ensure that the information is authentic, valid and current.

7.2 Reliance method

You may verify the identity of a **corporation** or other **entity** by relying on the measures that were previously taken by:

- another **RE**(a person or entity that is referred to in section 5 of the PCMLTFA);Footnote 43 **or**
- an entity that is affiliated with you **or** with another RE **and** carries out activities outside of Canada that are similar to those of a person or entity referred to in any of paragraphs 5(a) to (g) of the PCMLTFA (an **affiliated foreign entity**).Footnote 44

Measures previously taken by an affiliated foreign entity To rely on measures previously taken by an **affiliated foreign entity**, you must be satisfied, after considering the risk of a money laundering or terrorist activity financing offence in the foreign state in which it carries out its activities, that:Footnote 45

- the **affiliated foreign entity** has policies in place similar to the record keeping, verifying identity, and compliance program requirements under the PCMLTFA, including the requirement to develop and apply policies to assess, in the course of their activities, the risk of a money laundering offence or a terrorist activity financing offence, and the requirement to take enhanced measures where the risk has been identified as high; **and**
- the **affiliated foreign entity's** compliance with those policies is subject to the supervision of a competent authority under the legislation of that foreign state.

Measures previously taken by another reporting entity or an affiliated foreign entity To rely on the measures previously taken by **another RE** or an **affiliated foreign entity** to verify the identity of a corporation or other entity, you must:Footnote 46

- as soon as feasible, obtain from the **other RE** or **affiliated foreign entity** the information that was used to confirm the identity of the corporation or other entity, as the case may be, and be satisfied that:
  - the information is valid and current; and
  - **for a corporation**, its identity was verified by the **other RE** or **affiliated foreign entity** by referring to a record as described in the confirmation of existence method above, **or** if the measures to verify the corporation's identity were performed prior to June 1, 2021, that the **other RE** or **affiliated foreign entity** confirmed the corporation's existence and ascertained its name, address, and the names of its directors in accordance with the methods in the PCMLTFR as they read at that time;Footnote 47 and
  - **for an entity other than a corporation**, its identity was verified by the **other RE** or **affiliated foreign entity** by referring to a

record as described in the confirmation of existence method above, **or** if the measures to verify the entity's identity were performed prior to June 1, 2021, the **other RE** or **affiliated foreign entity** confirmed the entity's existence in accordance with the methods in the PCMLTFR as they read at that time;Footnote 48 **and**

- have a written agreement or arrangement in place with the **other RE** or **affiliated foreign entity** that upon request requires them to provide you, as soon as feasible, with all of the information that they referred to in order to verify the identity of the **corporation** or other **entity,** as the case may be.Footnote 49

Your compliance program's policies and procedures must describe the processes you will follow when using the reliance method to verify the identity of corporations and other entities and how you will ensure that the information is valid and current.

7.3 Simplified identification method

If you are an **RE** that isreferred to in any of paragraphs 5(a) to (g) of the PCMLTFA, you may use the simplified identification method to meet your obligation to verify the identity of a **corporation** or other **entity**. Specifically, you are deemed to comply with your requirement to verify the identity of a **corporation** or other **entity** if, based on your risk assessment, you consider there is a low risk of a money laundering offence or terrorist activity financing offence, **and** if:Footnote 50

- the **corporation** or other **entity** whose identity is being verified:
    1. is referred to in any of paragraphs 5(a) to (g) of the PCMLTFA;
    2. is a foreign corporation or entity that carries out activities that are similar to those of an entity referred to in any of paragraph 5(a) to (g) of the PCMLTFA;
    3. administers a pension or investment fund that is regulated under the legislation of a foreign state and that either is created by a foreign government or is subject to the supervision of a competent authority under the legislation of that foreign state;
    4. is one whose shares are traded on a Canadian stock exchange or a stock exchange designated under subsection 262(1) of the Income Tax Act;
    5. is a subsidiary of a **corporation** or an **entity** that is referred to in paragraphs a. to d. in this section, and is one whose financial statements are consolidated with the financial statements of that corporation or entity;
    6. is an institution or agency of, or in the case of a corporation, is owned by, the government of a foreign state; **or**
    7. is a public service body, as defined in subsection 123(1) of the Excise Tax Act; **and**

- you are satisfied that, within the applicable time period for which you had to verify identity, as explained in the sector-specific guidance on When to verify the identity of persons and entities, the corporation or other entity exists **and** that every person who deals with you on behalf of the corporation or other entity is authorized by it to do so.

If you subsequently consider, based on your risk assessment, that the risk of a money laundering offence or terrorist activity financing offence has increased and is no longer low then you **must**, as soon as feasible, verify the identity of the corporation or other entity, as the case may be, by referring to the appropriate records, as explained in **section 7.1, Confirmation of existence method**.

Record keeping requirements for the simplified identification method
If you use the simplified identification method to verify the identity of a corporation or other entity, you must keep a record that sets out:

- the grounds for considering there is a low risk of a money laundering offence or terrorist activity financing offence; and
- the information obtained about the corporation or other entity, as the case may be, and about the persons that assure you that the corporation or other entity exists and that the persons you deal with are authorized to act on behalf of the corporation or the entity.Footnote 52

Your compliance program's policies and procedures must describe the processes you follow when using the simplified identification method to verify the identity of corporations and other entities.

8. Verifying the identity of an entity if it has been previously verified

You do **not** need to verifythe identity of a corporation or other entity for subsequent transactions or activities, as required, if you have already verified their identity by using:

- One of the methods explained in this guidance; or
- in the case of an **entity**, you confirmed the entity's existence in accordance with the PCMLTFR, and you complied with the related record keeping provisions, as they read at the time prior to June 1, 2021; **or**
- in the case of a **corporation**, you confirmed the corporation's existence and ascertained its name and address and the names of its directors in accordance with PCMLTFR, and you complied with the related record keeping provisions, as they read at the time prior to June 1, 2021

You must not have doubts about the information that was previously used to verify the identity of the corporation or other entity. If you have doubts, you must verify identity again using the methods explained in this guidance.Footnote 54

9. Restrictions on the use of personal information

The use of personal information in Canadian commercial activities is protected by the Personal Information Protection and Electronic Documents Act (PIPEDA), or by similar provincial legislation. You have to inform clients about the collection of their personal information. However, you do not have to inform them when you include their personal information in the reports you are required to submit to FINTRAC.

The Office of the Privacy Commissioner of Canada can provide further guidance, and has created a Question and Answer document about PIPEDA and the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, to help clarify your responsibilities under PIPEDA.

Beneficial ownership requirements

Overview

This guidance came into force on June 1, 2021.

Beneficial ownership requirements under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and associated Regulations apply to all reporting entities (REs).

The concealment of beneficial ownership information is a technique used in money laundering and terrorist activity financing schemes. Identifying beneficial ownership removes the anonymity of the individuals behind the transactions and account activities, which is a key component of Canada's anti-money laundering and anti-terrorist financing regime. By collecting beneficial ownership information and confirming its accuracy, REs are performing an important step to mitigate the risk of money laundering and terrorist activity financing, and ultimately, to protect the integrity of Canada's financial system.

1. Who are beneficial owners?

Beneficial owners are the individuals who directly or indirectly own or control 25% or more of a corporation or an entity other than a corporation. In the case of a trust, they are the trustees, the known beneficiaries and the settlors of the trust. If the trust is a widely held trust or a publicly traded trust, they are the trustees and all persons who own or control, directly or indirectly, 25% or more of the units of the trust.

Beneficial owners cannot be other corporations, trusts or other entities. They must be the individuals who are the owners or controllers of the entity. It is important to consider and review the names found on official documentation in order to confirm the accuracy of the beneficial ownership information. It may be necessary to search through many layers of information in order to confirm

who are the beneficial owners, as the names found on official documentation may not always reflect the actual beneficial owners.

2. When must I obtain beneficial ownership information?

You must obtain beneficial ownership information when you verify the identity of an entity in accordance with the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFR).Footnote 2 For more information about when you are required to verify the identity of entities, see your sector's guidance on When to identify persons and entities.

The beneficial ownership information that you must obtain varies depending on whether the entity is a corporation, an entity other than a corporation (such as a partnership), a trust, or a widely held or publicly traded trust. The specific beneficial ownership information that you must obtain for each type of entity is detailed in section " 5. What beneficial ownership information do I need to obtain and confirm the accuracy of?".

3. When must I confirm the accuracy of beneficial ownership information?

You must take reasonable measures to confirm the accuracy of the beneficial ownership information when you first obtain it **and** in the course of conducting ongoing monitoring of your business relationships.

4. Are there circumstances where I do not have to obtain beneficial ownership information and confirm its accuracy?

You do not have to obtain beneficial ownership information and take reasonable measures to confirm its accuracy in the following situations:

1. For a group plan account held within a dividend or a distribution reinvestment plan. This includes plans that permits purchases of additional shares or units by the member with contributions other than the dividends or distributions paid by the plan sponsor, if the sponsor is an entity:
   - whose shares or units are traded on a Canadian stock exchange; and
   - that operates in a country that is a member of the Financial Action Task Force.
2. If you are a **financial entity**, beneficial ownership requirements do not apply to your activities in respect of the processing of payments by credit card or prepaid payment product for a merchant.Footnote 5
3. If you are a **life insurance company, broker or agent**, and you deal in reinsurance, beneficial ownership requirements do not apply to you for those dealings.Footnote 6

All RE sectors

The beneficial ownership requirements do not apply if you are not required to verify the identity of an entity under the Regulations because of a related exception. This is because your obligation to verify identity for a particular transaction, activity, or client does not apply in that circumstance.

5. What beneficial ownership information do I need to obtain and confirm the accuracy of?

When you verify an entity's identity in accordance with the PCMLTFR, you **must obtain** the following information about beneficial owners:Footnote 7

Corporations

- the names of all directors of the corporation and the names and addresses of all persons who directly or indirectly own or control 25% or more of the shares of the corporation.

Trusts

- the names and addresses of all trustees and all known beneficiaries and settlors of the trust.

Widely held or publicly traded trusts

- the names of all trustees of the trust and the names and addresses of all persons who directly or indirectly own or control 25% or more of the units of the trust.

Entities other than corporations or trusts

- the names and addresses of all persons who directly or indirectly own or control 25% or more of the entity.

In all cases, you must obtain information establishing the ownership, control and structure of the entity.Footnote 8

You **must also take reasonable measures to confirm** the accuracy of the information when you first obtain it and in the course of the ongoing monitoring of your business relationships.Footnote 9

If you verify the identity of a **not-for-profit organization**, you must also determine if the entity is:Footnote 10

- a charity registered with the Canada Revenue Agency under the Income Tax Act; or
- an organization, other than one referred to above, that solicits charitable donations from the public.

6. How do I obtain the required beneficial ownership information?

To obtain beneficial ownership information, which includes information on the ownership, control and structure, you could have the entity provide it, either verbally or in writing, or you could search for publicly available information.

For example:

- the entity can provide you with official documentation;
- the entity can tell you the beneficial ownership information and you can write it down for record keeping purposes; or
- the entity can fill out a document to provide you with the information.

7. How do I confirm the accuracy of beneficial ownership information?

You must take reasonable measures to confirm the accuracy of the beneficial ownership information that you obtain.Footnote 11 These reasonable measures cannot be the same as the measures you used to obtain the information.

Your reasonable measures could include referring to official documentation or records. For example, for a corporation or other entity, you could refer to records such as, but not limited to, the:

- minute book;
- securities register;
- shareholders register;
- articles of incorporation;
- annual returns;
- certificate of corporate status;
- shareholder agreements;
- partnership agreements; or
- board of directors' meeting records of decisions.

It is also acceptable to have a client sign a document to confirm the accuracy of the beneficial ownership information you obtained, which includes information on ownership, control and structure. In this case, it is possible for one document to be used to satisfy the two steps—namely to obtain the information and to confirm its accuracy by means of the signature.

In the case of a trust, you could confirm the accuracy of the information by reviewing the trust deed, which should provide you with the information needed.

Other reasonable measures can include:

- asking the client to provide supporting official documentation;
- conducting an open-source search; or
- consulting commercially available information.

As a best practice, you should also confirm whether a not-for-profit organization is a charity registered with the Canada Revenue Agency by consulting the charities listing on the Canada Revenue Agency website.

The reasonable measures that you take to confirm the accuracy of beneficial ownership information, which includes ownership, control, and structure information, must align with your risk assessment of the entity's risk for money laundering or terrorist activity financing offences. The reasonable measures you take with entities assessed to pose a high risk must go further to help you understand and confirm the beneficial ownership, as well as establish the overall ownership, control, and structure of that entity.

The reasonable measures that you take with entities that have a complex business structures must go further to ensure that you are able to understand and confirm the accuracy of beneficial ownership, which includes establishing the ownership, control and structure of that entity. This does not mean, however, that you need to consider or treat a complex entity as posing a high risk. You need to choose reasonable measures that are appropriate to the situation.

8. What if I cannot obtain beneficial ownership information or confirm its accuracy?

If you are unable to obtain the beneficial ownership information, to keep it up to date in the course of the ongoing monitoring of business relationships, or to confirm its accuracy, when it is first obtained, or during the course of ongoing monitoring then you must:Footnote 12

- take reasonable measures to verify the identity of the entity's chief executive officer or of the person who performs that function; and
- apply the special measures for high-risk clients, including enhanced ongoing monitoring.

For more information on enhanced ongoing monitoring, see FINTRAC's Ongoing monitoring requirements guidance.

9. How do I verify the identity of an entity's chief executive officer or of the person who performs that function?

The PCMLTFR does not require that you verify the identity of the chief executive officer or of the person who performs that function in accordance with the prescribed methods. However, you could use one of the methods outlined in the Methods to verify the identity of persons and entities guidance to meet this obligation.

Additionally, there is no record keeping obligation if you have identified the chief executive officer or a person who performs that function using the prescribed methods to verify identity. However, during a FINTRAC examination, you

could be asked to demonstrate the reasonable measures that you took to identify the chief executive officer or person who performs that function.

10. What if there are no beneficial owners?

You may obtain information confirming that there is no individual who directly or indirectly owns or controls 25% or more of a corporation, a widely held or publicly traded trust, or an entity other than a corporation or trust. This is not the same thing as being **unable to obtain** the beneficial ownership information.

If **you determine that there is no individual** who directly or indirectly owns or controls 25% or more of a corporation, a widely held or publicly traded trust, or an entity other than a corporation or trust, you must keep a record of the measures you took and the information you obtained in order to reach that conclusion.Footnote 13 However, you are still required to obtain and take reasonable measures to confirm information about the ownership, control and structure of the entity.

11. What beneficial ownership records do I need to keep?

You must keep a record of the beneficial ownership information you obtain and of the measures you take to confirm the accuracy of the information.

The measures that you take to confirm beneficial ownership information can be part of your overall policies and procedures, so a separate record may not be needed. You only need to keep an individual record of the specific measures you take to confirm the accuracy of beneficial ownership information in situations where the measures differ from those that are documented in your policies and procedures.

For a **corporation**, you must record:

- the names of all directors of the corporation;
- the names and addresses of all persons who directly or indirectly own or control 25% or more of the shares of the corporation; and
- information establishing the ownership, control and structure of the corporation.

For a **trust**, you must record:

- the names and addresses of all trustees, known beneficiaries and known settlors of the trust; and
- information establishing the ownership, control and structure of the trust.

For a **widely held or publicly traded trust**, you must record:

- the names of all trustees of the trust;
- the names and addresses of all persons who directly or indirectly own or control 25% or more of the units of the trust; and

- information establishing the ownership, control and structure of the trust.

For an **entity other than a corporation or trust**, you must record:

- the names and addresses of all persons who directly or indirectly own or control 25% or more of the entity; and
- information establishing the ownership, control and structure of the entity.

If you verify the identity of a **not-for-profit organization**, you must also keep a record that indicates whether the entity is:

- a charity registered with the Canada Revenue Agency under the Income Tax Act; or
- an organization, other than a registered charity, that solicits charitable donations from the public.

In situations where no individual directly or indirectly owns or controls 25% or more of a corporation, a widely held or publicly traded trust, or an entity other than a corporation or trust, you must keep a record of the measures you took to confirm the accuracy of the information, as well as the information you obtained in order to reach that conclusion. The date you took the measures should also be included as a best practice.

Retention: You must keep these records for at least five years from the day the last business transaction is conducted.

Ongoing monitoring requirements

Overview

1. What is ongoing monitoring?

Ongoing monitoring is a process that you must develop and use to review all the information you have obtained about the clients with whom you have a business relationship, in order to:

- detect any suspicious transactions that you are required to report to FINTRAC;
- keep client identification information, beneficial ownership information, and the purpose and intended nature of the business relationship record up to date;
- reassess the level of risk associated with your client's transactions and activities; and
- determine whether transactions or activities are consistent with the client information you obtained and your risk assessment of the client.

For more information about when you enter into a business relationship with a client see FINTRAC's Business relationship requirements guidance.

Your process for conducting ongoing monitoring could include the monitoring of an individual client or of groups of clients. References to the ongoing monitoring of a client in this guidance refers to both an individual client and groups of clients, depending on your processes.

2. When must I conduct ongoing monitoring?

When you enter into a business relationship with a client you must **periodically conduct** ongoing monitoring of that business relationship, based on your risk assessment.Footnote 2

The frequency at which you conduct ongoing monitoring will depend on the risk level assigned to clients in your risk assessment. For example, clients identified as posing a low risk may require less frequent ongoing monitoring whereas those in your high-risk category will require that you take enhanced measures. For more information on risk assessment requirements and enhanced measures, see FINTRAC's Compliance program requirements guidance.

FINTRAC expects that your policies and procedures will include the frequency at which you will conduct ongoing monitoring of your clients, based on your risk assessment for a client or group of clients.

3. When must I conduct enhanced ongoing monitoring?

You must take enhanced measures and conduct enhanced ongoing monitoring of a client that you have identified as posing a high risk in your risk assessment. This means that you must take extra measures in addition to what is required, as appropriate for the level of client risk.Footnote 3

You could consider the following methods to conduct enhanced ongoing monitoring of your high-risk clients:

- reviewing transactions based on an approved schedule that involves management sign-off;
- developing reports and reviewing these reports of high-risk transactions more frequently;
- flagging certain activities or those that deviate from your expectations and raise concerns, as necessary;
- setting business limits or parameters on accounts or transactions that would trigger early warning signals and require a mandatory review; or
- reviewing transactions more frequently against suspicious transaction indicators relevant to business relationships.

4. What are the exceptions to ongoing monitoring?

You do not have to conduct ongoing monitoring in the following situations:

1. **Financial entities**:You do not have toconduct ongoing monitoring for a group plan account held within a dividend or a distribution reinvestment

plan (including a plan that allows members to purchase additional shares or units with contributions other than the dividends or distributions paid by the sponsor of the plan), if the sponsor of the plan:Footnote 4

- is an entity whose shares or units are traded on a Canadian stock exchange; **and**
- operates in a country that is a member of the Financial Action Task Force.

2. **Insurance companies, brokers or agents**:You do not have to conduct ongoing monitoring when you are dealing in reinsurance.Footnote 5

5. What records do I need to keep for ongoing monitoring?

You must keep records of the measures you take **and** of the information obtained from the ongoing monitoring of your clients with whom you have a business relationship.Footnote 6 This includes:

- your processes in place to perform ongoing monitoring;
- your processes in place to perform the enhanced ongoing monitoring of high-risk clients;
- your processes for recording the information obtained as a result of your ongoing monitoring;
- your processes for recording the information obtained as a result of your enhanced ongoing monitoring of high-risk clients; and
- the information obtained as a result of your ongoing monitoring and enhanced ongoing monitoring of high-risk clients.

You must outline the measures you use to conduct the ongoing monitoring of your business relationships in your policies and procedures, which can form part of your ongoing monitoring records. However, the information you obtain as a result of your ongoing monitoring is likely to be specific to a particular business relationship and not captured in your policies and procedures, so it should be documented separately. You can document and update the information you obtain through your ongoing monitoring activities across several records. For example, updates to the client identification, beneficial ownership or business relationship information you have, could be recorded in any file you maintain on a client.

Retention: You must keep a record of the ongoing monitoring measures taken and the information obtained from that ongoing monitoring for at least five years from the date the record was created.Footnote 7

6. When does the requirement for ongoing monitoring end?

You are no longer required to conduct ongoing monitoring when your business relationship with a client ends. For more information about when a business relationship ends, see FINTRAC's Business relationship requirements guidance.

7. When does the requirement for enhanced ongoing monitoring end?

You are no longer required to conduct enhanced ongoing monitoring when your business relationship ends **or** when, based on your risk assessment, you no longer consider a client to pose a high risk. When you no longer consider a client high-risk, you are still required to conduct ongoing monitoring of the client at the frequency determined by the client's new risk rating. For more information about when a business relationship ends, see FINTRAC's Business relationship requirements guidance.

Third party determination requirements : FINTRAC's compliance guidance

This guidance explains the third party determination requirements under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (the Act) and associated Regulations.

2. Who is a third party and how to make a determination

A third party is the person or entity that instructs another person or entity to conduct a transaction or activity on their behalf. As such, the third party is the instructing party to the transaction or activity, and is also understood to be the party that the transaction occurs on behalf of (the "on behalf of" party).

Note: The Financial Action Task Force, the Egmont Group and other anti-money laundering and anti-terrorist financing authoritative bodies have observed that third parties have been used in several money laundering and terrorist financing cases. It is not uncommon for criminals to use third parties as a method to evade detection by distancing themselves from the proceeds of crime.

You must take reasonable measures to determine whether a third party is involved when you carry out certain transactions or activities, as explained in this guidance.

Reasonable measures for third party determination could include asking the client if they are acting at the instruction of another person or entity, or asking whether another person or entity will be instructing on the account. The steps you take as reasonable measures to make a third party determination must be documented in your compliance program's policies and procedures.

3. When to make a determination

You must take reasonable measures to make a third party determination when you are required to:

- report a large cash transaction or keep a large cash transaction record

- report a large virtual currency transaction or keep a large virtual currency transaction record
- keep a signature card or an account operating agreement
- keep an information record, or
- submit a Casino Disbursement Report

You must also provide information in an electronic funds transfer report (**casinos, money services businesses, foreign money services businesses, and financial entities only**) for any person or entity on whose behalf an electronic funds transfer is requested or received.

Large Cash Transaction Report or large cash transaction record

When you receive cash in an amount of $10,000 or more, and are required to submit a Large Cash Transaction Report to FINTRAC **or** to keep a large cash transaction record, you must take reasonable measures to determine whether **the** person **from whom you receive the cash** is acting on behalf of a third party.

This is the case even if you receive cash from an armoured car.

Note: This requirement applies to the 24-hour rule.

Large Virtual Currency Transaction Report or large virtual currency transaction record

When you receive an amount of virtual currency equivalent to $10,000 or more, and are required to submit a Large Virtual Currency Transaction Report to FINTRAC **or** to keep a large virtual currency transaction record, you must take reasonable measures to determine whether **the person from whom you receive the virtual currency** is acting on behalf of a third party.

Note: This requirement applies to the 24-hour rule.

Signature card or account operating agreement

As a **financial entity**, a **securities dealer** or a **casino**, you must take reasonable measures to determine whether an account will be used by or on behalf of a third party, **when you open an account** and are required to keep a signature card or an account operating agreement.

When you open a **credit card account** or a prepaid payment product account, you do not need to make a third party determination because you are not required to keep a signature card or an account operating agreement for these account types.

Information record

If you are required to keep an information record for certain transactions or activities, you must take reasonable measures to determine whether the person or entity for which the information record is kept on, is acting on behalf of a third party. This must be done at the time you create the information record.

This requirement applies to the following sectors:

- **money services business**
- **foreign money services business**
- **an agent of the Crown**
- **life insurance company broker or agent**
- **mortgage administrator, broker or lender**
- **real estate developer, broker or sales representative**,

Casino Disbursement Report

As a **casino,** when you are required to report a disbursement of $10,000 or more, you must take reasonable measures, at the time of the disbursement, to determine whether:

- the requester of the casino disbursement is acting on behalf of a third party

Note: This requirement applies to the 24-hour rule.

4. What measures to take

If you determine that there is a third party involved, you must take reasonable measures to obtain the following information about the third party:

- If the third party is a **person**—their name, address, telephone number (not required if the third party determination is made for a large cash transaction or large virtual currency transaction), date of birth and occupation, or in the case of a sole proprietor, the nature of their principal business
- If the third party is a **corporation or an other entity**—its name, address, telephone number (not required if the third party determination is made for a large cash transaction or large virtual currency transaction), the nature of its principal business, its registration or incorporation number and the jurisdiction (province or state) and country of issue of that number, and
- the **relationship** between the third party and the following person or entity, as applicable:
  - the person who conducts the large cash transaction
  - the person who conducts the large virtual currency transaction

  - the account holder(s)
  - the person or entity that the information record is kept on, or
  - the person or entity that requests the casino disbursement.

The relationship between the person or entity and the third party can be for example, an accountant, broker, customer, employee, friend or relative.

- A record must be kept of the information obtained.
- If you receive cash or virtual currency from an armoured car on behalf of another party (such as your client), you must obtain and keep a record of the information detailed above at the time the cash or virtual currency is received.

Retention: At least 5 years from the date the third party determination record was created

5. What if I am not able to make a determination, but I suspect that a third party is involved

If you are not able to make a third party determination, but have reasonable grounds to suspect that a third party is involved, you must keep a record that:

- describes the reason(s) why you suspect that the person or entity is acting on behalf of a third party, and
- as applicable, your record must also indicate:
  - When you receive cash in an amount of $10,000 or more, and are required to submit a Large Cash Transaction Report to FINTRAC **or** to keep a large cash transaction record—whether according to the person who gave you the cash, they are acting on their own behalf only
  - When you receive an amount of virtual currency equivalent to $10,000 or more, and are required to submit a Large Virtual Currency Transaction Report to FINTRAC **or** to keep a large virtual currency transaction record—whether according to the person from whom you received the virtual currency, they are acting on their own behalf only
  - When you open an account and are required to keep a signature card or an account operating agreement— whether according to a person who is authorized to act in respect of the account, the account will only be used by or on behalf of an account holder
  - When you create an information record—whether, according to the person or entity for which the information record is kept, they are acting on their own behalf only, and
  - When you are required to report a casino disbursement of $10,000 or more— whether, according to the person or entity that makes the request for the disbursement, they are acting on their own behalf only.

Retention: At least 5 years from the date the record was created.

6. What are the exceptions to making a third party determination

As a financial entity, you do **not** need to make a third party determination when you open an account and are required to keep a signature card or an account operating agreement, if the account is for the processing of payments by credit card or prepaid payment product for a merchant.

If you are a financial entity, securities dealer or casino, you do **not** need to make a third party determination when you open an account and are required to keep a signature card or an account operating agreement, if every account holder is a financial entity or a securities dealer that is engaged in the business of dealing in securities in Canada.

If you are a life insurance company, broker or agent, you do **not** need to make a third party determination when you keep an information record on a beneficiary in connection with the sale of a life insurance policy under which you are to remit an amount of $10,000 or more to the beneficiary over the duration of the policy, regardless of the means of payment.

7. What are the exceptions to keeping a record of a third party determination

If you are a **financial entity**, a **securities dealer** or a **casino**, you do not have to take reasonable measures to obtain information and keep a record of that information for a third party determination if an account is opened by a legal counsel, an accountant or a real estate broker or sales representative, and you have reasonable grounds to believe that the account is to be used only for clients of the legal counsel, accountant or real estate broker or sales representative, as the case may be.

If you are a **securities dealer,** you do not have to take reasonable measures to obtain information and keep a record of that information for a third party determination when an account operating agreement is kept for the account of a person or entity that is engaged in the business of dealing in securities only outside of Canada, and when:

- the account is in a country that is a member of the Financial Action Task Force
- the account is in a country that is not a member of the Financial Action Task Force but has implemented the recommendations of the Financial Action Task Force relating to client identification and, at the time that the account is opened, the securities dealer has obtained written assurance from the account holder that the country has implemented those recommendations, or

- the account is in a country that is not a member of the Financial Action Task Force and has not implemented the recommendations of the Financial Action Task Force relating to client identification but, at the time that the account is opened, the securities dealer has verified the identity of all third parties in accordance with the methods to verify the identity of persons and entities under the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations.

Business relationship requirements : FINTRAC's compliance guidance

From: Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)

This guidance explains when reporting entities enter into a business relationship with a client and related obligations under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (the Act) and associated Regulations.

1. Who must comply

This guidance applies to all reporting entities, however, some requirements and examples may only apply to certain reporting entities.

If you are a life insurance company, or an entity that is a broker or agent, that offers loans or prepaid payment products to the public, or maintains accounts related to these products, other than the excluded types in the Regulations, then you are considered a financial entity **for those activities** and you can find your business relationship obligations as a financial entity in the guidance below.

2. What is a business relationship

A business relationship is a relationship established between a reporting entity and a client to conduct financial transactions or provide services related to financial transactions.

3. When do I enter into a business relationship with a client

When you enter into a business relationship varies by reporting entity sector, and depends on the activities and transactions that a client conducts with you. For more information on when you enter into a business relationship with a client, see your sector-specific obligations below.

In this section

- Financial entities, securities dealers and casinos

- Accountants, agents of the Crown, British Columbia notaries, dealers in precious metals and precious stones, and life insurance companies, brokers and agents
- Real estate developers, brokers, or sales representatives, and mortgage administrators, mortgage brokers or mortgage lenders
- Money services businesses and foreign money services businesses

Financial entities, securities dealers and casinos

You enter into a business relationship with a client when 1 of the following occurs:

- **you open an account for a client**(except in certain circumstances, consult: Circumstances when a business relationship is not created), or
- when a client does not hold an account with you, the **second time, within a 5-year period,** that the client engages in a financial transaction **for which you are required to verify their identity**

Accountants, agents of the Crown, British Columbia notaries, dealers in precious metals and precious stones, and life insurance companies, brokers and agents

You enter into a business relationship with a client the second time that you are required to verify their identity **within a 5-year period**.

Real estate developers, brokers, or sales representatives, and mortgage administrators, mortgage brokers or mortgage lenders

You enter into a business relationship with a client the first time that you are required to verify their identity.

Money services businesses and foreign money services businesses

You enter into a business relationship with a client:

- the second time you are required to verify their identity within a **5-year period, or**
- when you enter into a service agreement with an entity (the entity must be in Canada if you are a Foreign Money Services Business)

4. Circumstances where a business relationship is not created

Financial entities, securities dealers, and casinos

You do **not** enter into a business relationship when opening an account, for the following circumstances, when you:

- open a business account, if you have already verified the identity of at least 3 persons authorized to give instructions for the account
- open a second account for a person who already has an account with you
- open an account at the request of an entity, for a life insurance company affiliated with the entity to deposit a death benefit under a life insurance policy or annuity, if:
  - the account is opened in the name of a beneficiary that is a person
  - only that death benefit may be deposited into the account, and
  - the policy or annuity contract under which the claim for the death benefit is made has been in existence for a period of at least 2 years before the day on which the claim is made
- open an account for the sale of mutual funds if there are reasonable grounds to believe that the client's identity has been verified by a securities dealer in respect of:
  - the sale of the mutual funds for which the account was opened, or
  - a transaction that is part of a series of transactions that includes that sale
- sell an exempt policy as defined in subsection 306(1) of the Income Tax Regulations
- sell a group life insurance policy that does not provide for a cash surrender value or a savings component
- sell an immediate or deferred annuity that is paid for entirely with funds that are directly transferred from a registered pension plan or from a pension plan that is required to be registered under the Pension Benefits Standards Act, 1985, or similar provincial legislation
- sell a registered annuity policy or a registered retirement income fund
- sell an immediate or deferred annuity that is paid for entirely with the proceeds of a group life insurance policy
- conduct atransaction that is part of a reverse mortgage or structured settlement
- open an account for the deposit and sale of shares from a corporate demutualization or the privatization of a Crown corporation
- open an account in the name of an affiliate of a financial entity, if the affiliate carries out activities that are similar to those of persons and entities referred to in paragraphs 5(a) to (g) of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act
- open a registered plan account, including a locked-in retirement plan account, a registered retirement savings plan account and a group registered retirement savings plan account

- open an account that is established in accordance with the escrow requirements of a Canadian securities regulator or Canadian stock exchange or provincial legislation
- open an account, if the account holder or settlor is a pension fund that is regulated under federal or provincial legislation
- open an account in the name of, or in respect of which instructions are authorized to be given by, a financial entity, a securities dealer, a life insurance company or an investment fund that is regulated under provincial securities legislation
- open an account solely in the course of providing accounting services to a securities dealer, and
- open an account, if you are a **financial entity** or **securities dealer** that is not required to verify the identity of, or to keep a signature card for a person who is a member of a group plan account if:
  - the member's contributions are made by the sponsor of the plan or by means of payroll deductions, and
  - the identity of the plan sponsor has been verified

All reporting entity sectors

You do not enter into a business relationship that would otherwise have been formed after the first or second time you are required to verify identity (as applicable to your reporting entity sector), if you are not required to verify the identity of a client under the Regulations because of a related exception. This is because your obligation to verify identity for a particular transaction, activity, or client does not apply in that circumstance. For example, if your requirement to verify identity does not apply because your client is a public body, a very large corporation, or a subsidiary of either of those, whose financial statements are consolidated, then a business relationship would not be formed.

However, a business relationship would be formed in instances where you have the obligation to verify identity, but the Regulations allow you to not do so for a particular reason. This is because the underlying obligation to verify a client's identity still exists, even if you relied upon the applicable reasoning for not verifying identity. This could occur as the result of a suspicious transaction or attempted transaction, or as the result of not having to re-verify the identity of a client.

- **Suspicious transaction reporting:**

When you are required to report a Suspicious Transaction Report to FINTRAC, you are required to take reasonable measures to verify the identity of the person or entity that conducts or attempts to conduct the transaction. Despite whether your reasonable measures are unsuccessful, or if you believe taking reasonable measures would inform the person or entity that you are filing a Suspicious

Transaction Report, this transaction must factor into your business relationship requirements, as either the first or second time you are required to verify the identity of a client.

- **Re-verifying identity:**

Your business relationship requirements must still factor in a transaction or activity for which you have the requirement to verify identity but choose not to because the Regulations allow it. The Regulations allow you to choose not to re-verify the identity of a client if:

- you previously did so using the methods specified in the Regulations in place at the time
- you have kept the associated records, and
- you have no doubts about the information used

5. When to determine if I have entered into a business relationship with a client

You should determine that you have entered into a business relationship as soon as possible after opening an account **or** after verifying your client's identity for either the first or second transaction or activity (as applicable to your reporting entity sector) where you had the obligation to do so. As a best practice, you should make a business relationship determination within 30 calendar days of opening the account **or** of the first or second transaction or activity (as applicable).

6. Business relationship records to keep

Once you enter into a business relationship with a client, you must keep a record of the purpose and intended nature of the business relationship. For sector-specific examples of the purpose and intended nature of a business relationship, see Annex A.

As a best practice, to help you meet your know your client requirements and conduct ongoing monitoring of your business relationships, this record should also:

- describe your business dealings with the client, and
- include information that would help you anticipate the types of transactions and activities that the client may conduct. You could then use this information to identify unusual or suspicious transactions while conducting your ongoing monitoring.

If you already have a record of this information that is readily available in other records that you are required to keep, you are not required to keep an additional record. For example, for clients who already hold accounts, you may use the information found in the intended use of the account record, client credit file, credit card account record or a service agreement to satisfy this obligation.

Retention: You must keep these records for 5 years from the day they were created.

7. When a business relationship ends

Account-based business relationships

A business relationship ends 5 years after the day on which a client closes their last account with you.

Non-account-based business relationships

A business relationship ends when a period of at least 5 years has passed since the day of the last transaction that required you to verify the identity of the client.

Mandate

As Canada's financial intelligence unit and anti-money laundering and anti-terrorist financing supervisor, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), or 'the Centre', helps to combat money laundering, terrorist activity financing and threats to the security of Canada, while ensuring the protection of personal information under its control.

FINTRAC is one of 13 federal departments and agencies that play a key role in Canada's Anti-Money Laundering and Anti Terrorist Financing regime.

The Centre's mandate is to ensure the compliance of businesses subject to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and associated Regulations, and to generate actionable financial intelligence for police, law enforcement and national security agencies to assist in the investigation of money laundering and terrorist activity financing offences or threats to the security of Canada. The Centre acts at arm's length and is independent from the police services, law enforcement agencies and other entities to which it is authorized to disclose financial intelligence.

FINTRAC is headquartered in Ottawa, with regional offices located in Montréal, Toronto, and Vancouver. It reports to the Minister of Finance, who is in turn accountable to Parliament for the activities of the Centre.

Money laundering

Money laundering is the process used to disguise the source of money or assets derived from criminal activity. There are three recognized stages in the money laundering process:

1. **Placement** involves placing the proceeds of crime in the financial system.

2. **Layering** involves converting the proceeds of crime into another form and creating complex layers of financial transactions to disguise the trail and the source and ownership of funds. This stage may involve transactions such as the buying and selling of stocks, commodities or property.
3. **Integration** involves placing the laundered proceeds back into the economy to create the perception of legitimacy.

The money laundering process is continuous, with new 'dirty' money constantly being introduced into the financial system.

Terrorist activity financing

Terrorist activity financing is the use of funds, property or other services to encourage, plan, assist or engage in acts of terrorism, where the primary motivation is not financial gain.

Two main differences distinguish terrorist activity financing from money laundering:

- Funds can be from legitimate sources, not just criminal acts; and
- Money is the means, not the end—the goal is to use funds to facilitate or implement terrorist activities.

Threats to the security of Canada

FINTRAC's role is to provide CSIS with financial intelligence to assist that agency in fulfilling its mandate of investigating threats to the security of Canada. Threats to the security of Canada are defined in the Canadian Security Intelligence Service Act as:

1. espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage;
2. foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive, or involve a threat to any person;
3. activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political, religious or ideological objective within Canada or a foreign state; and,
4. activities directed toward undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of the constitutionally established system of government in Canada, but does not include lawful advocacy, protest or dissent, unless carried on in conjunction with any of the activities referred to in paragraphs (a) to (d).
5. and intelligence agencies.

Canada's anti-money laundering and anti-terrorist financing regime

FINTRAC occupies an important position in the constellation of organizations involved in Canada's fight against money laundering and terrorism. Each of these organizations has a particular relationship with FINTRAC. Due to the nature of its mandate, the Centre's work is situated at the beginning of a process that starts with the reports to FINTRAC by financial institutions and intermediaries. With the assistance of specialized automated tools, skilled staff analyze the reported transactions and information from other sources to extract financial intelligence that would be relevant to the investigation or prosecution of money laundering offences, terrorist activity financing offences, and threats to the security of Canada.

Money laundering and terrorist financing cases can be extremely complex, often involving many players implicated in transnational and covert illicit activity. The investigations are often time and resource intensive. For this reason, the time between FINTRAC's initial disclosure and the conclusion of an investigation can be quite lengthy.

FINTRAC's core product is case-specific financial intelligence. FINTRAC is also well situated to provide strategic intelligence about trends and typologies of money laundering and terrorist financing. Because money laundering and terrorist financing are almost always transnational in character, and because an important part of FINTRAC's role is to exchange information with like bodies in other countries, it is also well placed to provide a strategic overview from an international perspective.

The Centre has signed information exchange agreements with certain foreign FIUs worldwide, enabling it to provide financial intelligence to its counterparts that can be crucial to investigations of cases involving the international movement of funds. Equally, it can receive information from these FIUs, which is useful to its own analysis.

When FINTRAC is satisfied that it has reasonable grounds to suspect that the information would be relevant to such investigations or prosecutions, it discloses this financial intelligence to law enforcement and/or intelligence agencies. These agencies, where appropriate, conduct investigations, and if warranted, bring charges against the individuals involved. The recipients of the intelligence include the Royal Canadian Mounted Police (RCMP), provincial and municipal police agencies, CSIS, CRA, IRCC and foreign FIUs with which the Centre has a Memorandum of Understanding (MOU) for the exchange of information.

FINTRAC is also active in many initiatives aimed at fostering international cooperation at the policy level. Notable among these is its participation in the Egmont Group, where FINTRAC is engaged in the sharing of best practices and other activities designed to strengthen support for member countries' anti-money laundering and anti-terrorist financing regimes.

Responsibilities

FINTRAC fulfills its mandate by engaging in the following activities:

- Receiving financial transaction reports and voluntary information in accordance with the PCMLTFA and Regulations;
- Safeguarding personal information under its control;
- Ensuring compliance of reporting entities with the PCMLTFA and Regulations;
- Maintaining a registry of money services businesses in Canada;
- Producing financial intelligence relevant to investigations of money laundering, terrorist activity financing and threats to the security of Canada;
- Researching and analyzing data from a variety of information sources that shed light on trends and patterns in money laundering and terrorist activity financing; and
- Enhancing public awareness and understanding of money laundering and terrorist activity financing.

In addition, FINTRAC is part of the Egmont Group, an international network of financial intelligence units that collaborate and exchange information to combat money laundering and terrorist activity financing.

FINTRAC also contributes to other multilateral fora such as the Financial Action Task Force (FATF), the Asia-Pacific Group on Money Laundering (APG) and the Caribbean Financial Action Task Force (CFATF), lending participation in international policymaking and the provision of technical assistance to other FIUs.

Privacy and protection of personal information

FINTRAC is subject to the *Privacy Act*, which strictly regulates how federal institutions can use and disclose personal information collected about individuals.

In addition, the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* stipulates that FINTRAC is to ensure that the personal information under its control is protected from unauthorized disclosure. Any unauthorized use or disclosure of information is prohibited and can result in severe penalties, including a fine of up to $500,000 or up to five years' imprisonment.

The Act also sets out that information can only be disclosed to law enforcement where there are reasonable grounds to suspect that the information would be relevant to investigating or prosecuting a money laundering offence or a terrorist activity financing offence, or to CSIS when there are reasonable grounds to suspect that it is relevant to threats to the security of Canada. Even in those circumstances, only "designated information" can be disclosed.

A financial transaction report is retained by FINTRAC for ten years. If it was not disclosed, it must be destroyed.

The complementary roles of the Office of the Superintendent of Financial Institutions and FINTRAC

Who is the Office of the Superintendent of Financial Institutions?

The Office of the Superintendent of Financial Institutions (OSFI) is Canada's prudential regulator and supervisor of most banks, federal insurance companies, and trust and loans companies. Its role is to determine whether they are in sound financial condition. OSFI also regulates and supervise federally regulated private pension plans to determine whether they meet their minimum funding requirements.

What does OSFI do?

OSFI is an independent agency of the Government of Canada, established to protect depositors, policyholders, financial institution creditors, and pension plan members, while allowing financial institutions to compete and take reasonable risks.

OSFI's overarching mandate is to contribute to public confidence in the Canadian financial system by:

fostering sound risk management and governance practices through a regulatory framework designed to control and manage risk supervising and intervening early if there are material deficiencies, and taking corrective measures, or requiring that institution act to address the situation monitoring and evaluating system-wide or sectoral developments that may have a negative impact on the financial condition of federally regulated financial institutions balancing the rights and interests of depositors, policyholders, financial institution creditors, and pension plan beneficiaries, while allowing financial institutions to compete effectively and take reasonable risks In 2023, OSFI's mandate was expanded to include ensuring that financial institutions have appropriate policies in place to protect themselves from threats to their integrity and security, including foreign interference.

Prudential regulation and supervision have traditionally focused on financial elements, such as capital and liquidity. Over the last few years, OSFI has focused on non-financial elements, such as technology and cyber, and culture risks. This change recognizes that inadequate mitigation of non-financial risks, just like financial risks, can have prudential consequences.

How does OSFI work with FINTRAC?

FINTRAC's sharing financial intelligence and regulatory compliance information is important to OSFI given its new expanded mandate.

When a financial institution fails to meet its regulatory compliance requirements of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, it

could indicate weakness in an institution's risk control environment or corporate culture.

Based on this information, OSFI will undertake supervisory examinations to verify that the institution is adhering to the appropriate regulatory guidelines, as money laundering has a direct impact on the security and integrity of a financial institution, prudential considerations are elevated.

OSFI's high-risk tolerance for early intervention means that it will respond proactively to address where risks could jeopardize the public's confidence in the soundness and integrity of the Canadian financial system, including vulnerabilities associated with money laundering.

Who is FINTRAC?

FINTRAC is Canada's financial intelligence unit and anti-money laundering and anti-terrorist financing supervisor. The Centre helps to combat money laundering, terrorist activity financing, sanctions evasion and threats to the security of Canada.

What does FINTRAC do?

FINTRAC ensures the compliance of thousands of businesses with requirements under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA), including financial entities, securities dealers, life insurance companies, brokers and agents, casinos, money services businesses, and real estate brokers and sales representatives, among others.

With this mandate, FINTRAC is the primary agency responsible for conducting anti-money laundering and anti-terrorist financing assessments of federally regulated financial institutions and ensuring their compliance with the PCMLTFA.

Businesses subject to the PCMLTFA are required to establish a compliance program, identify clients, keep records and report certain types of financial transactions to FINTRAC, including international electronic funds transfers, large cash transactions, large virtual currency transactions, casino disbursements and suspicious transactions.

FINTRAC applies a risk-based approach to ensuring the compliance of businesses subject to the PCMLTFA, including:

Monitoring and assessing the quality, timeliness and volume of financial transaction reporting Undertaking hundreds of supervisory activities every year, including examinations and follow-up examinations Enforcing action plans in cases of non-compliance Issuing administrative monetary penalties Disclosing cases of non-compliance to law enforcement for criminal investigation Compliance with the PCMLTFA helps deter criminals, terrorist financiers and sanctions evaders from using Canada's financial system for illicit purposes. It also ensures that FINTRAC receives the information that it needs to produce financial intelligence

to assist in the investigation and prosecution of money laundering, terrorist activity financing, sanctions evasion and threats to the security of Canada.

FINTRAC analyzes the reporting it receives from businesses, as well as the information it receives from law enforcement, government departments and agencies, foreign financial intelligence units and members of the public, to determine whether a disclosure of tactical financial intelligence is required to recipients listed in the Act.

How does FINTRAC work with OSFI?

In fulfilling its core supervisory and financial intelligence mandates, FINTRAC works closely with OSFI.

Under the PCMLTFA and the OSFI Act, FINTRAC and OSFI have respective authorities to share information related to the compliance of federally regulated financial institutions with Parts 1 and 1.1 of the PCMLTFA.

FINTRAC and OSFI can also share compliance-related information for the purpose of assessing risks to the integrity of Canada's financial system that may arise from the grant, revocation, suspension or amendment of an approval under the Bank Act, the Insurance Companies Act and the Trust and Loan Companies Act where this information also relates to money laundering activities or terrorist activity financing.

Separately, the PCMLTFA authorizes FINTRAC to disclose tactical financial intelligence to OSFI where there are reasonable grounds to suspect that the information would be relevant to threats to the security of Canada and that the information is relevant to the exercise of the powers or performance of the duties and functions of the Superintendent of OSFI.

Finally, under the PCMLTFA, FINTRAC is able to share with OSFI its strategic intelligence products related to money laundering, terrorist activity financing, sanctions evasion and the financing of threats to the security of Canada# Reporting suspicious transactions to FINTRAC : FINTRAC's compliance guidance

This guidance explains the requirement to report suspicious transactions to FINTRAC.

1. Who must comply

All reporting entities and their employees must report suspicious transactions.

If you are **a person who is an employee of a reporting entity** and your employer is actively reporting suspicious transactions, we do not require duplicate reporting. An employee is only expected to report suspicious transactions to FINTRAC in the rare instances where they believe that their employer has not submitted a Suspicious Transaction Report as required by the Proceeds of

Crime (Money Laundering) and Terrorist Financing Act (the Act) and associated Regulations. To submit a Suspicious Transaction Report in this scenario, the employee may use the paper report form as explained in section 4 below.

A **service provider** can submit and correct a Suspicious Transaction Report on your behalf. However, as the reporting entity, you are ultimately responsible for meeting the requirements under the Act and associated Regulations, even if a service provider is reporting on your behalf. This legal responsibility **cannot** be delegated.

No person or entity will be prosecuted for sending a Suspicious Transaction Report in good faith or for providing FINTRAC with information about suspicions of money laundering or terrorist financing.

2. What is a Suspicious Transaction Report

A suspicious transaction report is a type of report that you must submit to FINTRAC when a financial transaction occurs, or is attempted, in the course of your activities and there are **reasonable grounds to suspect** that the transaction is related to the commission or the attempted commission of a money laundering or terrorist activity financing offence.

Note: You are not allowed to inform anyone, including the client, of the contents of a Suspicious Transaction Report, or that you have made or will make such a report, if the intent is to prejudice a criminal investigation. This applies whether such an investigation has begun or not. It is important to not tip off your client about the fact that you are filing a Suspicious Transaction Report—therefore, you should not be requesting information that you would not normally request during a transaction if you believe this would tip off the client.

The Suspicious Transaction Report is one of the most valuable and unique report types submitted to FINTRAC. In addition to the prescribed information, Suspicious Transaction Reports allow you to expand the descriptive details surrounding a transaction that is derived from your assessment of what you are seeing through your business interactions and activities.

FINTRAC uses the following types of information in its analysis and production of financial disclosures:

- aliases
- nicknames
- other names and initials
- beneficial ownership information
- IP addresses
- account numbers
- email addresses
- virtual currency transaction addresses and their details
- email money transfers (EMTs)
- mobile money transfers

- details of purchases
- locations
- relationships
- background information

Because of the importance of FINTRAC's financial intelligence to the overall safety and security of Canadians and Canada's financial system, FINTRAC reviews and assesses every Suspicious Transaction Report it receives. When warranted, such as in the case of Suspicious Transaction Reports related to threats to the security of Canada, FINTRAC expedites its analysis in order to disclose financial intelligence to law enforcement and other intelligence partners within 24 hours.

3. What are reasonable grounds to suspect

Reasonable grounds to suspect is the required threshold to submit a Suspicious Transaction Report to FINTRAC and is a step above simple suspicion, meaning that there is a **possibility** that a money laundering or terrorist activity financing offence has occurred.

You **do not** have to verify the facts, context or money laundering or terrorist activity financing indicators that led to your suspicion, nor do you have to prove that a money laundering or terrorist activity financing offence has occurred in order to reach this threshold. Your suspicion must be reasonable and therefore, not biased or prejudiced.

Reaching this threshold means that you considered:

- the facts
- the context
- the money laundering or terrorist activity financing indicators
- the sanctions evasion characteristics related to a financial transaction

After having reviewed this information, you concluded that there are reasonable grounds to suspect that this particular financial transaction is related to the commission of a money laundering or terrorist activity financing offence. It also means that you are able to demonstrate and articulate your suspicion of money laundering or terrorist activity financing in such a way that another individual with similar knowledge, experience, or training would likely reach the same conclusion based on a review of the same information.

Many factors will support your assessment and conclusion that a money laundering or terrorist activity financing offence has possibly occurred. These factors, along with an explanation of your assessment, should be included in the narrative section of the Suspicious Transaction Report, specifically, the Details of suspicion section.

The reasonable grounds to suspect threshold may be better understood when you have an understanding of other thresholds:

- simple suspicion
- reasonable grounds to believe

Simple suspicion is a lower threshold than reasonable grounds to suspect and is synonymous with a "gut feeling" or "hunch". In other words, simple suspicion means that you have a feeling that something is unusual or suspicious, but do not have any facts, context or money laundering or terrorist activity financing indicators to support that feeling or to reasonably conclude that a money laundering or terrorist activity financing offence has occurred. Simple suspicion could prompt you to assess related transactions to see if there is any additional information that would support or confirm your suspicion.

Reasonable grounds to believe is a higher threshold than reasonable grounds to suspect and is **beyond** what is required to submit a Suspicious Transaction Report. Reasonable grounds to believe means that there are verified facts that support the **probability** that a money laundering or terrorist activity financing offence has occurred. In other words, there is enough evidence to support a reasonable and trained person to **believe**, **not just suspect**, that a money laundering or terrorist activity financing offence has occurred. For example, **law enforcement** must reach reasonable grounds to believe that criminal activity has occurred before they can obtain judicial authorizations, such as a **production order**.

If you are in receipt of a production order from law enforcement related to a predicate offence, you must perform an assessment of the facts, context, and money laundering or terrorist activity financing indicators to determine whether you have reasonable grounds to suspect that a particular transaction is related to the commission of a money laundering or terrorist activity financing offence.

4. When to submit a Suspicious Transaction Report

You must submit the Suspicious Transaction Report to FINTRAC **as soon as practicable** after you have completed measures that enable you to establish that there are reasonable grounds to suspect that the transaction or attempted transaction is related to the commission of a money laundering or terrorist activity financing offence.

Note: There is no monetary threshold associated with the reporting of a suspicious transaction.

Measures you can take to establish the reasonable grounds to suspect threshold

The measures you can take to establish that there are reasonable grounds to suspect that the transaction or attempted transaction is related to the commission of a money laundering or terrorist activity financing offence include the following:

- screening for and identifying suspicious transactions

- assessing the facts and context surrounding the suspicious transaction
- linking money laundering or terrorist activity financing indicators to your assessment of the facts and context
- explaining your grounds for suspicion in a Suspicious Transaction Report, where you articulate how the **facts**, **context** and **money laundering and terrorist activity financing indicators** allowed you to reach your grounds for suspicion

Your measures must be described in your compliance policies and procedures.

What is a fact A fact, for the purpose of completing a suspicious Transaction Report, is defined as an event, action, occurrence or element that exists or is known to have happened or existed. It cannot be an opinion.

For example:

- Facts about a transaction could include the date, time, location, amount or type.
- Facts known to a reporting entity could include account details, particular business lines, a client's financial history or information about a person or entity (for example, that the person has been convicted of a designated offence or is the subject of a production order, or that an entity is being investigated for fraud or any other indictable offence).

What is context Context, for the purpose of completing a Suspicious Transaction Report, is defined as information that clarifies the circumstances or explains a situation or transaction. This type of information is essential to differentiate between what may be suspicious and what may be reasonable in a given scenario.

You may observe or understand the context of a transaction through:

- a general awareness of the events occurring in a person or entity's business environment or community
- your knowledge of the typical financial activities found within your business
- regular know your client activities (for example, verifying the identity of persons and entities, their occupation or business, how they generate their wealth, their typical or expected transactional behaviours)
- the information obtained through the application of your risk assessment
- illustrative client details (for example, the financial background, behaviour and actions of your client)

A transaction may not appear suspicious in and of itself. However, a review of additional contextual elements surrounding the transaction may create suspicion. Conversely, the context of a particular transaction, which may have seemed unusual or suspicious from the onset, could lead you to reassess your client's

current and past transactions and conclude that they are reasonable in that circumstance.

Your suspicion of money laundering or terrorist activity financing will likely materialize from your assessment of multiple elements (transactions, facts, context, and any other related information that may or may not be an indicator of money laundering or terrorist activity financing. When these elements are viewed together, they create a picture that will either support or negate your suspicion of the commission of a money laundering or terrorist activity financing offence.

Examples of how suspicion may arise

- **A person:**
  - asks several questions about your reporting obligations to FINTRAC (context)
  - wants to know how they can avoid their transaction being reported to FINTRAC (context)
  - structures their amounts to avoid client identification or reporting thresholds (fact)
  - keeps changing their explanation for conducting a transaction or knows few details about its purpose (context)
- **Transactions constantly being made on behalf of another person or entity:**
  - a client conducts a transaction while accompanied, overseen or directed by another party (fact)
  - payments to or from unrelated parties (foreign or domestic) (fact)
  - client appears to be or states that they are acting on behalf of another party (context)

For reporting entity sectors that deal with accounts:

- **A person making a deposit to a personal account, where the person:**
  - has an income or job or account history that is not consistent with the deposit amounts (fact)
  - keeps changing their reason for the deposit, and cannot or will not provide a reason (context)
  - exhibits nervous behaviour (context)
- **Transactions to a business account with the following additional elements:**
  - deposits to the account are made by numerous parties that are not signing authorities or employees (fact)
  - the account activity involves wire transfers in and out of the country (fact), which do not fit the expected pattern for that business (context)
- **Transactions frequently being made on behalf of another person or entity:**

– multiple payments made to an account by non-account holders (fact)
– account is linked to seemingly unconnected parties (context)

What is a money laundering or terrorist activity financing indicator, or sanctions evasion characteristic Money laundering and terrorist activity financing indicators, and sanctions evasion characteristics are potential red flags that can initiate suspicion and indicate that something may be unusual without a reasonable explanation. Red flags typically stem from one or more facts, behaviours, patterns or other contextual factors that identify irregularities related to a client's transactions. These often present inconsistencies with what is expected or considered normal based on the facts and context you know about your client and their transactional activities.

Criminal organizations often try to avoid the detection of money laundering or terrorist activity financing by using multiple concealment methods. Indicators of money laundering and terrorist activity financing can bring to light suspicious transactional activity, but it is your holistic assessment of facts, context and money laundering and terrorist activity financing indicators that will enable you to determine whether you have reached reasonable grounds to suspect that a transaction is related to the commission of a money laundering or terrorist activity financing offence. Indicators are also helpful to articulate your rationale for reaching the reasonable grounds to suspect threshold in a Suspicious Transaction Report. The explanation of how you reached your grounds for suspicion is extremely important for FINTRAC's development and disclosure of financial intelligence.

For more information and examples of money laundering and terrorist activity financing indicators applicable to your business sector:

- Consult money laundering and terrorist financing indicators under All FINTRAC guidance – Transaction reporting
- FINTRAC also publishes strategic intelligence products (for example, operational alerts and briefs) that focus on the identification of money laundering or terrorist activity financing related methods, techniques, and vulnerabilities

For information on the characteristics of financial transactions related to suspected sanctions evasion, consult FINTRAC's Special Bulletin on financial activity associated with suspected sanctions evasion.

What is "as soon as practicable" **As soon as practicable** means that you have completed the measures that have allowed you to determine that you reached the reasonable grounds to suspect threshold and as such the development and submission of that Suspicious Transaction Report must be treated as a priority. The greater the delay to submit a Suspicious Transaction Report, the greater the need for a suitable explanation. Suspicious Transaction Reports can be complex, yet you must treat them as a priority and ensure they are timely.

You must also complete the measures that allowed you to conclude that you have reasonable grounds to suspect the transaction is related to the commission of a money laundering or terrorist activity financing offence **before** you submit the report to FINTRAC.

Failure to submit a Suspicious Transaction Report, or not submitting one in a timely manner, may impede FINTRAC's ability to carry out its mandate. FINTRAC expects that when you have completed your measures and determined that you have reasonable grounds to suspect that a transaction is related to the commission of a money laundering or terrorist activity financing offence, you will prioritize the submission of that Suspicious Transaction Report.

Note: In situations involving time-sensitive information, such as suspected terrorist financing and threats to national security, you are encouraged, as a best practice, to expedite the submission of your Suspicious Transaction Reports. We recommend that this be included in your compliance policies and procedures.

5. How to submit a report to FINTRAC

You must submit a suspicious transaction report to FINTRAC **electronically** using the following options:

- FINTRAC Web Reporting System (FWR) (geared towards reporting entities with lower reporting volumes)
- FINTRAC API report submission (secure system-to-system transfer of report information)

Paper reporting

If you do **not** have the technical capability to submit reports electronically, you must submit reports in paper form to FINTRAC. You can access and print the Suspicious Transaction Report in paper form on the Paper reporting forms web page, or request to have one faxed or mailed to you by calling 1-866-346-8722.

Changes to a Suspicious Transaction Report

Once you have submitted a Suspicious Transaction Report, it is possible to modify the report, for instance to add missing information or make corrections, but you must provide an explanation for the change.

If you submitted a Suspicious Transaction Report to FINTRAC and need to make a subsequent change to the report, you must make the change and submit the revised report to FINTRAC **within 20 days of the date in which you made the request for change**, based on system requirements.

6. The form for reporting suspicious transactions

Form structure

The form for reporting suspicious transactions has 6 sections:

- General information
- Transaction information
- Starting action
- Completing action
- Details of suspicion
- Action taken

Main sections of the form | Type of information for each section |
General information | - Reporting entity report reference number- Information about your business including contact details- Ministerial Directives |
Transaction information | - Transaction status (completed or attempted)- Reason transaction was not completed (if applicable) - Date and time of transaction - Method of transaction- Location where transaction was conducted or attempted - Purpose of the transaction- Reporting entity transaction reference number |
Starting action | - Direction of starting action (in or out)- Amount and type of funds, assets or virtual currency (in or out)- Currency or virtual currency type- Information about the source of funds, assets or virtual currency - Virtual currency address reference and/or account information - Information about how the funds or virtual currency were obtained- Conductor (person or entity that conducted or attempted the transaction and their associated information)- Third party (person or entity on whose behalf the transaction is conducted or attempted and their associated information) |
Completing action | - Details of disposition- Amount and currency or virtual currency type- Virtual currency address, reference and/or account information- Any other person or entity involved in the completing action and their associated information- Beneficiary (any person or entity that was the beneficiary of the transaction and their associated information) |
Details of suspicion | This is a free form text section where you can describe in clear, simple and concise language your grounds for suspicion of a money laundering, terrorist activity financing or sanctions evasion offence including the facts, context, and indicators that allowed you to reach reasonable grounds for suspicion.In this section, you can indicate:- whether the suspicious activity is related to a money laundering, terrorist activity financing or sanctions evasion offence.- the public-private partnership project name(s)- whether the report includes information about an individual who has been determined to be a politically exposed person- Report reference numbers of previously submitted reports that may relate to the suspicious activity mention in this report |
Action taken | - This is a free form text section where you can describe what action, if any, was or will be taken as a result of the suspicious transaction(s) |
NoteThis table shows the type of information for each section **but does not list every field** on the form.- To access most fields and their category (manda-

tory, mandatory for processing or reasonable efforts), refer to: - Annex A: Field instructions to complete a Suspicious Transaction Report (which provides instructions on completing the form) |

Structure of the Suspicious Transaction Report form: Main sections and types of information for each section

Form highlights

The structure of the form allows you to include **1 or more transactions** in a report.

- When **entering multiple transactions** into a report, you can enter transactions that have:
  - the same or different transaction status (for example, a report can include completed transactions and attempted transactions), **and**
  - have taken place at the same or different locations
- For **each completed or attempted transaction**, you must provide all of these details:
  - information obtained about that transaction
  - the details of suspicion
  - the action you have taken in the fields provided in the Suspicious Transaction Report

For example, if you know or obtained the following information, you must provide it in the Suspicious Transaction Report:

- name of the person or entity who completed or attempted to complete the transaction
- type and amount of funds, assets or virtual currency involved in the completed transaction or attempted transaction
- how the funds, assets or virtual currency were used (details of disposition) for a completed transaction or going to be used in an attempted transaction
- whether the person or entity who conducted or attempted the transaction did so on anyone else's behalf
- account details of an account involved in a completed transaction or was going to be involved in an attempted transaction
- For a **completed transaction**, there should be at least **1 starting action** and **1 completing action**.
  - You must also provide the name of the beneficiary to the transaction if you know or obtained this information.

        * For instance, if this transaction had also been submitted to FINTRAC in a different report (LVCTR, LCTR, EFTR, CDR), you may have obtained beneficiary name at that time.

- A transaction can have **multiple starting actions and/or completing actions**—depending on the client's instructions.
  - Within each starting action, you can include multiple conductors, account holders, sources of funds or virtual currency, and third parties.
    * If the conductor or third party is an entity, you can also include information about the entity's director(s), beneficial owner(s), trustee(s), settlor(s), and beneficiary(s) as applicable.
  - Within **each completing action**, you can include multiple account holders, beneficiaries and other persons or entities involved in the completing action.
- **For each starting action, you will need to indicate the direction of the funds, asset or virtual currency** used to start the transaction as either **in** or **out**.
  - The direction of the starting action is **in** when a client physically brings in or electronically transfers in funds, assets or virtual currency to your business to start a transaction.
  - The direction of the starting action is **out** when your client requests to start a transaction with client funds, assets or virtual currency already held by or deposited at your business.

For example:

- The **direction of the starting action is in**, if a client brings cash to your business to purchase a bank draft.
- The **direction of the funds is out for the starting action**, if a client does not bring in any funds but requests to purchase a bank draft with the client's funds already held by or deposited at your business.

Important information about the number of transactions, starting actions and completing actions in a report

- You must complete the General Information section of the report and provide information for each transaction.
- Every transaction must have at least:
  - 1 starting action, and
  - 1 completing action (if available)
- A report can have multiple transactions and within each transaction, you can include multiple starting and completing actions.
- When completing the report, you must ensure that the information you provide reflects your client's instructions and is consistent with your policies and procedures.

Example 1

- On July 10, 2023, Ms. Green walks into branch 1 of Maple Credit Union and deposits $9,900 cash into her savings account.
- On July 11, 2023, Ms. Green walks into branch 2 of Maple Credit Union with a cheque for $20,000 and deposits $12,000 into her savings account and $8,000 into her chequing account.
- On July 12, 2023, Ms. Green walks into branch 1 of Maple Credit Union and instructs that $20,000 be withdrawn from her savings account and transferred to ABC Automotive Company's account at Hemlock Bank.

Based on a review of facts, context and indicators, as well as their procedures to assess suspicious transactions, Maple Credit Union establishes that there are **reasonable grounds to suspect** that the transactions are related to the commission of a money laundering or terrorist activity financing offence.

Therefore, Maple Credit Union submits a Suspicious Transaction Report.

The Suspicious Transaction Report provides general information about Maple Credit Union and indicates that Ms. Green conducted 3 transactions:

- The **first transaction** was conducted at branch 1 on July 10, 2023:
  - **1 starting action** involving $9,900 **cash coming in,** and
  - **1 completing action** where $9,900 is **deposited into a savings account**.
  - As Ms. Green is the **sole account holder**, she is the **beneficiary** of this transaction.
- The **second transaction** was conducted at branch 2 on July 11, 2023:
  - **1 starting action** involving a $20,000 **cheque coming in,** and
  - **2 completing actions** where $12,000 is **deposited into a savings account** and $8,000 is **deposited into a chequing account**.
  - Ms. Green is the **sole account holder** for both accounts and therefore the **beneficiary** of this transaction.
- The **third transaction** was conducted at branch 1 on July 12, 2023:
  - **1 starting action** involving $20,000 **funds withdrawal out,** and
  - **1 completing action**—an **outgoing domestic funds transfer** for $20,000 where ABC Automotive Company is the **beneficiary**.

In the **Details of suspicion section** of the Suspicious Transaction Report, Maple Credit Union provides the facts, context and indicators that allowed it to conclude that there are reasonable grounds to suspect that the transactions are related to the commission or attempted commission of a money laundering or terrorist activity financing offence.

In the **Action taken section**, Maple Credit Union describes the action it has taken.

7. Other requirements associated with suspicious transactions

Compliance program

Your compliance policies and procedures must outline your process and criteria on:

- how you identify and assess Suspicious Transactions Reports
- submitting reports to FINTRAC

If you have an automated or triggering system in place to detect suspicious transactions, a person may still assess the transaction(s), as a best practice, to determine whether there are reasonable grounds to suspect that a transaction is related to the commission of a money laundering or terrorist activity financing offence, and to ensure that, in these cases, the submission of a Suspicious Transaction Report.

Your compliance program must also include **training** on suspected money laundering and terrorist financing activities in relation to your business.

You must also assess the effectiveness of your compliance program as a part of your **two-year effectiveness review**. This includes assessing how effective you are in detecting, assessing and submitting Suspicious Transaction Reports. The following are examples of how this can be done:

- Review previously submitted Suspicious Transaction Reports to ensure that you are consistent in the detection, assessment and submission of these reports.
  - If certain money laundering or terrorist activity financing indicators have supported your suspicions of money laundering or terrorist activity financing, you can assess whether these indicators apply to other situations to ensure that you are not missing suspicious transactions that should be or should have been reported to FINTRAC. This approach can help you build consistency within your organization.
- Work with others in your business sector to learn how they are detecting, assessing and reaching the reasonable grounds to suspect threshold and to establish common ideas of what could be considered unusual or suspicious.

  For more information, consult FINTRAC's strategic intelligence products:
  - Strategic intelligence
- Review a sample of your Suspicious Transaction Reports to assess the timeliness of your reporting of suspicious transactions.
  - Specifically, you can review your business processes to ensure that you are submitting Suspicious Transaction Reports to FINTRAC as soon as practicable after you have completed measures that enable you to determine that there are reasonable grounds to suspect that

the transaction or attempted transaction is related to the commission of a money laundering or terrorist activity financing offence.

- Review a sample of your Suspicious Transaction Reports to assess the quality of information reported.
  - This can include reviewing the integrity and consistency of know your client information held by your business and ensuring that all know your client information was included in the Suspicious Transaction Reports.

Large cash transactions

If the suspicious transaction involves a reportable large cash transaction, then you must submit a Large Cash Transaction Reports to FINTRAC **in addition to** a Suspicious Transaction Report.

Electronic funds transfers

If the suspicious transaction involved a reportable electronic funds transfer, then you must submit an Electronic Funds Transfer Report to FINTRAC **in addition to** a Suspicious Transaction Report.

Large virtual currency transactions

If the suspicious transaction involved a reportable large virtual currency transaction, then you must submit a Large Virtual Currency Transaction Report to FINTRAC **in addition to** a Suspicious Transaction Report.

Casino disbursements

If the suspicious transaction involved a reportable casino disbursement, then you must submit a Casino Disbursement Report to FINTRAC **in addition to** a Suspicious Transaction Report.

Terrorist property

In addition to reporting a suspicious transaction, you may also be required to submit a Terrorist Property Reports to FINTRAC if you are required to make a disclosure under the Criminal Code or the Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism.

Record keeping requirements

When you submit a Suspicious Transaction Report to FINTRAC, you must keep a copy of it for **at least 5 years** after the day the report is sent.

Verifying the identity of persons and entities

You are required to take reasonable measures to verify the identity of every person or entity that conducts or attempts to conduct a suspicious transaction. This means that you are expected to ask the client for this information unless you think doing so will tip them off to your suspicion.

Third party determination

There are requirements to determine whether a person or entity is acting on behalf of another person or entity for a financial activity or transaction.

Ministerial directives

You must consider all requirements issued under a ministerial directive along with your suspicious transaction reporting requirements.

Voluntary self-declaration of non-compliance

If you discover instances of non-compliance related to your suspicious transaction reporting requirements, FINTRAC strongly encourages you to report a voluntary self-declaration of non-compliance.

8. Reporting subsequent suspicious transactions

Once you have reached the reasonable grounds to suspect threshold, you must submit a Suspicious Transaction Report. If there are subsequent transactions, you must keep reporting the transactions as long as the suspicion remains.

You are expected to periodically re-assess the client to verify that the level of suspicion has not changed. This process may be part of your documented risk assessment or ongoing monitoring.

If you continue to report Suspicious Transaction Reports on the same person or entity, you can reference a previous Suspicious Transaction Report in the Related Report(s) section by providing all of the following information:

- the reporting entity report reference number and the reporting entity transaction reference number
- the reasonable grounds to suspect (facts, context and money laundering and terrorist financing indicators) that were included in the first Suspicious Transaction Report submission
- any new additional information

If you are reporting Suspicious Transaction Reports due to new facts, context, or money laundering or terrorist activity financing indicators revealed during your assessment of the client, you are expected to detail this new information in the Suspicious Transaction Reports.

- For example, through the course of your assessment, you may have identified new money laundering or terrorist activity financing indicators, or new people or entities transacting with your client. You may choose to include that information under a separate heading in the Details of suspicion section of the Suspicious Transaction Report so that it is properly labeled as new information.

9. FINTRAC's expectations for completing a Suspicious Transaction Report

It is your responsibility to ensure that the information provided in a Suspicious Transaction Report is complete and accurate. It is also important that you submit comprehensive and high quality Suspicious Transaction Report to facilitate FINTRAC's analysis process and disclosure to recipients.

In the narrative sections of the Suspicious Transaction Report: Details of suspicion and Action taken, it is important to **avoid jargon or non-public references**, such as terms and acronyms that are specific to your organization. Please use clear, simple and concise language so that an outsider can easily understand the information that you provide.

A variety of information is often collected as part of an assessment to determine if you are required to submit a Suspicious Transaction Report and this information is valuable to include in your report to FINTRAC.

A well-completed Suspicious Transaction Report should consider the following questions:

- **Who** are the parties to the transaction?
  - Provide information on:
    - **conductor(s)**
    - **third party(ies)**
    - **beneficiary(ies)**
    - **account holder(s)**
    - **source(s) of funds or virtual currency**
    - **any other person or entity involved in the transaction(s)**
  - Provide **identifying information** on the parties involved in the transaction. This could include the information you recorded to identify the conductor, as well as any information you have on the other parties to the transaction or its recipients. See the Annexes of the Methods to verify the identity of persons and entities for a summary of information that must be recorded when verifying identity.
  - **When possible**, provide information on:
    - **owner(s)**
    - **director(s)**

        * **officer(s)**
        * **trustee(s)**
        * **settlor(s)**
        * **those with signing authority**
    - If the transaction involves an entity, you can include information on the ownership, control and structure of the business in the Suspicious Transaction Report.
    - Provide **clear information about each person or entity's role** in each of the financial transactions described. For example, it is important to know who is sending and receiving the funds and this can be elaborated in the Details of suspicion section of the Suspicious Transaction Report.
    - **Provide the relationships between the parties (if known).** This is very helpful to FINTRAC when trying to establish networks of persons or entities suspected of being involved in the commission or attempted commission of a money laundering, terrorist activity financing or sanctions evasion offence.
- **When** was the transaction completed/attempted? If it was not completed, why not?
    - Provide the **facts, context and** money laundering and terrorist activity financing indicators, or sanctions evasion characteristics regarding the transaction
- **What** are the financial instruments or mechanisms used to conduct the transaction?
- **Where** did this transaction take place?
- **Why** are the transaction(s) or attempted transaction(s) related to the commission or attempted commission of a money laundering, terrorist activity financing or sanctions evasion offence?
    - State the money laundering or terrorist activity financing indicators, or sanctions evasion characteristics used to support your suspicion.
    - State the **suspected** criminal offence related to money laundering, terrorist activity financing or sanctions evasion, if known.
- **How** did the transaction take place?

Transactions and their details must be entered in the appropriate structured fields of the form.

- Transactions may be referenced in the narrative section if there are additional facts or context.
- Examples of structured fields where you can enter information include the following **:**
    - a person's alias

  - electronic transfers (such as email money transfers (EMTs) or wire transfers) including IP addresses and sender/recipient email addresses
  - location of automated teller machine (ATM) withdrawals
  - the ownership, control and structure of an entity
  - the source of funds or virtual currency
  - any related and previously submitted Suspicious Transaction Report report reference numbers and transaction reference numbers
  - credit card activity including details of purchases (dates, amounts, retailer (online or in-store) and details of payments (dates, amounts, conductor and source of payment)

If there are transaction details for which there is no structured field for this information, you can include this information in the narrative section of the Suspicious Transaction Report.

- Information provided in the narrative section of the Suspicious Transaction Report can contribute greatly to FINTRAC's analysis. This includes the following types of information:
  - the history the client has with you
  - links made to other people, businesses and accounts
  - information on the ownership, control and structure of an entity that is not already captured in the fields provided in the Suspicious Transaction Report form, particularly for any business entities that have a complex structure
  - the intended or expected use of an account versus the activity you may have observed
  - any other information about your interactions with the client
  - relationships between parties to the transaction
  - the money laundering or terrorist activity financing indicators or factors that assisted in forming the basis of your suspicion
  - any information, including publicly available information and/or information from law enforcement, that made you suspect that the transaction might be related to terrorist financing, money laundering, or both
  - the location where a transaction was conducted, when this location does not belong to your business—for example, the location of a white label ATM that you do not own
  - information on any politically exposed persons, including their names, role and involvement in the transactions being reported
  - any details surrounding why an attempted transaction was not completed
  - any context or clarification about the information that was reported in the structured sections

If there are multiple details for a field, provide the detail that is specific to the transaction.

This may occur for some fields such as the following:

- email address
- telephone number
- URL
- Username
- Device identifier number
- Internet protocol address

For example:

- Your client Billy Bird has three email addresses (Sky@example.ca, Sky22@example.ca and BlueSky@example.ca.); and sends email money transfers (EMTs) to Oscar Ocean who is also your client. Oscar has two email addresses (Starfish@example.ca and Whaleshark@example.ca).
- A recipient, who is not your client, has the email address, FastCar@example.ca and goes by an alias name, "Smitty".

The email addresses that you report in a Suspicious Transaction Report will depend on the transaction details.

The table below provides some transaction details and the expected email address that should be reported.

Transaction details	Email address to be reported in the Suspicious Transaction Report
Billy Bird sends an outgoing email money transfer (EMT) for $500 using Sky@example.ca to Oscar Ocean at Starfish@example.ca	- Sky@example.ca (conductor email address field) - Starfish@example.ca (beneficiary email address field).
Billy Bird sends an outgoing email money transfer (EMT) for $900 using Sky22@example.ca to Oscar Ocean at Whaleshark@example.ca.	- Sky22@example.ca (conductor email address field) - Whaleshark@example.ca (beneficiary email address field).
Billy Bird sends an outgoing email money transfer (EMT) for $1,000 using Sky22@example.ca to "Smitty" at FastCar@example.ca	- Sky22@example.ca (conductor email address field)- FastCar@example.ca (beneficiary email address field).

Any additional email addresses that you have on your client (and were not related to a specific transaction) can be reported in the Details of suspicion section of the Suspicious Transaction Report. In the example above, you can explain in this section that your client, Billy Bird, has a third email address (BlueSky@example.ca) that was not used in these transactions.

Note: If your client (conductor) is not sending an email money transfer (EMT), you should still report the client's email address that you have on file in the

conductor email address field. If your client has more than one email address, the additional email addresses can be provided in the narrative section of the Suspicious Transaction Report (Details of suspicion).

FINTRAC has been able to identify networks of suspected money launderers and terrorist financiers through pieces of information such as email addresses and secondary identifiers (nicknames) or phone numbers. This type of information may seem insignificant but can be very important to FINTRAC, as it may identify connections among persons, entities or crimes when compared against other FINTRAC intelligence.

The Suspicious Transaction Report structure is intended to encourage reporting even in situations where you may not have information because the client did not provide any or asking for details might "tip off" the client to your suspicions. It is FINTRAC's expectation that if you have the information within your organization, that it be reported.

10. Common Suspicious Transaction Report deficiencies to avoid

The following are examples of deficiencies that FINTRAC has identified through its assessments and other compliance activities. FINTRAC is sharing these examples to illustrate common errors that you can avoid.

- **Using a higher threshold as your basis for reporting**
  - You are required to submit a Suspicious Transaction Report when you have completed the measures that enable you to establish that there are **reasonable grounds to suspect** that a transaction is related to the commission of a money laundering or terrorist activity financing offence as explained in section 3. Reasonable grounds to believe is a higher threshold than reasonable grounds to suspect and is beyond what is required to submit a Suspicious Transaction Report.
- **Failing to list all the transactions and accounts relevant to your suspicion in the specified fields**
  - You are required to report all the transactions and accounts that led to your determination that there are reasonable grounds to suspect that the transaction is related to the commission or attempted commission of a money laundering or terrorist activity financing offence in the specified fields of the report. Providing a summary of the transactions in the narrative section (Details of suspicion) is not enough.
- **Not providing or naming all parties to the transactions when the information is available**
  - All parties to the transaction, including their associated information, must be provided in their corresponding structured fields if this information is available. This includes any conductors, third parties, beneficiaries, account holders, sources of funds or virtual currency,

and any other persons or entities involved in the transaction.

- If an entity is involved, then owners, directors, officers, trustees, settlors and those with signing authority should be provided as applicable. You should also specify whether the parties are known or unknown.
- This has been observed in transactions such as wire transfers that involve multiple parties.
  - For example, if you are reporting a wire transfer, you should include any information you have on both the ordering client and beneficiary. This could include, but is not limited to, their names, their account number and institution, their relationship, and any known identifiers. FINTRAC acknowledges that this information may not always be at your disposal, but when you know it, you should provide it.
- **The information provided in the narrative section of the Suspicious Transaction Report (Details of suspicion) does not elaborate on your grounds for suspicion or link to the transaction(s) in the report**
  - You must explain the reason(s) for your determination that there are reasonable grounds to suspect that the transaction(s) is/(are) related to the commission or attempted commission of a money laundering or terrorist financing offence. This includes providing,in the narrative section of the Suspicious Transaction Report,all of the relevant facts, context and money laundering and terrorist activity financing indicators that are related to the transaction(s) in the report and support your suspicion.
  - This deficiency has been observed when a reporting entity does not articulate the reasons for their suspicion or does not explain how or why certain information is relevant to their suspicion.

Annex A: Field instructions to complete a Suspicious Transaction Report

This annex contains instructions on how to complete the fields in a Suspicious Transaction Report.

Note:

- Some fields only become applicable on the completion of other fields.
- Some field instructions may only apply to the electronic report submissions and not paper submissions.
- Fields that are **not applicable** are to **be left blank**. When a field is not applicable:
  - **do not enter** “Not applicable”, “N/A” or “n/a”, or
  - **do not substitute** any other abbreviations, special characters (“x”, “-”or “*”) or words (“unknown”) in the field

- **Failure to provide applicable reporting information** will result in non-compliance and may lead to criminal or administrative penalties.

Standardized field instructions

This section contains instructions for:

- the expected level of effort to obtain the prescribed information for the reporting fields
- completing some fields that appear in multiple sections of the form.

In this section

Field categories Fields are categorized as either:

- mandatory
- mandatory for processing
- mandatory if applicable, or
- reasonable measures

Field categories	Instructions
Mandatory	These fields are indicated with an asterisk symbol **(*)** and **must** be completed. However, **in the case of an attempted transaction**, these fields become "reasonable measures" fields and you must take reasonable measures, as indicated in the instructions below, to obtain the information for any mandatory field. Legal references- Proceed of Crime (Money Laundering) and Terrorist Financing Suspicious Transaction Reporting Regulations, SOR/2001-317 - section 11(2)
Mandatory for processing	These fields are indicated with a double dagger symbol **(‡)** and **must** be completed.

Field categories	Instructions
Mandatory if applicable	These fields are indicated with a dagger symbol **(†)** and **must** be completed if they are applicable to you or the transaction being reported.
Reasonable measures	You must take reasonable measures to obtain the information for all non-mandatory fields in the report, **if they are applicable**.Reasonable measures are the steps that you must take, as outlined in your policies and procedures, to obtain the information that can include asking the person or entity involved in the transaction for the information.If you obtain the information, you must report it. You must also provide the information if it is contained within your systems or records.For all fields, you are not required to obtain the information or take reasonable measures to obtain the information if you believe doing so will tip off the person or entity that you are submitting a Suspicious Transaction Report.**Note**: **Fields that are not applicable are to be left blank.**- When a field is not applicable, **do not enter** "Not applicable", "N/A" or "n/a" or substitute any other abbreviations, special characters ("x", "-" or "*") or words ("unknown") in these fields. Legal references- Proceed of Crime (Money Laundering) and Terrorist Financing Suspicious Transaction Reporting Regulations, SOR/2001-317 - section 11(1) - section 11(3)

Instructions for field categories

Name fields

Name fields	Instructions
Surname	Provide the last name of the person.
Given name	Provide the first name of the person.**Note:** If a person has only a single name, enter "XXX" in the "Given name" field and the person's single name in the "Surname" field.
Other/Initial	Provide the middle or other name(s) of the person, or their initial(s) if no other names apply.
Alias	Provide the name a person uses, or by which they are known, other than the name provided under surname, given name, or other/initial.
Name of entity	Provide the full name of the entity.

Instructions for the name fields

Address fields Provide the address details in the structured or unstructured fields (as applicable) as explained below.

Structured address fields Structured address fields include:

- Apartment/Room/Suite/Unit number
- House/Building number
- Street address
- City
- District
- Country
- Province or state (code) – For provinces or states in Canada, the United States or Mexico, select from the list of options.
- Province or state (name) – For provinces or states outside Canada, the United States or Mexico, provide the name of the province or state.
- Sub-province and/or sub-locality
- Postal or zip code

If you have the ability to separate the information

You must report it in the structured address fields.

For example, if a person lives at #10-123 Main Street, Richmond, British Columbia, Canada A1B 2C3, complete the address fields as follows:

Structured address fields	Information provided
Apartment/Room/Suite/Unit number	10

Structured address fields	Information provided
House/Building number	123
Street address	Main Street
City	Richmond
Country	Canada
Postal code	A1B 2C3

Example illustrating how to provide information if you have the ability to separate address information

If you are unable to separate the address information into the structured address fields

If, for example, your system groups the Apartment/Room/Suite/Unit number with the House/Building number and Street address, then provide:

- all the address information in the street address field
- the city, province, country and postal code in their respective fields

If there is no civic address

If a person or entity's address is in an area where there is **no civic address**, provide a description of the physical location.

For example, if a person lives in the third house to the right after the community center in Tinytown, Saskatchewan, Canada X1Y 2Z2, complete the address fields as follows:

Structured address fields	Information provided
Street address	Third house to the right after the community center
City	Tinytown
Province	SK
Country	Canada
Postal code	X1Y 2Z2

Example illustrating how to provide information if there is no civic address

Note: If you use the structured address fields, you **cannot** use the unstructured address fields to provide additional information.

Unstructured address field You should only use the unstructured address field when it is not possible to separate the address information. This typically occurs when you are uploading a large volume of reports and the data originates from outside your organization. For example, when you are in final receipt of an electronic funds transfer and the foreign address of the person who requested

the transfer information cannot be easily populated into the structured address fields.

If possible, enter information about the country in the Country field and provide the unstructured address information in the following format:

- street address/city/province or state/postal code or zip code

Invalid addresses The following **are not valid addresses**, and **should not** be provided in either the structured or unstructured address fields:

- a post office box without a complete physical address (for example, PO Box 333)
- general delivery address
- only a suite number (for example, Suite 256) without additional address information

A **legal land description** can be acceptable as long as the land description is specific enough to pinpoint the physical location of the client's address. If the legal land description refers to an area or a parcel of land on which multiple properties are located, the legal land description would not be sufficient.

Persons who are transient or have no fixed address For **persons who are transient** (for example, travelling in a recreational vehicle or temporarily working in a camp) and have **no fixed address**, you are required to provide the following information:

Type of person	What to provide
Canadian residents	Their permanent Canadian address, even if that is not where they are currently residing
Foreign clients travelling in Canada for a short period of time	Their foreign residential address
Foreign clients living in Canada for a longer period of time (such as a student)	The person's temporary Canadian address

Address information to provide for persons who are transient or have no fixed address

Occupation/business fields

Occupational/business fields	Instructions
Occupation	When entering occupation information, you should be as descriptive as possible. For example, if the person is:- a manager, provide the area of management, such as "hotel reservations manager" or "retail clothing store manager"- a consultant, provide the type of consulting, such as "IT consultant" or "forestry consultant"- a professional, provide the type of profession, such as "petroleum engineer" or "family physician"- a labourer, provide the type of labour performed, such as "road construction worker" or "landscape labourer"- not working, you should still be as descriptive as possible, and indicate "student," "unemployed," "retired," etc. You can enter a numeric classification code and the code title in this field (for example, NOC – National Occupational Classification). However, a numeric code on its own is not sufficient as you need a written description of the occupation as explained above.**Note**: If your client indicates that they are the manager of Blue Moon Auto Parts Ltd., you would enter "manager of auto parts company" in the occupation field and "Blue Moon Auto Parts Ltd." in the name of employer field as explained below.

Occupational/business fields	Instructions
Name of employer	Enter the name of the person's employer.Do not provide the name of a supervisor or manager.This field is meant to capture the name of the business that employs the person.If the person has multiple employers, you only need to provide one but it should be the person's primary employer. Providing the name of employer can augment the description of a person's occupation. For example, "retail clothing store manager for ABC high-end clothing store" and "retail clothing store manager for XYZ discount clothing store" are more descriptive than "retail clothing store manager" on its own.
Nature of entity's principal business	You should be as descriptive as possible when entering the entity's principal business.If the entity's principal business is "sales," provide the type of sales, such as "pharmaceutical sales" or "retail clothing sales." You can enter a numeric classification code **and** the code title in this field (for example, NAICS – North American Industry Classification System). However, a numeric code on its own is not sufficient, as you need a written description of the nature of the entity's principal business as explained above.

Instructions for the occupation/business fields

Identification fields

Identification fields	Instructions
Identifier type	Select the identifier type for the person or entity as applicable.If the identifier type is not listed, select "Other" and provide details.If you use the dual process method to identify a person, you must provide details of both sources of information in the identifier type fields. **Note**: Don't report a Social Insurance Number (SIN) to FINTRAC. In addition, you cannot use documentation for identification purposes where it is prohibited by provincial legislation.For more information on how to identify persons and entities, refer to:- FINTRAC's guidance on Methods to verify the identity of persons and entities
Number associated with identifier type	This is the number indicated on the identifier type that was used to verify the identity of the person or entity. For example, on a driver's licence, the licence number is the identification number and on a Certificate of Incorporation, the incorporation number is the identification number.
Jurisdiction of issue (country, province or state)	Provide the country, province, or state that issued the documentation used to identify the person or entity.

Type of jurisdiction	What and how to provide
A country	Enter that country as the jurisdiction of issue.
A province or state in Canada, the United States or Mexico	Select the province or state **code** from the list of options.
A province or state outside Canada, the United States or Mexico	Provide:- that province or state **name** as the jurisdiction of issue, and- the corresponding country information

How to provide the jurisdiction that issued the documentation used for identification |

Instructions for the identification fields

Telephone number fields

Location of telephone number	Instructions
Canada or the United States	Enter the area code and local number (for example, 999-999-9999).
Outside Canada or the United States	Enter the:- country code- city code, and- local number using a dash (-) to separate each oneFor example, “99-999-9999-9999” would indicate:- a 2-digit country code- a 3-digit city code, and- an 8-digit local number

Instructions for the telephone number fields

Specific field instructions

This section contains instructions for the report fields and are laid out in the same order as they appear on the Suspicious Transaction Report form.

Note: For some fields, the instructions:

- have not been provided and are indicated as “Instructions not specified”
- refer to the Standardized field instructions section

In this section

- General information
- Transaction information
- Starting action
- Completing action
- Details of suspicion
- Action taken

General information

Fields	Instructions
* **Reporting entity number**	You must enroll in FINTRAC Web Reporting System (FWR) to submit reports electronically.Provide the 7-digit identifier number assigned to you by FINTRAC at enrolment.
‡ **Reporting entity report reference number**	A number assigned to each **report** by:- you (the reporting entity), or- the individual or organization submitting the report on your behalfThis number must be **unique to your business, meaning it can only be used once**.

Instructions for the fields under "General information"

Which one of the following types of reporting entities best describes you?

Field	Instructions
* **Activity sector**	Enter your business activity sector.If you are involved in more than 1 type of business activity, indicate the one applicable to the transaction being reported.If there is more than 1 business activity for 1 or more transactions on the report, select only 1 to indicate your principal type of business activity.

Instructions for the question related to the type of reporting entities best describing you

Whom can FINTRAC contact about this report? Enter the contact information of the person you would like FINTRAC to liaise with in the event that a follow up is required.

You must ensure that all of your contacts' information is up to date in FINTRAC Web Reporting System (FWR) prior to submitting your report(s).

Report information

Fields	Instructions
Ministerial directive	If a transaction is being reported to FINTRAC under a ministerial directive, then indicate this by selecting the ministerial directive in the report.Leave this field blank if the transaction(s) are not part of a ministerial directive.**Note**:- Only **one** Ministerial Directive (IR2020) is available for a Suspicious Transaction report. If you select Ministerial Directive, then the report can only contain one transaction. This transaction must be a completed transaction that includes a starting and completing action. In addition, you **must not** complete the "Details of suspicion" and "Action taken" sections of the Suspicious Transaction Report form.- If a transaction is being reported to FINTRAC under a Ministerial Directive **and the transaction also meets the reasonable grounds to suspect threshold**, then you must submit two reports to FINTRAC. In the first report, select Ministerial Directive and do not complete the "Details of suspicion" and "Action taken" sections of the Suspicious Transaction Report form. In the second report, do not select Ministerial Directive but complete all applicable fields of the form, including the "Details of suspicion" and "Action taken" sections.

Instructions for the fields under "Report information"

Transaction information: Transaction 1 of X

Information about the transaction

Fields	Instructions
*** Was the transaction attempted?**	- Select yes if the transaction was attempted. - Select no if the transaction was completed.
†Reason transaction was not completed	If the transaction was not completed, provide the reason.
† Date of transaction	Enter the date of the transaction or attempted transaction. It cannot be a future date and must be different from the posting date.This field is **mandatory**, unless you:- are a financial entity, and - indicate that the transaction was a night deposit or a quick drop.If you do not provide the date of transaction in this field, you **must** provide the date of posting **if** different from date of transaction. Refer to the field Date of posting for more information.
Time of transaction	Enter the time of the transaction or attempted transaction and provide the time zone (that is, UTC offset) based on the location where the transaction or attempted transaction took place (for example, the location of where the cash was received). The time must be entered in the following format: HH:MM:SS±ZZ:ZZ. - For example, 1:25:06 pm in Ottawa, ON would be reported as 13:25:06-05:00.A report can contain multiple transactions that took place in different time zones.If you do not know the time of an attempted transaction, but you are aware of the approximate time frame of when the attempted transaction occurred, you can indicate this in the narrative section of the report (Details of suspicion)—for example, afternoon, morning, between 3 to 4 pm.

Fields	Instructions
*** Method of transaction**	Select the method that describes how the transaction occurred (example, the method that describes how you received the cash, funds, or virtual currency).If the method is not listed, select "Other."**Note**:- "Night deposit" and "quick drop" are **only applicable to financial entities**.- If you select either of these methods of transaction, you **will not be required** to complete the conductor information fields.
† If "Other," please specify	Provide a brief description of the method of transaction.
Date of posting (if different from date of transaction)	Enter the date the transaction is posted, if this differs from the date of the transaction. It cannot be a future date and it must be different from the transaction date.This field is **mandatory if**:- the transaction was a night deposit or quick drop and the date of transaction was not provided, or- the posting date differs from the transaction dateIn all other cases, this is a reasonable efforts field.
Time of posting (if different from the time of transaction)	Enter the time of posting, if this differs from of the time of the transaction.The time must be entered in the following format: HH:MM:SS±ZZ:ZZ. - For example, 1:25:06 pm in Ottawa, ON would be reported as 13:25:06-05:00.
‡ Reporting entity transaction reference number	This is a unique number assigned to **each transaction** by:- you (the reporting entity), or- the individual or organization submitting the report on your behalf

Fields	Instructions
Purpose of transaction	This is the reason for the transaction. The **bolded text** below are examples of purpose of transaction:- A client brings cash tips from his job as a server for deposit into his bank account to **save for the purchase of a home**.- A client purchases jewellery that will be **a gift for a friend**.- A client exchanges Canadian dollars (CAD) to British pound sterlings (GBP) for **vacation purposes**.- A client brings purchases a bank draft in order to **buy a boat**.You may be able to determine the purpose of a transaction by asking the client.

Instructions for the fields under "Information about the transaction"

Information about where the transaction was conducted or attempted
Provide information about the physical location where the transaction took place or was attempted.

For example, if the transaction was conducted at:

- a branch, provide the reporting entity location number of that branch
- an automated teller machine (ATM), provide the reporting entity location number of that ATM

For the following situations, provide the **location number of where the transaction was processed** – this could be a branch location or a head office location, depending on your business process:

- There is no physical location (for instance, the transaction was conducted online).
- The location where the transaction occurred does not belong to your business (for instance the location of a white label ATM that you do not own).

Note:

- Information about a location that does not belong to your business can be provided in the narrative section of the Suspicious Transaction Report.

Field	Instructions
*** Reporting entity location number**	This represents information about where the transaction took place. For example, if the client deposited cash at Branch 1, then select the location number that is associated with Branch 1.If the client conducts a transaction online, then select the location number that is associated with the location that processes the client's online instructions – this could be a branch location or head office location, depending on your business process. The location number is:- created and assigned to you by FINTRAC during the enrolment process to FINTRAC Web Reporting System (FWR), and- maintained by your FWR administrator.For more information about this, contact your FWR administrator.

Instructions for the field under "Information about where the transaction was conducted or attempted"

Starting action Provide information about how the transaction was started.

Fields	Instructions
‡ Direction of Starting Action (In /Out)	Indicate the direction of the starting action as either **in** or **out** for the funds, assets or virtual currency involved. - The direction of the starting action is **in** when a client physically brings in or electronically transfers in funds, assets or virtual currency to your business to start a transaction. - The direction of the starting action is **out** when your client requests to start a transaction with funds, assets or virtual currency already held by or deposited at your business.

Fields	Instructions
‡ Type of funds, assets or virtual currency (In/Out	If the direction of the starting action is **in**, select one of the following based on what the client brought or transferred in to start the transaction:- **Bank draft** – To be used when the client brings in a bank draft to start a transaction. The term bank draft refers to a negotiable instrument that can be used as payment (similar to a cheque). Unlike a cheque though, a bank draft is guaranteed by the issuing bank.- **Cash** – To be used when the client brings in coins or bank notes that are intended for circulation in Canada or coins or bank notes of countries other than Canada to start a transaction.- **Casino product** – To be used when the client brings in chips, plaques, tokens or other casino products to start a transaction.- **Cheque** – To be used when the client brings in a cheque, including personal, certified and casino cheques, to start a transaction. - **Domestic funds transfer** – To be used when the starting action involves the final receipt of funds from within Canada. This includes transfers within the same organization where funds are transferred from one account to another account.- **Email money transfer (EMT)** – To be used when the starting action involves an incoming email transfer using the recipient's email address.- **International funds transfer** – To be used when the starting action involves the final receipt of funds from outside Canada. - **Investment product** – To be used when the starting action involves an incoming transfer of an investment product (for example, transfer of shares from one investment account to another).- **Jewellery** – To be used when the client brings in jewellery to start a transaction. Jewellery means objects made of precious metals, precious stones or pearls that are intended for personal adornment.- **Mobile money transfer** – To be used when the starting action involves an

Fields	Instructions
† If "Other," please specify	Provide a description of the type of funds, assets for virtual currency.
*** Amount**	Enter the total amount of funds, assets or virtual currency involved in the starting action.If this amount **was not** in Canadian dollars (CAD), do not convert it to CAD but provide the currency or virtual currency type in the next field.
† Currency / † Virtual currency type	Enter the fiat currency (including if it was in Canadian dollars) **or** virtual currency of the starting action. If the currency **or** virtual currency type is not in the lists provided, you must select "Other" and provide the full name of the currency.
† If "Other," please specify	If "Other", provide the full name of the currency or virtual currency type.
Exchange rate	Provide the rate of exchange that you used for the transaction. This can be an exchange rate for fiat currency or virtual currency.
† Virtual currency transaction identifier	This is a unique identifier.It is commonly represented by a hash consisting of mixed numerical and alphabetical characters.
† Sending virtual currency address	The sending virtual currency address is made up of a number of alpha-numeric characters. The address length is determined by the type of virtual currency used in the transaction. The sending virtual currency address is associated with whoever is sending the virtual currency (typically the conductor).

Fields	Instructions
† Receiving virtual currency address	The receiving virtual currency address is made up of a number of alpha-numeric characters.The address length is determined by the type of virtual currency used in the transaction.The receiving virtual currency address is associated with whoever is receiving the virtual currency (typically the beneficiary)
† Reference number	If the transaction involved a reference number, provide it in this field.If the transaction involves an account at a **financial entity**, **securities dealer** or **casino**, **do not** provide the account number information in this field **.** The account number must be provided in the Account number field.For all other reporting entities, if you have an internal account number that is used as a reference number, then provide the internal account number in this field.
Other number related to reference number	Provide any other number related to the reference number as applicable.
† Financial institution number	Provide the financial institution number of the account from which the transaction initiated.
† Branch number	Provide the branch number of the account from which the transaction is initiated.
† Account number	If the transaction involves an account at a **financial entity**, **securities dealer** or **casino**, provide the account number. If you are not an account-based reporting entity (for example, a money services business), but the transaction involves an account at an account-based reporting entity (for example, a financial entity), provide that account number in this field.

Fields	Instructions
† Account type	Provide the account typeIf the account type is not in the list provided, you must select “Other” and provide the account type.
† If “Other,” please specify	If “Other” is selected, you must provide the account type.
† Account currency	Provide the account currency (fiat) type code.Currencies are represented both numerically and alphabetically, using either three digits or three letters.If the account currency type code can not be found, you must select “Other” and provide the currency (fiat) type.
† Account virtual currency type	Provide the account virtual currency type.If the account virtual currency type is not in the list provided, you must select “Other” and provide the account virtual currency type.
† If “Other,” please specify	If “Other” is selected, you must provide the account currency (fiat) type or account virtual currency type.
Date account opened	Provide the date the account was opened.
Date account closed	Provide the date the account was closed.
† Status of account at time of transaction	Provide the status of the account at the time of the transaction (e.g. active, inactive, dormant, closed).
How were the funds or virtual currency obtained?	This is how the conductor initially acquired the funds or virtual currency used for the transaction, **not** where the funds or virtual currency may have been transferred from.For example, you can obtain funds or virtual currency from activities such as:- employment- sale of a large asset, and- giftsThis information must be reported if obtained.

Fields	Instructions
‡ Was information about the source (person/entity) of funds or virtual currency obtained?	This field is a "Yes/No" question.**Select "Yes"** if you have:- the name of any person or entity that is the source of the funds or virtual currency- their account number or policy number, or- an identifying number if there is no account number or policy numberOtherwise, **select "No"** to indicate that you do not have the information.

Instructions for the fields under "Starting action 1 of Y of transaction X"

Account holder Person

Fields	Instructions
† Surname	Refer to Name fields under "Standardized field instructions".
† Given name	Same instructions (Name fields)
Other/initial	Same instructions (Name fields)

Instructions for the fields under "Person 1 of N starting action Z"

Entity

Fields	Instructions
† Name of entity	Refer to Name fields under "Standardized field instructions".

Instructions for the fields under "Entity 1 of N starting action Z"

Source of funds or virtual currency If you have information on any source of funds or virtual currency involved in the transaction, you must report it.

If there are multiple sources, you must provide information for each source.

Person

Fields	Instructions
† Surname	Refer to Name fields under "Standardized field instructions".
† Given name	Same instructions (Name fields)
Other/initial	Same instructions (Name fields)
Account number	Provide the account number for the source of funds.It is acceptable to include the financial institution number and branch number as part of an account number.
Policy number	Instructions not specified
Identifying number	If there is no account or policy number, provide an identifying number if available.

Instructions for the fields under "Person 1 of N of starting action Y"

Entity

Fields	Instructions
† Name of entity	Refer to Name fields under "Standardized field instructions".
Account number	Provide the account number for the source of funds.It is acceptable to include the financial institution number and branch number as part of an account number.
Policy number	Instructions not specified
Identifying number	If there is no account or policy number, provide an identifying number if available.

Instructions for the fields under "Entity 1 of N of starting action Y"

Note about source of funds or virtual currency fields Although the following fields are about how the conductor obtained the funds or virtual currency, they are different:

- How were the funds or virtual currency obtained?
- Was information about the source (person/entity) of funds or virtual currency obtained?
- Source of funds or virtual currency – person or entity

The following example demonstrates the differences.

Example :

Vicky Violet brings in $12,000 cash for deposit into her bank account and tells the bank that she obtained this cash when she sold her car to Griffin Grey.

She was only able to provide Griffin Grey's name to the bank because she did not have information on his account number, policy number or identifying number.

As such, the source of funds or virtual currency fields would be completed as follows:

Source of funds fields	Information provided in t
How were the funds obtained?	**Sale of car**
Was information about the source (person / entity) of funds obtained?	**Yes**
Source of funds	**Griffin Grey**

How the source of funds fields would be completed for this example

Conductor information

Field	Instructions
‡ Have you obtained any conductor information related to this transaction or attempted transaction?	This field is a "Yes/No" question."No" should only be selected if the conductor is **not** your client, **and** after taking reasonable measures, you were not able to obtain **any** conductor details.

Instructions for the fields under "Conductor – indicator"

Fields	Instructions
Surname	Refer to Name fields under "Standardized field instructions".
Given name	Same instructions (Name fields)
Other/Initial	Same instructions (Name fields)
Alias	Same instructions (Name fields)
Client number	A unique identifying number assigned by the reporting entity to the person conducting the transaction.
Apartment/Room/Suite/Unit number	Refer to Address fields under "Standardized field instructions".
House/Building number	Same instructions (Address fields)
Street address	Same instructions (Address fields)

Fields	Instructions
City	Same instructions (Address fields)
District	Same instructions (Address fields)
Country	Same instructions (Address fields)
Province or state	Same instructions (Address fields)
Sub-province and/or sub-locality	Same instructions (Address fields)
Postal or zip code	Same instructions (Address fields)
Unstructured address details	Refer to Unstructured address field under "Standardized field instructions".
Telephone number	Refer to Telephone number fields under "Standardized field instructions".
Extension	Same instructions (Telephone number fields)
Email address	Instructions not specified
URL	Enter the uniform resource location, commonly known as the web address, for the conductor. This includes the URL for personal or business websites, blogs and any social media. If the conductor has more than one URL, provide the main URL in this field and the others in the Details of suspicion section. The URL does not include handles which can be included in the Details of suspicion section.
Date of birth	Instructions not specified
Country of residence	Enter the primary country of residence for the person.It can be the same or different from the country entered in the address section.
Country of citizenship	Enter the primary country of citizenship for the person. It can be same or different from the country entered into the address section.
Occupation	Refer to Occupation/business fields under "Standardized field instructions".
Name of employer	Same instructions (Occupation/business fields)

Instructions for the fields under “Person 1of A of starting action Y”

Fields	Instructions
Apartment/Room/Suite/Unit number	Refer to Address fields under “Standardized field instructions”.
House/Building number	Same instructions (Address fields)
Street address	Same instructions (Address fields)
City	Same instructions (Address fields)
District	Same instructions (Address fields)
Country	Same instructions (Address fields)
Province or state	Same instructions (Address fields)
Sub-province and/or sub-locality	Same instructions (Address fields)
Postal or zip code	Same instructions (Address fields)
Unstructured address details	Refer to Unstructured address field under “Standardized field instructions”.
Telephone number	Refer to Telephone number fields under “Standardized field instructions”.
Extension	Same instructions (Telephone number fields)

Instructions for the fields under “Information about the employer’s address”

Identification of the person

Fields	Instructions
Identifier type	Refer to Identification fields under “Standardized field instructions”.
† If “Other”, please specify	If “Other” identifier type is selected, you must specify the identifier type.
Number associated with identifier type	Same instructions (Identification fields)
Jurisdiction of issue (country)	Same instructions (Identification fields)
Jurisdiction of issue (province or state)	Same instructions (Identification fields)

Instructions for the fields under “Identification of 1 of N of person conductor A”

Fields	Instructions
Type of device used	Provide the type of device used.If "Other" type of device used is selected, you must specify the type of device used.
† If "Other", please specify	If "Other" type of device used is selected, you must specify the type of device used.
Username	A username is how a person or an entity refers to themselves online.
Device identifier number	The device identifier number is a number assigned to the device, such as a Media Access Control (MAC) address or International Mobile Equipment Identity (IMEI) number.
Internet protocol address	Provide the Internet Protocol (IP) address.It is the unique identifying number assigned to every device connected to the internet.
Date and time of online session in which request was made	This is the date and time the conductor accessed the online environment where the transaction was requested.

Instructions for the fields under "Information about conducting or attempting to conduct the transaction online"

Conductor – Entity Provide all the information you have on one, or multiple entities specified as the conductors of the transaction.

Fields	Instructions
Name of entity	Refer to Name fields under "Standardized field instructions".
Client number	A unique identifying number assigned by the reporting entity to the entity conducting the transaction.
Apartment/Room/Suite/Unit number	Refer to Address fields under "Standardized field instructions".
House/Building number	Same instructions (Address fields)
Street address	Same instructions (Address fields)
City	Same instructions (Address fields)
District	Same instructions (Address fields)

Fields	Instructions
Country	Same instructions (Address fields)
Province or state	Same instructions (Address fields)
Sub-province and/or sub-locality	Same instructions (Address fields)
Postal or zip code	Same instructions (Address fields)
Unstructured address details	Refer to Unstructured address field "Standardized field instructions".
Telephone number	Refer to Telephone number fields under "Standardized field instructions".
Extension	Same instructions (Telephone number fields)
Email address	Instructions not specified
URL	Enter the uniform resource location, commonly known as the web address, for the conductor. This includes the URL for personal or business websites, blogs and any social media. If the conductor has more than one URL, provide the main URL in this field and the others in the Details of suspicion section. The URL does not include handles which can be included in the Details of suspicion section.

Instructions for the fields under "Entity 1 of A starting action Y"

Fields	Instructions
Entity structure / type	Provide the entity ownership structure type:- Corporation- Trust- Widely held or publicly traded trust, or - Entity other than a corporation or trust
If "Entity other than a corporation or trust" is selected, please specify	If "Entity other than a corporation or trust" is selected, provide specification.
Nature of entity's principal business	Refer to Occupation/business fields under "Standardized field instructions".

Fields	Instructions
Is the entity registered or incorporated?	This field is a "Yes/No" question.Indicate whether entity is registered or incorporated

Information respecting the structure of Entity 1 of N of entity conductor A

Incorporation of the entity

Fields	Instructions
Incorporation number	Provide the incorporation number of the entity conducting the transaction for each jurisdiction where the entity is incorporated.
Jurisdiction of issue (country) of incorporation	Provide the country that issued the documentation used to identify the entity for each jurisdiction where the entity is incorporated.
Jurisdiction of issue (province or state) of incorporation	Provide the jurisdiction of issue (province or state) of incorporation for each jurisdiction where the entity is incorporatedIf the jurisdiction is a province or state **in** Canada, the United States or Mexico, **select the code from the list of options.**If the jurisdiction is **outside** Canada, the United States or Mexico, **provide the name of the province or state.**

Information under Incorporation 1 of N of entity conductor A

Registration of the entity

Fields	Instructions
Registration number	Provide the registration number of the entity conducting the transaction for each jurisdiction where the entity is registered.For Canadian entities, a registration number can include the 9-digit business number assigned to that entity by the Canadian Revenue Agency (CRA)
Jurisdiction of issue (country) of registration	Provide the country that issued the documentation for each jurisdiction where the entity is registered.
Jurisdiction of issue (province or state) of registration	Provide the jurisdiction of issue (province or state) for each jurisdiction where the entity is registeredIf the jurisdiction is a province or state **in** Canada, the United States or Mexico, **select the code from the list of options.**If the jurisdiction is **outside** Canada, the United States or Mexico, **provide the name of the province or state.**

Registration 1 of N of entity conductor A

Identification of the entity Provide the following information that was used to verify the identity of the entity. For some entities, this information may be the same as the registration or incorporation information.

Fields	Instructions
Identifier type	Refer to Identification fields under "Standardized field instructions".
† If "Other", please specify	If "Other" identifier type is selected, you must specify the identifier type.
Number associated with identifier type	Same instructions (Identification fields)
Jurisdiction of issue (country)	Same instructions (Identification fields)
Jurisdiction of issue (province or state)	Same instructions (Identification fields)

Instructions for the fields under "Identification 1 of N of entity conductor A"

Person authorized to bind the entity or act with respect to the account (maximum 3) If the conductor is an entity, you must provide the information for **up to 3 persons** who are authorized to:

- bind the entity, or
- act with respect to the account

Fields	Instructions
Surname	Refer to Name fields under "Standardized field instructions".
Given name	Same instructions (Name fields)
Other/Initial	Same instructions (Name fields)

Instructions for the fields under "Person 1 of N (max 3)"

Entity Structure/Type: Corporate Information

Director(s) of a corporation

Fields	Instructions
Surname	Refer to Name fields under "Standardized field instructions".
Given name	Same instructions (Name fields)
Other/Initial	Same instructions (Name fields)
Apartment/Room/Suite/Unit number	Refer to Address fields under "Standardized field instructions".
House/Building number	Same instructions (Address fields)
Street address	Same instructions (Address fields)
City	Same instructions (Address fields)
District	Same instructions (Address fields)
Country	Same instructions (Address fields)
Province or state	Same instructions (Address fields)
Sub-province and/or sub-locality	Same instructions (Address fields)
Postal or zip code	Same instructions (Address fields)
Unstructured address details	Refer to Unstructured address field under "Standardized field instructions".
Telephone number	Refer to Telephone number fields under "Standardized field instructions".
Extension	Same instructions (Telephone number fields)

Instructions for the fields under "Director 1 of N of starting action Y"

Person who directly or indirectly owns or controls 25% or more shares of the corporation

Fields	Instructions
Surname	Refer to Name fields under "Standardized field instructions".
Given name	Same instructions (Name fields)
Other/Initial	Same instructions (Name fields)

Instructions for the fields under "Person 1 of N of starting action Y"

Trust Information Trustee(s) of a trust

Fields	Instructions
Surname	Refer to Name fields under "Standardized field instructions".
Given name	Same instructions (Name fields)
Other/Initial	Same instructions (Name fields)
Apartment/Room/Suite/Unit number	Refer to Address fields under "Standardized field instructions".
House/Building number	Same instructions (Address fields)
Street address	Same instructions (Address fields)
City	Same instructions (Address fields)
District	Same instructions (Address fields)
Country	Same instructions (Address fields)
Province or state	Same instructions (Address fields)
Sub-province and/or sub-locality	Same instructions (Address fields)
Postal or zip code	Same instructions (Address fields)
Unstructured address details	Refer to Unstructured address field under "Standardized field instructions".
Telephone number	Refer to Telephone number fields under "Standardized field instructions".
Extension	Same instructions (Telephone number fields)

Instructions for the fields under "Trustee 1 of N of starting action Y"

Settlor(s) of a trust

Fields	Instructions
Surname	Refer to Name fields under "Standardized field instructions".
Given name	Same instructions (Name fields)
Other/Initial	Same instructions (Name fields)
Apartment/Room/Suite/Unit number	Refer to Address fields under "Standardized field instructions".
House/Building number	Same instructions (Address fields)
Street address	Same instructions (Address fields)
City	Same instructions (Address fields)
District	Same instructions (Address fields)
Country	Same instructions (Address fields)
Province or state	Same instructions (Address fields)
Sub-province and/or sub-locality	Same instructions (Address fields)
Postal or zip code	Same instructions (Address fields)
Unstructured address details	Refer to Unstructured address field under "Standardized field instructions".
Telephone number	Refer to Telephone number fields under "Standardized field instructions".
Extension	Same instructions (Telephone number fields)

Instructions for the fields under "Settlor 1 of N of starting action Y"

Widely held or publicly traded trust information Person who directly or indirectly owns or controls 25% or more units of a widely held or publicly traded trust

Fields	Instructions
Surname	Refer to Name fields under "Standardized field instructions".
Given name	Same instructions (Name fields)
Other/Initial	Same instructions (Name fields)
Apartment/Room/Suite/Unit number	Refer to Address fields under "Standardized field instructions".
House/Building number	Same instructions (Address fields)
Street address	Same instructions (Address fields)
City	Same instructions (Address fields)
District	Same instructions (Address fields)
Country	Same instructions (Address fields)

Fields	Instructions
Province or state	Same instructions (Address fields)
Sub-province and/or sub-locality	Same instructions (Address fields)
Postal or zip code	Same instructions (Address fields)
Unstructured address details	Refer to Unstructured address field under "Standardized field instructions".
Telephone number	Refer to Telephone number fields under "Standardized field instructions".
Extension	Same instructions (Telephone number fields)

Instructions for the fields under "Person 1 of N of starting action Y"

Beneficiary(ies) of a trust, other than a widely held or publicly traded trust

Fields	Instructions
Surname	Refer to Name fields under "Standardized field instructions".
Given name	Same instructions (Name fields)
Other/Initial	Same instructions (Name fields)
Apartment/Room/Suite/Unit number	Refer to Address fields under "Standardized field instructions".
House/Building number	Same instructions (Address fields)
Street address	Same instructions (Address fields)
City	Same instructions (Address fields)
District	Same instructions (Address fields)
Country	Same instructions (Address fields)
Province or state	Same instructions (Address fields)
Sub-province and/or sub-locality	Same instructions (Address fields)
Postal or zip code	Same instructions (Address fields)
Unstructured address details	Refer to Unstructured address field under "Standardized field instructions".
Telephone number	Refer to Telephone number fields under "Standardized field instructions".
Extension	Same instructions (Telephone number fields)

Instructions for the fields under “Beneficiary 1 of N of starting action Y”

Entity other than a corporation or trust information Person who directly or indirectly owns or controls 25% or more of an entity other than a corporation or trust

Fields	Instructions
Surname	Refer to Name fields under “Standardized field instructions”.
Given name	Same instructions (Name fields)
Other/Initial	Same instructions (Name fields)

Instructions for the fields under “Person 1 of N of starting action Y”

Fields	Instructions
Type of device used	Provide the type of device used.If “Other” type of device used is selected, you must specify the type of device used.
† If “Other”, please specify	If “Other” type of device used is selected, you must specify the type of device used.
Username	A username is how a person or an entity refers to themselves online.
Device identifier number	The device identifier number is a number assigned to the device, such as a Media Access Control (MAC) address or International Mobile Equipment Identity (IMEI) number.
Internet protocol address	Provide the Internet Protocol (IP) address.It is the unique identifying number assigned to every device connected to the internet.
Date and time of online session in which request was made	This is the date and time the conductor accessed the online environment where the transaction was requested.

Instructions for the fields under “Information about conducting or attempting to conduct the transaction online”

On behalf of On behalf of indicator

Field	Instructions
‡ Was this transaction conducted or attempted on behalf of another person or entity?	This field is a "Yes/No" question.Select "Yes" if the transaction was conducted on behalf of another person or entity.The "on behalf of" party is also known as:- the "third party", or- the party providing instructions for the transaction**If the transaction was conducted on behalf of another person, you must include the relevant information below.**

Instructions for the field under "On behalf of indicator"

Fields	Instructions
Surname	Refer to Name fields under "Standardized field instructions".
Given name	Same instructions (Name fields)
Other/Initial	Same instructions (Name fields)
Alias	Same instructions (Name fields)
Client number	Instructions not specified
Apartment/Room/Suite/Unit number	Refer to Address fields under "Standardized field instructions".
House/Building number	Same instructions (Address fields)
Street address	Same instructions (Address fields)
City	Same instructions (Address fields)
District	Same instructions (Address fields)
Country	Same instructions (Address fields)
Province or state	Same instructions (Address fields)
Sub-province and/or sub-locality	Same instructions (Address fields)
Postal or zip code	Same instructions (Address fields)
Unstructured address details	Refer to Unstructured address field under "Standardized field instructions".
Telephone number	Refer to Telephone number fields under "Standardized field instructions".
Extension	Same instructions (Telephone number fields)

Fields	Instructions
URL	Enter the uniform resource location, commonly known as the web address, for the conductor. This includes the URL for personal or business websites, blogs and any social media. If the conductor has more than one URL, provide the main URL in this field and the others in the Details of suspicion section. The URL does not include handles which can be included in the Details of suspicion section.
Email address	Instructions not specified
Date of birth	Instructions not specified
Country of residence	Enter the primary country of residence for the person.It can be the same or different from the country entered in the address section.
Country of citizenship	Enter the primary country of citizenship for the person. It can be same or different from the country entered into the address section.
Occupation	Refer to Occupation/business fields under "Standardized field instructions".
Name of employer	Same instructions (Occupation/business fields)

Instructions for the fields under "Person 1 of B of conductor A"

Fields	Instructions
Apartment/Room/Suite/Unit number	Refer to Address fields under "Standardized field instructions".
House/Building number	Same instructions (Address fields)
Street address	Same instructions (Address fields)
City	Same instructions (Address fields)
District	Same instructions (Address fields)
Country	Same instructions (Address fields)
Province or state	Same instructions (Address fields)
Sub-province and/or sub-locality	Same instructions (Address fields)
Postal or zip code	Same instructions (Address fields)

Fields	Instructions
Unstructured address details	Refer to Unstructured address field under "Standardized field instructions".
Telephone number	Refer to Telephone number fields under "Standardized field instructions".
Extension	Same instructions (Telephone number fields)

Instructions for the fields under "Information about the employer's address"

Identification of person on whose behalf the transaction was conducted

Fields	Instructions
Identifier type	Refer to Identification fields under "Standardized field instructions".
† If "Other", please specify	If "Other" identifier type is selected, you must specify the identifier type.
Number associated with identifier type	Same instructions (Identification fields)
Jurisdiction of issue (country)	Same instructions (Identification fields)
Jurisdiction of issue (province or state)	Same instructions (Identification fields)

Instructions for the fields under "Identification 1 of N on behalf of person B"

Fields	Instructions
Type of device used	Provide the type of device used.If "Other" type of device used is selected, you must specify the type of device used.
† If "Other". Please specify	If "Other" is selected, specify the type of device used.
Username	A username is how a person or an entity refers to themselves online.
Device identifier number	The device identifier number is a number assigned to the device, such as a Media Access Control (MAC) address or International Mobile Equipment Identity (IMEI) number.

Fields	Instructions
Internet protocol address	Provide the Internet Protocol (IP) address.It is the unique identifying number assigned to every device connected to the internet.
Date and time of online session in which request was made	This is the date and time the conductor accessed the online environment where the transaction was requested.

Instructions for the fields under "Information about conducting or attempting to conduct the transaction online"

Fields	Instructions
Relationship	Select the relationship of the "on behalf of" party to the person or entity conducting the transaction.The "on behalf of" party is understood to be the person or entity that instructs the person or entity conducting the transaction.
† If "Other", please specify	If "Other" is selected, specify the relationship of the "on behalf of" party to the person or entity conducting the transaction.

Instructions for the fields under "Relationship of the person named above to the person or entity conducting or attempting to conduct the transaction"

If the transaction was conducted on behalf of another entity, you must include the relevant information.

Fields	Instructions
Name of entity	Refer to Identification fields under "Standardized field instructions".
Client number	Instructions not specified
Apartment/Room/Suite/Unit number	Refer to Address fields under "Standardized field instructions".
House/Building number	Same instructions (Address fields)
Street address	Same instructions (Address fields)
City	Same instructions (Address fields)
District	Same instructions (Address fields)

Fields	Instructions
Country	Same instructions (Address fields)
Province or state	Same instructions (Address fields)
Sub-province and/or sub-locality	Same instructions (Address fields)
Postal or zip code	Same instructions (Address fields)
Unstructured address details	Refer to Unstructured address field under "Standardized field instructions".
Telephone number	Refer to Telephone number fields under "Standardized field instructions".
Extension	Same instructions (Telephone number fields)
Email address	Instructions not specified
URL	Enter the uniform resource location, commonly known as the web address, for the conductor. This includes the URL for personal or business websites, blogs and any social media. If the conductor has more than one URL, provide the main URL in this field and the others in the Details of suspicion section. The URL does not include handles which can be included in the Details of suspicion section.

Instructions for the fields under "Entity 1 of B of conductor A"

Fields	Instructions
Entity structure / type	Provide the entity ownership structure type:- Corporation- Trust- Widely held or publicly traded trust, or - Entity other than a corporation or trust
If "Entity other than a corporation or trust" is selected, please specify	If "Entity other than a corporation or trust" is selected, provide specification.
Nature of entity's principal business	Refer to Occupation/business fields under "Standardized field instructions".

Fields	Instructions
‡Do you have incorporation or registration information?	This field is a "Yes/No" question.Select "Yes" if you have the information.Select 'No' if you do not have the information.
Incorporated or registered?	Provide the incorporation or registration type:- Incorporated- Registered- Incorporated and registered, or - Unknown

Instructions for the fields under "Information respecting the structure of Entity 1 of B"

Incorporation of the entity

Fields	Instructions
Incorporation number	Provide the incorporation number of the entity conducting the transaction for each jurisdiction where the entity is incorporated.
Jurisdiction of issue (country) of incorporation	Provide the country that issued the documentation used to identify the entity for each jurisdiction where the entity is incorporated.
Jurisdiction of issue (province or state) of incorporation	Provide the jurisdiction of issue (province or state) of incorporation for each jurisdiction where the entity is incorporatedIf the jurisdiction is a province or state **in** Canada, the United States or Mexico, **select the code from the list of options.**If the jurisdiction is **outside** Canada, the United States or Mexico, **provide the name of the province or state.**

Instructions for fields under "Incorporation 1 of N of entity B"

Registration of the entity

Fields	Instructions
Registration number	Provide the registration of the entity conducting the transaction For Canadian entities, a registration number can include the 9-digit business number assigned to that entity by the Canada Revenue Agency (CRA).
Jurisdiction of issue (country) of registration	Provide the country that issued the documentation for each jurisdiction where the entity is registered.
Jurisdiction of issue (province or state) of registration	Provide the jurisdiction of issue (province or state) for each jurisdiction where the entity is registeredIf the jurisdiction is a province or state **in** Canada, the United States or Mexico, **select the code from the list of options.**If the jurisdiction is **outside** Canada, the United States or Mexico, **provide the name of the province or state.**

Instructions for fields under "Registration 1 of N of entity B"

Identification of the entity on whose behalf the transaction was conducted Provide the following information that was used to verify the identity of the entity on whose behalf the transaction was conducted.

For some entities, this information may be the same as the registration or incorporation information.

Fields	Instructions
Identifier type	Refer to Identification fields under "Standardized field instructions".
† If "Other", please specify	If "Other" identifier type is selected, you must specify the identifier type.
Number associated with identifier type	Same instructions (Identification fields)
Jurisdiction of issue (country)	Same instructions (Identification fields)
Jurisdiction of issue (province or state)	Same instructions (Identification fields)

Instructions for the fields under “Identification 1 of N on behalf of entity B”

Person authorized to bind the entity or act with respect to the account (maximum 3)

Fields	Instructions
Surname	Refer to Name fields under “Standardized field instructions”.
Given name	Same instructions (Name fields)
Other/Initial	Same instructions (Name fields)

Instructions for the fields under “Person 1 of N (max.3)”

Beneficial Ownership information (Entity structure / type) Corporate information: Directors of a corporation

Fields	Instructions
Surname	Refer to Identification fields under “Standardized field instructions”.
Given Name	Same instructions (Identification fields)
Other/Initial	Same instructions (Identification fields)
Apartment/Room/Suite/Unit number	Refer to Address fields under “Standardized field instructions”.
House/Building number	Same instructions (Address fields)
Street address	Same instructions (Address fields)
City	Same instructions (Address fields)
District	Same instructions (Address fields)
Country	Same instructions (Address fields)
Province or state	Same instructions (Address fields)
Sub-province and/or sub-locality	Same instructions (Address fields)
Postal or zip code	Same instructions (Address fields)
Unstructured address details	Refer to Unstructured address field under “Standardized field instructions”.
Telephone number	Refer to Telephone number fields under “Standardized field instructions”.
Extension	Same instructions (Telephone number fields)

Instructions for the fields under “Director 1 of N of starting action Y”

Person who directly or indirectly owns or controls 25% or more shares of the corporation

Fields	Instructions
Surname	Refer to Identification fields under "Standardized field instructions".
Given Name	Same instructions (Identification fields)
Other/Initial	Same instructions (Identification fields)

Instructions for the fields under "Person 1 of N of starting action Y"

Trust Information Trustee(s) of a trust

Fields	Instructions
Surname	Refer to Identification fields under "Standardized field instructions".
Given Name	Same instructions (Identification fields)
Other/Initial	Same instructions (Identification fields)
Apartment/Room/Suite/Unit number	Refer to Address fields under "Standardized field instructions".
House/Building number	Same instructions (Address fields)
Street address	Same instructions (Address fields)
City	Same instructions (Address fields)
District	Same instructions (Address fields)
Country	Same instructions (Address fields)
Province or state	Same instructions (Address fields)
Sub-province and/or sub-locality	Same instructions (Address fields)
Postal or zip code	Same instructions (Address fields)
Unstructured address details	Refer to Unstructured address field under "Standardized field instructions".
Telephone number	Refer to Telephone number fields under "Standardized field instructions".
Extension	Same instructions (Telephone number fields)

Instructions for the fields under "Trustee 1 of N of starting action Y"

Settlor(s) of a trust

Fields	Instructions
Surname	Refer to Identification fields under "Standardized field instructions".
Given Name	Same instructions (Identification fields)
Other/Initial	Same instructions (Identification fields)
Apartment/Room/Suite/Unit number	Refer to Address fields under "Standardized field instructions".
House/Building number	Same instructions (Address fields)
Street address	Same instructions (Address fields)
City	Same instructions (Address fields)
District	Same instructions (Address fields)
Country	Same instructions (Address fields)
Province or state	Same instructions (Address fields)
Sub-province and/or sub-locality	Same instructions (Address fields)
Postal or zip code	Same instructions (Address fields)
Unstructured address details	Refer to Unstructured address field under "Standardized field instructions".
Telephone number	Refer to Telephone number fields under "Standardized field instructions".
Extension	Same instructions (Telephone number fields)

Instructions for the fields under "Settlor 1 of N of starting action Y"

Widely held or publicly traded trust information Person who directly or indirectly owns or controls 25% or more units of a widely held or publicly traded trust.

Fields	Instructions
Surname	Refer to Identification fields under "Standardized field instructions".
Given Name	Same instructions (Identification fields)
Other/Initial	Same instructions (Identification fields)

Fields	Instructions
Apartment/Room/Suite/Unit number	Refer to Address fields under "Standardized field instructions".
House/Building number	Same instructions (Address fields)
Street address	Same instructions (Address fields)
City	Same instructions (Address fields)
District	Same instructions (Address fields)
Country	Same instructions (Address fields)
Province or state	Same instructions (Address fields)
Sub-province and/or sub-locality	Same instructions (Address fields)
Postal or zip code	Same instructions (Address fields)
Unstructured address details	Refer to Unstructured address field under "Standardized field instructions".
Telephone number	Refer to Telephone number fields under "Standardized field instructions".
Extension	Same instructions (Telephone number fields)

Instructions for the fields under "Person 1 of N of starting action Y"

Beneficiary(s) of a trust, other than a widely held or publicly traded trust

Fields	Instructions
Surname	Refer to Identification fields under "Standardized field instructions".
Given Name	Same instructions (Identification fields)
Other/Initial	Same instructions (Identification fields)
Apartment/Room/Suite/Unit number	Refer to Address fields under "Standardized field instructions".
House/Building number	Same instructions (Address fields)
Street address	Same instructions (Address fields)
City	Same instructions (Address fields)
District	Same instructions (Address fields)
Country	Same instructions (Address fields)
Province or state	Same instructions (Address fields)
Sub-province and/or sub-locality	Same instructions (Address fields)

Fields	Instructions
Postal or zip code	Same instructions (Address fields)
Unstructured address details	Refer to Unstructured address field under "Standardized field instructions".
Telephone number	Refer to Telephone number fields under "Standardized field instructions".
Extension	Same instructions (Telephone number fields)

Instructions for the fields under "Beneficiary 1 of N of starting action Y"

Entity other than a corporation or trust information Person who directly or indirectly owns or controls 25% or more of an entity other than a corporation or trust

Fields	Instructions
Surname	Refer to Identification fields under "Standardized field instructions".
Given Name	Same instructions (Identification fields)
Other/Initial	Same instructions (Identification fields)

Instructions for the fields under "Person 1 of N of starting action Y"

Fields	Instructions
Type of device used	Provide the type of device used.If "Other" type of device used is selected, you must specify the type of device used.
† If "Other". Please specify	If "Other" type of device used is selected, you must specify the type of device used.
Username	A username is how a person or an entity refers to themselves online.
Device identifier number	The device identifier number is a number assigned to the device, such as a Media Access Control (MAC) address or International Mobile Equipment Identity (IMEI) number.

Fields	Instructions
Internet protocol address	Provide the Internet Protocol (IP) address.It is the unique identifying number assigned to every device connected to the internet.
Date and time of online session in which request was made	This is the date and time the conductor accessed the online environment where the transaction was requested.

Instructions for the fields under "Information about conducting or attempting to conduct the transaction online"

Fields	Instructions
Relationship	Select the relationship of the "on behalf of" party to the person or entity conducting or attempting to conduct the transaction. The "on behalf of" party is understood to be the person or entity that instructs the person or entity conducting or attempting to conduct the transaction
† If "Other". Please specify	If "Other" is selected, specify the relationship of the "on behalf of" party to the person or entity conducting the transaction.

Instructions for the fields under "Relationship of the entity named above to the person or entity conducting or attempting to conduct the transaction"

Completing action Provide information about how the transaction was completed.

*** Details of disposition** This field describes what happened to the cash involved in the transaction.

Select the following disposition(s) based on the client's instructions.

Types of dispositions to select from	Instructions
Added to virtual currency wallet	Select when virtual currency is added to a virtual currency wallet.**This cannot be the first disposition**. For example, the cash received must be exchanged to virtual currency (first disposition) before it can be added to a virtual currency wallet (subsequent disposition).
Cash out	Select when cash is paid out by a non-account based reporting entity, such as a money services business.
Cash withdrawal (account based)	Select when cash is withdrawn from an account-based reporting entity, such as a bank or credit union.
Denomination exchange	Select when the cash received is exchanged from one unit value to another (for example, 20s to 100s) within the same currency.
Deposit to account	Select when cash is deposited into an account at an account-based reporting entity, such as a bank or credit union.
Exchange to fiat currency	Select for:- a fiat-to-fiat currency exchange (for example, Canadian dollars to US dollars), or- a virtual currency-to-fiat exchange (for example, bitcoin to Canadian dollars)**A virtual currency-to-fiat exchange cannot be the first disposition**. The cash received must be exchanged to virtual currency (first disposition) before the virtual currency can be exchanged to fiat (subsequent disposition).
Exchange to virtual currency	Select for:- a fiat-to-virtual currency exchange (for example, Canadian dollars to bitcoin), or- a virtual currency-to-virtual currency exchange (for example, bitcoin to ethereum (ETH))

Types of dispositions to select from	Instructions
Holding funds	Select when a non-account-based reporting entity (for example, a money services business) receives cash and holds these funds for a client for the purpose of a future transaction (for example, receipt of funds to buy virtual currency when it hits a certain threshold).
Investment product purchase or deposit	Select when a client buys or makes a deposit to a Guaranteed Investment Contract (GIC), RRSP, stock from an exchange (for example, Toronto Stock Exchange (TSX)), or any other such investments.
Issued cheque	Select for the issuance of:- a certified cheque or- a disbursement through a casino cheque, etc.
Life insurance policy purchase or deposit	Select when a client buys or puts a deposit down to purchase a life insurance policy.
Outgoing domestic funds transfer	Select when the transaction instructions are for the transfer of funds within Canada.
Outgoing email money transfer (EMT)	Select when the funds are transferred using a recipient's email address.
Outgoing international funds transfer	Select when the transaction instructions are for the transfer of funds outside of Canada.
Outgoing mobile money transfer	Select when the funds are transferred using a recipient's phone number.
Outgoing virtual currency transfer	Select when a reporting entity transfers virtual currency from a client's virtual currency wallet to another virtual currency wallet.**This cannot be the first disposition**. For example, the cash received must be exchanged to virtual currency (first disposition) before it can be added to a virtual currency wallet (second disposition) and then transferred to another virtual currency wallet.

Types of dispositions to select from	Instructions
Payment to account	Select when funds or virtual currency are used to pay down a loan, mortgage, line of credit or credit card account balance.
Purchase of bank draft	Select when a client purchases a bank draft from a financial entity.The term bank draft refers to a negotiable instrument that can be used as payment (similar to a cheque). Unlike a cheque, a bank draft is guaranteed by the issuing bank.
Purchase of casino product	Select when a client purchases a casino product.A casino product can include, but is not limited to:- chips- plaques, and- tokens
Purchase of jewellery	Select when a client purchases jewellery from a dealer in precious metals and precious stones.Jewellery means objects made of precious metals, precious stones or pearls that are intended for personal adornment.
Purchase of money order	Select when a client purchases a money order.A money order is a certificate, usually issued by a government or financial institution that allows the stated payee to receive cash on demand.A money order functions much like a cheque as the purchaser of the money order may stop the payment.
Purchase of precious metals	Select when a client purchases precious metals from a dealer in precious metals and precious stones.Precious metals means:- gold- silver- palladium, and- platinum in the form of:- coins- bars- ingots- granules, or- in other similar forms
Purchase of precious stones	Select when a client purchases precious stones from a dealer in precious metals and precious stones.Precious stones means:- diamonds- sapphires- emeralds- tanzanites- rubies, or- alexandrites

Types of dispositions to select from	Instructions
Purchase of prepaid payment product/card	Select when a client purchases a prepaid payment product.The product must be tied to a prepaid payment product account held by a financial entity.A prepaid payment product is a product that is issued by a financial entity that enables a person or entity to engage in a transaction by giving them electronic access to funds or to virtual currency paid into a prepaid payment product account held with the financial entity in advance of a transaction taking place.
Real estate purchase or deposit	Select when a client purchases or puts a deposit down on real estate.
Purchase of / Payment for goods	Select when a client purchases or pays for goods not already captured by any other disposition type included in the list above (for example, a car, yacht).
Purchase of / Payment of services	Select when a client purchases or pays for services not already captured by any other disposition type included in the list above (for example, cable, internet, hydro).

Types of dispositions to select from	Instructions
Other	Select when the disposition is not captured by any other disposition type included in the list above.Upon selecting “Other,” you must provide a description of the disposition.“Other” should not be used to combine multiple dispositions that are listed above. Specifically, if the completing action has multiple dispositions that are included in the list above, then each disposition should be selected and not combined under “Other”.**Note: If the disposition is “Other”, provide details that describe the disposition of the transaction in the field “† If”Other“, please specify”.**

Instructions for types of disposition to select for the field “* Details of disposition”

Number of dispositions in a completing action A completing action may have **1 or more dispositions**, depending on the client’s instructions and your business process.

Example 1: A single disposition

Your client brings in $12,000 cash and instructs to deposit the entire amount into the client’s savings account.

There is only 1 disposition:

- “deposit to account”.

Example 2: Multiple dispositions

Your client brings in $12,000 cash and instructs to:

- deposit $5,000 into the client’s savings account, and
- exchange $7,000 to bills in a larger denomination

There are 2 dispositions:

- “deposit to account”, and
- “denomination exchange”

Example 3: A single disposition or multiple dispositions (depending on your business process)

Your client brings in $12,000 cash and instructs to transfer $12,000 to a friend outside Canada.

Financial entity

If your business process is to:

- deposit the cash into the client's account before the amount is sent to the client's friend, there are 2 dispositions:
  - "deposit to account", and
  - "outgoing international funds transfer"
- send the amount to the friend without depositing into an account, then there is 1 disposition:
  - "outgoing international funds transfer"

Money services business

If your business process is to:

- hold the funds until a later date on which you send the amount, there are 2 dispositions:
  - "holding funds", and
  - "outgoing international funds transfer"
- send the amount to the friend without holding the funds, then there is 1 disposition:
  - "outgoing international funds transfer"

Completing action fields

Fields	Instructions
† If 'Other', please specify	Select when the disposition is not captured by any other disposition type included in the list above.Upon selecting "Other," you must provide a description of the disposition."Other" should not be used to combine multiple dispositions that are listed above. Specifically, if the completing action has multiple dispositions that are included in the list above, then each disposition should be selected and not combined under "Other".**Note**: If the disposition is "Other", provide details that describe the disposition of the transaction in the field " **† If "Other", please specify**".
*** Amount**	Enter the amount involved in the completing action. For example, this may be the amount of:- virtual currency after an exchange to virtual currency- funds being initiated for an outgoing international funds transfer- funds indicated on the bank draft
† Currency	If the disposition involves a fiat currency, enter the currency even if it was in Canadian dollars.If the currency type is not in the list provided, you must select "Other" and provide the name of the currency.
† Virtual currency type	If the disposition involves virtual currency, select the virtual currency. If the currency type is not in the list provided, you must select "Other" and provide the name of the virtual currency.
† If "Other", please specify	If "Other" is selected, you must provide the name of the type of currency or virtual currency

Fields	Instructions
† Exchange rate	Provide the rate of exchange that you used for the transaction. This can be an exchange rate for fiat currency or virtual currency.
† Value in Canadian dollars	Provide the Canadian dollar value of the disposition if not in fiat or virtual currency. For example, provide the Canadian dollar value of the jewellery, precious metals or precious stones that were purchased. This may be the market, retail or other value that you would use in the ordinary course of your business at the time of transaction, and as detailed by and in accordance with your policies and procedures.
† Virtual currency transaction identifier	This is a unique identifier.It is commonly represented by a hash consisting of mixed numerical and alphabetical characters.
† Sending virtual currency address	The sending virtual currency address is made up of a number of alpha-numeric characters. The address length is determined by the type of virtual currency used in the transaction. The sending virtual currency address is associated with whoever is sending the virtual currency (typically the conductor).
† Receiving virtual currency address	The receiving virtual currency address is made up of a number of alpha-numeric characters.The address length is determined by the type of virtual currency used in the transaction.The receiving virtual currency address is associated with whoever is receiving the virtual currency (typically the beneficiary)

Fields	Instructions
† Reference number	If the transaction involved a reference number, provide it in this field.If the transaction involves an account at a financial entity, securities dealer or casino (account-based reporting entity), **do not provide the account number information in this field**—instead, provide that information in the account number field.For all other reporting entities, if you have an internal account number that is used as a reference number, then provide the internal account number in this field.
Other number related to reference number	Provide any other number related to the reference number as applicable.
† Financial institution number	Instructions not specified
† Branch number	Instructions not specified
† Account number	If the transaction involves an account at a **financial entity**, **securities dealer** or **casino**, provide the account number. If you are not an account-based reporting entity (for example, a money services business), but the transaction involves an account at an account-based reporting entity (for example, a financial entity), provide that account number in this field.
† Account type	Provide the account type.If the account type is not in the list provided, you must select "Other" and provide the account type.
† If "Other", please specify	If "Other" account type is selected, you must specify the account type.
† Account currency	Provide the account currency (fiat) type code.Currencies are represented both numerically and alphabetically, using either three digits or three letters.If the account currency type code can not be found, you must select "Other" and provide the currency (fiat) type.

Fields	Instructions
† Account virtual currency type	Provide the account virtual currency type.If the account virtual currency type is not in the list provided, you must select "Other" and provide the account virtual currency type.
† If "Other", please specify	If "Other", provide the full name of the currency or virtual currency type.
Date account opened	Provide the date the account was opened.
Date account closed	Provide the date the account was closed.
† Status of account at the time of transaction	Provide the status of the account at the time of the transaction (for example: active, inactive, dormant, closed).
‡ Was there any other person or entity involved in the completing action?	This field is a "Yes/No" question.See **Involved in the completing action,** below.

Instructions for the "Completing action fields"

Account holder – person

Fields	Instructions
† Surname	Refer to Name fields under "Standardized field instructions".
† Given name	Same instructions (Name fields)
Other/Initial	Same instructions (Name fields)

Instructions for the fields under "Person 1 of N completing action Z"

Account holder – entity

Field	Instructions
† Name of entity	Refer to Name fields under "Standardized field instructions".

Instructions for the field under "Entity 1 of N completing action Z"

Involved in the completing action Person involved in the completing action

If you have information about other persons involved in the completing action, you must include it.

Note: These persons **cannot be**:

- the conductor
- on behalf of party, or
- beneficiary of the transaction

Fields	Instructions
† Surname	Refer to Name fields under "Standardized field instructions".
† Given name	Same instructions (Name fields)
Other/initial	Same instructions (Name fields)
Account number	Provide the account number of the person involved in the completing action.If the transaction involves an account at a **financial entity**, **securities dealer** or **casino**, provide the account number. If you are not an account-based reporting entity (for example, a money services business), but the transaction involves an account at an account-based reporting entity (for example, a financial entity), provide that account number in this field.It is acceptable to include the financial institution number and branch number as part of an account number.
Policy number	Instructions not specified
Identifying number	Instructions not specified

Instructions for the fields under "Person 1 of N of completing action Z"

Entity involved in the completing action If you have information about other entities involved in the completing action, you must include it.

Note: These entities **cannot be**:

- the conductor
- on behalf of party, or
- beneficiary of the transaction

Fields	Instructions
† Name of entity	Refer to Name fields under "Standardized field instructions".
Account number	Provide the account number of the entity involved in the completing action.If the transaction involves an account at a **financial entity**, **securities dealer** or **casino**, provide the account number. If you are not an account-based reporting entity (for example, a money services business), but the transaction involves an account at an account-based reporting entity (for example, a financial entity), provide that account number in this field.It is acceptable to include the financial institution number and branch number as part of an account number.
Policy number	Instructions not specified
Identifying number	Instructions not specified

Instructions for the fields under "Entity 1 of N of completing action Z"

Beneficiary

Fields	Instructions
‡ Have you obtained any beneficiary information related to this transaction or attempted transaction? (Only select No if the beneficiary is **not** your client **and**, after taking reasonable measures, you were not able to obtain any beneficiary details.)	This field is a "Yes/No" question.Only select No if the beneficiary is **not** your client **and**, after taking reasonable measures, you were not able to obtain any beneficiary details.

Instructions for the fields under "Beneficiary Indicator"

Provide beneficiary information for each completing action.

A beneficiary, for example, can be:

- the person who receives the virtual currency

- the person named on a money order, or
- the person who receives the jewellery

The beneficiary **can be** the **same person or entity** that conducts the transaction or someone else.

The beneficiary **cannot be** the reporting entity.

Person beneficiary

Fields	Instructions
† Surname	Refer to Name fields under "Standardized field instructions".
† Given name	Same instructions (Name fields)
Other/Initial	Same instructions (Name fields)
Alias	Same instructions (Name fields)
Username	A username is how a person or an entity refers to themselves online.
Client number	Instructions not specified
Apartment/Room/Suite/Unit number	Refer to Address fields under "Standardized field instructions".
House/Building number	Same instructions (Address fields)
Street address	Same instructions (Address fields)
City	Same instructions (Address fields)
District	Same instructions (Address fields)
Country	Same instructions (Address fields)
Province or state	Same instructions (Address fields)
Sub-province and/or sub-locality	Same instructions (Address fields)
Postal or zip code	Same instructions (Address fields)
Unstructured address details	Refer to Unstructured address field under "Standardized field instructions".
Telephone number	Refer to Telephone number fields under "Standardized field instructions".
Extension	Same instructions (Telephone number fields)
Email address	Instructions not specified
Date of birth	Instructions not specified
Country of residence	Enter the primary country of residence for the person.It can be the same or different from the country entered in the address section.

Fields	Instructions
Occupation	Refer to Occupation/business fields under "Standardized field instructions".
Name of employer	Same instructions (Occupation/business fields)

Instructions for the fields under "Person 1 of C completing action Z"

Identification of the person beneficiary

Fields	Instructions
Identifier type	Refer to Identification fields under "Standardized field instructions".
† If "Other", please specify	If "Other" identifier type is selected, you must specify the identifier type.
Number associated with identifier type	Same instructions (Identification fields)
Jurisdiction of issue (country)	Same instructions (Identification fields)
Jurisdiction of issue (province or state)	Same instructions (Identification fields)

Instructions for the fields under "Identification 1 of N of the person beneficiary C"

Identification of the entity beneficiary

Fields	Instructions
† Name of entity	Refer to Identification fields under "Standardized field instructions".
Username	A username is how a person or an entity refers to themselves online.
Client number	Instructions not specified
Apartment/Room/Suite/Unit number	Refer to Address fields under "Standardized field instructions".
House/Building number	Same instructions (Address fields)
Street address	Same instructions (Address fields)
City	Same instructions (Address fields)
District	Same instructions (Address fields)
Country	Same instructions (Address fields)

Fields	Instructions
Province or state	Same instructions (Address fields)
Sub-province and/or sub-locality	Same instructions (Address fields)
Postal or zip code	Same instructions (Address fields)
Unstructured address details	Refer to Unstructured address field under "Standardized field instructions".
Telephone number	Refer to Telephone number fields under "Standardized field instructions".
Extension	Same instructions (Telephone number fields)
Email address	Instructions not specified
Nature of entity's principal business	Refer to Occupation/business fields under "Standardized field instructions".
Is the entity incorporated or registered?	This field is a "Yes/No" question.

Instructions for the fields under "Entity 1 of C of completing action Z"

Incorporation of the entity

Fields	Instructions
Incorporation number	Provide the incorporation number of the entity conducting the transaction for each jurisdiction where the entity is incorporated.
Jurisdiction of issue (country) of incorporation	Provide the jurisdiction of issue (country) of incorporation for each jurisdiction where the entity is incorporated

Fields	Instructions
Jurisdiction of issue (province or state) of incorporation	Provide the jurisdiction of issue (province or state) of incorporation for each jurisdiction where the entity is incorporatedIf the jurisdiction is a province or state **in** Canada, the United States or Mexico, **select the code from the list of options.**If the jurisdiction is **outside** Canada, the United States or Mexico, **provide the name of the province or state.**

Instructions for the fields under "Incorporation 1 of N of entity beneficiary A"

Registration of the entity

Fields	Instructions
Registration number	Provide the registration number of the entity conducting the transaction for each jurisdiction where the entity is registeredFor Canadian entities, a registration number can include the 9-digit business number assigned to that entity by the Canada Revenue Agency (CRA).
Jurisdiction of issue (country) of registration	Provide the country that issued the documentation used to identify the entity for each jurisdiction where the entity is registered.
Jurisdiction of issue (province or state) of registration	Provide the jurisdiction of issue (province or state) for each jurisdiction where the entity is registeredIf the jurisdiction is a province or state **in** Canada, the United States or Mexico, **select the code from the list of options.**If the jurisdiction is **outside** Canada, the United States or Mexico, **provide the name of the province or state.**

Instructions for the fields under "Registration 1 of N of entity beneficiary A"

Identification of the entity Provide the following information that was used to verify the identity of the entity that is a beneficiary.

For some entities, this information may be the same as the registration or incorporation information.

Fields	Instructions
Identifier type	Refer to Identification fields under "Standardized field instructions".
† If "Other", please specify	If "Other" is selected, you must specify the identifier type.
Number associated with identifier type	Same instructions (Identification fields)
Jurisdiction of issue (country)	Same instructions (Identification fields)
Jurisdiction of issue (province or state)	Same instructions (Identification fields)

Instructions for the fields under "Identification 1 of N of entity beneficiary C"

Fields	Instructions
Surname	Refer to Name fields under "Standardized field instructions".
Given name	Same instructions (Name fields)
Other/Initial	Same instructions (Name fields)

Instructions for the fields under "Person authorized to bind the entity beneficiary or act with respect to the account (maximum 3)"

Details of suspicion **Note:** The "Details of suspicion" section of the Suspicious Transaction Report form **must not be completed** if the transaction is being reported to FINTRAC under a Ministerial Directive.

***Description of suspicious activity** This section is the narrative that explains your grounds for suspicion that led to your decision to submit a Suspicious Transaction Report to FINTRAC.

You must describe in clear, simple and concise language your grounds for suspicion of a money laundering or terrorist financing offence – including the facts, context, and indicators that allowed you to reach reasonable grounds for suspicion.

The narrative should:

- **not assume** that the reader will be familiar with acronyms or terminology specific to your business.

- focus on the question: "Why do you think the transaction is suspicious of money laundering or terrorist financing?"
- **not refer** to any internal files or documents since FINTRAC cannot have access to these internal files or documents for its analysis.
- not include graphics, underlined, italicized or bolded text since they cannot be viewed in the Suspicious Transaction Report form
- be consistent with the information in the structured fields of the Suspicious Transaction Report form
  - For example, if you are referring to specific account activity in this section, the details of those accounts and transactions should be entered in the structured fields.

Detailed and high quality Suspicious Transaction Reports provide valuable and actionable intelligence for FINTRAC and this section is shared with law enforcement and intelligence agencies in FINTRAC disclosures.

Instructions for the fields under "details of suspicion"

Fields	Instructions
Suspicion type	Select:- money laundering- terrorist financing- money laundering and terrorist financing- sanctions evasion- money laundering and sanctions evasion- terrorist financing and sanctions evasion- money laundering, terrorist financing and sanctions evasionIf your primary suspicion type is sanctions evasion, and you do not have the system capability at this time to select the new sanctions evasion option, you must select "money laundering" as suspicion type from the drop down list and add #SANCTIONS as part of the grounds for suspicion in the Description of suspicious activity section.
Public-Private partnership name	Select the public-private partnership project name that the Suspicious Transaction Report is associated with, if applicable.

Fields	Instructions
Does this report include information about an individual you have determined to be a politically exposed person (PEP)?	This field is a "Yes/No" question.

Related Reports Are there previously submitted reports that may relate to the suspicious activity mentioned in this report?

Fields	Instructions
Reporting entity report reference number (1 of N)	Provide the reporting entity report reference number(s) of the previously submitted report(s) that may relate to the suspicious activity mentioned in this Suspicious Transaction Report.
Reporting entity transaction reference number (1 of Z of report N)	Provide the reporting entity transaction reference number(s) of the previously submitted report(s) that may relate to the suspicious activity mentioned in this Suspicious Transaction Report.

Instructions for the fields under "Report 1 of X"

Action taken **Note:** The "Action taken" section of the Suspicious Transaction Report form **must not be completed** if the transaction is being reported to FINTRAC under a Ministerial Directive.

*** Description of action taken** Describe the action(s) that you have taken or will be taking as a result of the suspicious transaction(s).

The following are examples of actions taken:

- reporting the information directly to law enforcement;
- initiating enhanced transaction monitoring;
- closing the account(s) in question or exiting the business relationship; and/or
- cancelling, reversing or rejecting the transaction.

Reporting a Suspicious Transaction Report to FINTRAC **does not** prevent you from contacting law enforcement directly.

However, even if you do contact law enforcement directly about your suspicions of money laundering or terrorist financing, you must still submit a Suspicious Transaction Report to FINTRAC.

Some **Suspicious Transaction Reports** have included the law enforcement agency's contact information in this part of the **Suspicious Transaction Report** when the suspicion was also reported directly to law enforcement and this information can be helpful.

Annex B - Scenarios

The following scenarios demonstrate form completion and the expected field information in a Suspicious Transaction Report based on the client's instructions and transaction(s) in each scenario.

Notes about these scenarios

- Specific money laundering and terrorist financing indicators and a full narrative of the reasonable grounds to suspect has not been provided.
  - For information on reasonable grounds to suspect and indicators for your sector, refer to 4. When to submit a Suspicious Transaction Report above, and the money laundering and terrorist financing indicators under All FINTRAC guidance – Transaction reporting.
  - Not all fields of the Suspicious Transaction Report form are displayed—only fields with completed information are displayed.
- Not all fields of the Suspicious Transaction Report form are displayed.
- Only fields with completed information are displayed.
- Some fields have been combined for the purpose of brevity. For example, conductor name, address, telephone number and other conductor fields have been combined as conductor information.
- Because some fields are mandatory and some are not, it has been assumed that the reporting entity had the information if a field has been completed.

In this annex

Scenario B.1: Person deposits cheque and sends an email money transfer (EMT)

- On July 6, 2022, Gordie Gold deposited a $1,500 cheque from Iron Construction Ltd. into a joint account (with Gemma Gold) at Moon Rays Financial by using his access card at an automated teller machine (ATM).
  - The cheque, which was payable to Gordie Gold, included the following memo line: Pay cheque—Job # 5.
- On the same evening, Gordie logged into online banking using his access card and sent an email money transfer (EMT) in the amount of $2,500 from his joint account with Gemma to Sunny Silver's account at Solar Bank.
  - Sunny is not a client of Moon Rays Financial.
  - The EMT message indicates the following: July 2022 rent.
- Moon Rays Financial is submitting the following Suspicious Transaction Report as it identified multiple indicators and determined that there are reasonable grounds to suspect the transactions are related to the commission of a money laundering offence.

Expected field information in the report

General information – Scenario B.1

Fields	Information provided by Moon Rays Financial
Reporting entity number	The reporting entity number assigned to Moon Rays Financial when it enrolled with FINTRAC Web Reporting System (FWR)
Reporting entity report reference number	The unique number for this report that was assigned by:- Moon Rays Financial, or- its service provider
Activity sector	Bank
Contact information for this report	Information about the person at Moon Rays Financial that FINTRAC can liaise with in the event that a follow up is required

General information about Moon Rays Financial

Transaction information – Scenario B.1

Fields	Information provided for transaction 1 of 2	Information provided for transaction 2 of 2
Transaction Status	Completed	Completed
Date of transaction	The date the cheque was deposited at Moon Rays Financial (July, 6, 2022)	The date the online transaction was conducted (July 6, 2022)
Time of transaction	The time the cheque was deposited at Moon Rays Financial	The time the online transaction was conducted on July 6, 2022
Method of transaction	Automated teller machine (ATM)	Online
Reporting entity transaction reference number	The unique number for this transaction that was assigned by:- Moon Rays Financial Bank, or- its service provider	The unique number for this transaction that was assigned by:- Moon Rays Financial, or- its service provider
Reporting entity location number	Information about where the transaction took place (ATM location)	Information about where the transaction took place -specifically, the location number that is associated with the location that receives and initiates the client's online instructions

"Transaction information" provided by Moon Rays Financial

Starting action – Scenario B.1

Fields	Information provided for starting action 1 of transaction 1	Information provided for starting action 1 of transaction 2
Direction of starting action	In	Out
Type of funds, assets or virtual currency (in/out)	Cheque	Funds withdrawal
Amount	1,500	2,500
Currency	CAD	CAD

Fields	Information provided for starting action 1 of transaction 1	Information provided for starting action 1 of transaction 2
Financial Institution and branch number	The financial institution and branch number which issued the cheque	The financial institution and branch number for Moon Rays Financial
Account number	The account number indicated on the cheque	The account number for the joint account of Gordie and Gemma Gold at Moon Rays Financial
Was information about the source (person/entity) of funds or virtual currency obtained?	No	No
Account holder	Iron Construction Ltd. (as indicated on the cheque)	Gordie and Gemma Gold
Conductor information	Information that Moon Rays Financial has on Gordie Gold which may include: - name- alias- client number- address- telephone number- email address- URL- date of birth- country of residence- country of citizenship- occupation- name and address of employer, and- identification details	Information that Moon Rays Financial has on Gordie Gold which may include:- name- alias- client number- address- telephone number- email address- URL- date of birth- country of residence- country of citizenship- occupation- name and address of employer, and- identification details
Information about conducting or attempting to conduct the transaction online	[Field left blank because not applicable]	Information including:- type of device used- username- device identifier number- internet protocol address- date and time of online session in which request was made

Fields	Information provided for starting action 1 of transaction 1	Information provided for starting action 1 of transaction 2
Was this transaction conducted or attempted on behalf of another person or entity?	No	No

"Starting action" information provided by Moon Rays Financial

Completing action – Scenario B.1

Fields	Information provided for completing action 1 of transaction 1	Information provided for completing action 1 of transaction 2
Details of disposition	Deposit to account	Outgoing email money transfer (EMT)
Amount	1,500	2,500
Currency	CAD	CAD
Financial institution number and branch number (if available for EMT)	The financial institution and branch number for Moon Rays Financial	The financial institution and branch number for Solar Bank
Account number (if available for EMT)	The account number for the joint account of Gordie and Gemma Gold at Moon Rays Financial	The account number of Sunny Silver at Solar Bank
Account holder (if available for EMT)	Gordie and Gemma Gold	Sunny Silver
Was there any other person or entity involved in the completing action?	No	No

Fields	Information provided for completing action 1 of transaction 1	Information provided for completing action 1 of transaction 2
Beneficiary information	Information that Moon Rays Financial has on Gordie and Gemma Gold as they are the account holders on the joint account in which the cheque was deposited. This may include; - name- alias- username- client number- address- telephone number- email address- date of birth- country of residence- occupation- name of employer, and- identification details	Sunny Silver's nameAlso, if obtained, information about Sunny Silver including:- name- alias- client number- address- telephone number- email address- date of birth- country of residence- occupation- name of employer, and- identification details

"Completing action" information provided by Moon Rays Financial

Details of suspicion – Scenario B.1

Details of Suspicion
The description of the facts, context and indicators that allowed Moon Rays Financial to establish that there are reasonable grounds to suspect that the transaction(s) are related to the commission of a money laundering offence.In this scenario, this could include the information from the cheque memo line (Pay cheque—Job # 5) and the EMT message (July 2022 rent).

"Details of Suspicion" information provided by Moon Rays Financial

Details of action taken – Scenario B.1

Action Taken
The action that Moon Rays Financial has taken as a result of the suspicious transaction(s).

"Details of Action Taken" information provided by Moon Rays Financial

Note:

- If the conductor (Gordie Gold) has multiple email addresses, provide the email address that the conductor used to send the EMT in the email address field for the conductor.
- Gordie's other email addresses can be provided in the narrative section of the report (Details of suspicion).
- The beneficiary email address field should be the email address that was used by the beneficiary to receive the email money transfer (EMT).

Scenario B.2: Entity exchanges cash to virtual currency and transfers to wallet

- On July 7, 2022, Gordie Gold walked into Cosmic Virtual Currency Money Service Business (Cosmic VC MSB) with $9,997 CAD cash.
  - Gordie advised Cosmic VC MSB that he is representing Gordie's Painting Inc. A company in which he is the CEO and sole director and shareholder.
  - Gordie also advised Cosmic VC MSB that the cash was payment from a recently sold painting to a client, Sunny Silver.
  - Gordie requested that the cash be exchanged to Ethereum (ETH) so that it could be added to Cosmic VC MSB's custodial virtual currency wallet. The virtual currency exchange rate was 0.0007.
  - Gordie then requested the ETH be transferred to his personal external virtual currency wallet.
- Cosmic VC MSB is submitting this Suspicious Transaction Report as it identified multiple indicators and determined that there are reasonable grounds to suspect the transaction is related to the commission of a money laundering offence.

Expected field information in the report

General information – Scenario B.2

Fields	Information provided by Cosmic VC MSB
Reporting entity number	The reporting entity number assigned to Cosmic VC MSB when it enrolled with FINTRAC Web Reporting System (FWR)
Reporting entity report reference number	The unique number for this report that was assigned by:- Cosmic VC MSB, or- its service provider
Activity sector	Money services business

Fields	Information provided by Cosmic VC MSB
Contact information for this report	Information about the person at Cosmic VC MSB that FINTRAC can liaise with in the event that a follow up is required

General information about Cosmic VC MSB

Transaction information – Scenario B.2

Fields	Information provided for transaction 1 of 1
Transaction Status	Completed
Date of transaction	The date the cash was received by Cosmic VC MSB (July, 7, 2022)
Time of transaction	The time the cash was received by Cosmic VC MSB on July 7, 2022
Method of transaction	In person
Reporting entity transaction reference number	The unique number for this transaction that was assigned by:- Cosmic VC MSB, or- its service provider
Reporting entity location number	Information about where the transaction took place

"Transaction information" provided by Cosmic VC MSB

Starting action – Scenario B.2

Fields	Information provided for starting action 1 of transaction 1
Direction of starting action	In
Type of funds, assets or virtual currency (in/out)	Cash
Amount	9,997
Currency	CAD
How were the funds or virtual currency obtained?	Gordie Gold advised that he received the cash when he sold a painting to his client, Sunny Silver

Fields	Information provided for starting action 1 of transaction 1
Was information about the source (person/entity) of funds or virtual currency obtained?	Yes
Source of funds or virtual currency	Sunny Silver
Conductor information	Information that Cosmic VC MSB has on Gordie's Painting Inc. which may include: - name- alias- client number- address- telephone number- email address- URL, and- identification details
Additional information about the conductor if it is an entity	- Person(s) authorized to bind the entity (Gordie Gold),- Type of entity (corporation) - Nature of entity's principal business (painting/contracting) - Incorporation and/or registration information - Director(s) of the corporation (Gordie Gold)- Person(s) who directly or indirectly owns or controls 25% or more shares of the corporation (Gordie Gold)
Was this transaction conducted or attempted on behalf of another person or entity?	No

"Starting action" information provided by Cosmic VC MSB

Completing action – Scenario B.2

Fields	Information provided for completing action 1 of transaction 1	Information provided for completing action 2 of transaction 1	Information provided for completing action 3 of transaction 1
Details of disposition	Exchange to virtual currency	Added to virtual currency wallet	Outgoing virtual currency transfer
Amount	7	7	7
Virtual Currency type	ETH	ETH	ETH

Fields	Information provided for completing action 1 of transaction 1	Information provided for completing action 2 of transaction 1	Information provided for completing action 3 of transaction 1
Exchange rate	.0007	[Field left blank because not applicable]	[Field left blank because not applicable]
Virtual Currency transaction identifier	[Field left blank because not applicable]	The unique identifier for this transaction (completing action 2) that is commonly represented by a hash consisting of mixed numerical and alphabetical characters	The unique identifier for this transaction (completing action 3) that is commonly represented by a hash consisting of mixed numerical and alphabetical characters
Receiving Virtual currency address	[Field left blank because not applicable]	The virtual currency address for Cosmic VC MSB as it received the virtual currency	The virtual currency address for Gordie Gold as he received the virtual currency in his personal wallet
Was there any other person or entity involved in the completing action?	No	No	No

Fields	Information provided for completing action 1 of transaction 1	Information provided for completing action 2 of transaction 1	Information provided for completing action 3 of transaction 1
Beneficiary information	Information that Cosmic VC MSB has on Gordie's Painting Inc. which may include:- name- username- client number- address- telephone number- email address- nature of entity's principal business (painting/ contracting) - incorporation and/or registration information- identification details, and- person(s) authorized to bind the entity (Gordie Gold)	Information that Cosmic VC MSB has on Gordie's Painting which may include: - name- username - client number - address - telephone number - email address - nature of entity's principal business (painting/ contracting) - incorporation and/or registration information- identification details, and- person(s) authorized to bind the entity (Gordie Gold)	Information that Cosmic VC MSB has on Gordie Gold which may include: - name - alias - username- client number - address - telephone number - email address - date of birth - country of residence - occupation,- name of employer, and - identification details

"Completing action" information provided by Cosmic VC MSB

Details of suspicion – Scenario B.2

Details of Suspicion
The description of the facts, context and indicators that allowed Cosmic VC MSB to establish that there are reasonable grounds to suspect that the transaction(s) is/are related to the commission of a money laundering offence.

"Details of Suspicion" information provided by Cosmic VC MSB

Details of action taken – Scenario B.2

Action Taken
The action that Cosmic VC MSB has taken because of the suspicious transaction(s).

"Details of Action Taken" information provided by Cosmic VC MSB

Scenario B.3: Person deposits on behalf of another person who later purchases casino chips and then redeems these chips

- On July 8th, 2022, Gordie Gold came into Vega Casino to deposit $9,000 cash on behalf of Sunny Silver.
  - The cash was deposited into Sunny's account and Gordie advised the casino that he and Sunny were friends.
  - The casino was not able to obtain information about the purpose of the transaction or the source of funds.
- On July 9th, 2022, Sunny purchased casino chips at Vega Casino using funds in her casino account totaling $9,000.
  - After leaving the front desk, Sunny was seen passing the chips to Chuck who is an individual known to the casino.
  - Within an hour, Sunny returned to the front desk to redeem the remaining casino chips and requested a cheque payable to herself totaling $5,000.
- Vega Casino is submitting this Suspicious Transaction Report as it identified multiple indicators and determined that there are reasonable grounds to suspect the transactions are related to the commission of a money laundering offence.

Expected field information in the report

General information – Scenario B.3

Fields	Information provided by Vega Casino
Reporting entity number	The reporting entity number assigned to Vega Casino when it enrolled with FINTRAC Web Reporting System (FWR)
Reporting entity report reference number	The unique number for this report that was assigned by:- Vega Casino, or- its service provider
Activity sector	Casino

Fields	Information provided by Vega Casino
Contact information for this report	Information about the person at Vega Casino that FINTRAC can liaise with in the event that a follow up is required

General information about Vega Casino

Transaction information – Scenario B.3

Fields	Information provided for transaction 1 of 3	Information provided for transaction 2 of 3	Information provided for transaction 3 of 3
Transaction Status	Completed	Completed	Completed
Date of transaction	The date Vega Casino received the cash from Gordie Gold (July 8, 2022)	The date casino chips were purchased (July 9, 2022)	The date casino chips were redeemed (July 9, 2022)
Time of transaction	The time Vega Casino received the cash on July 8, 2022	The time the casino chips were purchased on July 9, 2022	The time the casino chips were redeemed on July 9, 2022
Method of transaction	In person	In person	In person
Reporting entity transaction reference number	The unique number for this transaction that was assigned by:- Vega Casino, or- its service provider	The unique number for this transaction that was assigned by:- Vega Casino, or- its service provider	The unique number for this transaction that was assigned by:- Vega Casino, or- its service provider
Reporting entity location number	Information about where the transaction took place	Information about where the transaction took place	Information about where the transaction took place

Starting action – Scenario B.3

Fields	Information provided for starting action 1 of transaction 1	Information provided for starting action 1 of transaction 2	Information provided for starting action 1 of transaction 3
Direction of starting action	In	Out	In
Type of funds, assets or virtual currency (in/out)	Cash	Funds withdrawal	Casino product
Amount	9,000	9,000	5,000
Currency	CAD	CAD	CAD
Account number	[Field left blank because not applicable]	Sunny Silver's account number at Vega Casino	[Field left blank because not applicable]
Was information about the source (person /entity) of funds or virtual currency obtained?	No	No	No
Account holder	[Field left blank because not applicable]	Sunny Silver	[Field left blank because not applicable]

Fields	Information provided for starting action 1 of transaction 1	Information provided for starting action 1 of transaction 2	Information provided for starting action 1 of transaction 3
Conductor information	Information that Vega Casino has on Gordie Gold which may include: - name- alias- client number- address- telephone number- email address- URL- date of birth- country of residence- country of citizenship- occupation- name and address of employer, and- identification details	Information that Vega Casino has on Sunny Silver which may include:- name- alias- client number- address- telephone number- email address- URL- date of birth- country of residence- country of citizenship- occupation- name and address of employer, and- identification details	Information that Vega Casino has on Sunny Silver which may include:- name- alias- client number- address- telephone number- email address- URL- date of birth- country of residence- country of citizenship- occupation- name and address of employer, and- identification details
Was this transaction conducted or attempted on behalf of another person or entity?	Yes	No	No
Relationship of the person named above to the person or entity conducting or attempting to conduct the transaction	Friend	[Field left blank because not applicable]	[Field left blank because not applicable]

Scenario B.4: Person transfers funds between accounts and pays utility bill and credit card

- On July 9th, 2022, Gordie Gold logged into online banking at Moon Rays Financial using his access card and does the following:
  - transfers $1,500 from his joint account with Gemma Gold to his own personal account—and both accounts are held at Moon Rays Financial
  - pays an electric bill to ABC Electric Company (billing account reference number 12345-678) for $500 using funds from his own personal account, and
  - pays a credit card account balance of $1,000 to ABC Credit Card Company (credit card number 1234-5678-1234-5678) using funds from his personal account.
- Moon Rays Financial is submitting this Suspicious Transaction Report as it identified multiple indicators and determined that there are reasonable grounds to suspect the transactions are related to the commission of a money laundering offence.

Expected field information in the report

General information – Scenario B.4

Fields	Information provided by Moon Rays Financial
Reporting entity number	The reporting entity number assigned to Moon Rays Financial when it enrolled with FINTRAC Web Reporting System (FWR)
Reporting entity report reference number	The unique number for this report that was assigned by:- Moon Rays Financial, or- its service provider
Activity sector	Bank
Contact information for this report	Information about the person at Moon Rays Financial that FINTRAC can liaise with in the event that a follow up is required

General information about Moon Rays Financial

Transaction information – Scenario B.4

Fields	Information provided for transaction 1 of 3	Information provided for transaction 2 of 3	Information provided for transaction 3 of 3
Transaction Status	Completed	Completed	Completed
Date of transaction	The date the online transaction was conducted (July 9, 2022)	The date the online transaction was conducted (July 9, 2022)	The date the online transaction was conducted (July 9, 2022)
Time of transaction	The time the online transaction was conducted on July 9, 2022	The time the online transaction was conducted on July 9, 2022	The time the online transaction was conducted on July 9, 2022
Method of transaction	Online	Online	Online
Reporting entity transaction reference number	The unique number for this transaction that was assigned by:- Moon Rays Financial, or- its service provider	The unique number for this transaction that was assigned by:- Moon Rays Financial, or- its service provider	The unique number for this transaction that was assigned by:- Moon Rays Financial, or- its service provider
Reporting entity location number	Information about where the transaction took place – specifically the location number that is associated with the location that receives and initiates the client's online instructions	Information about where the transaction took place – specifically the location number that is associated with the location that receives and initiates the client's online instructions	Information about where the transaction took place – specifically the location number that is associated with the location that receives and initiates the client's online instructions

Starting action – Scenario B.4

Fields	Information provided for starting action 1 of transaction 1	Information provided for starting action 1 of transaction 2	Information provided for starting action 1 of transaction 3
Direction of starting action	Out	Out	Out
Type of funds, assets or virtual currency (in/out)	Funds withdrawal	Funds withdrawal	Funds withdrawal
Amount	1,500	500	1,000
Currency	CAD	CAD	CAD
Financial institution and branch number	The financial institution and branch number for Moon Rays Financial	The financial institution and branch number for Moon Rays Financial	The financial institution and branch number for Moon Rays Financial
Account number	The account number for the joint account of Gordie and Gemma Gold at Moon Rays Financial	The account number for Gordie Gold's personal account at Moon Rays Financial	The account number for Gordie Gold's personal account at Moon Rays Financial
Was information about the source (person /entity) of funds or virtual currency obtained?	No	No	No
Account holder	Gordie and Gemma Gold	Gordie Gold	Gordie Gold

Fields	Information provided for starting action 1 of transaction 1	Information provided for starting action 1 of transaction 2	Information provided for starting action 1 of transaction 3
Conductor information	Information that Moon Rays Financial has on Gordie Gold which may include: - name- alias- client number- address- telephone number- email address- URL- date of birth- country of residence- country of citizenship- occupation- name and address of employer, and- identification details	Information that Moon Rays Financial has on Gordie Gold which may include:- name- alias- client number- address- telephone number- email address- URL- date of birth- country of residence- country of citizenship- occupation- name and address of employer, and- identification details	Information that Moon Rays Financial has on Gordie Gold which may include:- name- alias- client number- address- telephone number- email address- URL- date of birth- country of residence- country of citizenship- occupation- name and address of employer, and- identification details
Information about conducting or attempting to conduct the transaction online	Information including:- type of device used- username- device identifier number- internet protocol address- date and time of online session	Information including:- type of device used- username- device identifier number- internet protocol address- date and time of online session	Information including:- type of device used- username- device identifier number- internet protocol address- date and time of online session in which the request was made
Was this transaction conducted or attempted on behalf of another person or entity?	No	No	No

Completing action – Scenario B.4

Fields	Information provided for completing action 1 of transaction 1	Information provided for completing action 1 of transaction 2	Information provided for completing action 1 of transaction 2
Details of disposition	Outgoing domestic funds transfer	Purchase of /Payment of services	Payment to account
Amount	1,500	500	1,000
Currency	CAD	CAD	CAD
Reference number	[Field left blank because not applicable]	12345-678 (the reference number associated with the bill payment)	[Field left blank because not applicable]
Financial institution and branch number	The financial institution and branch number which sent the outgoing domestic funds transfer	[Field left blank because not applicable]	[Field left blank because not applicable]
Account number	The account number for the personal account of Gordie Gold at Moon Rays Financial	[Field left blank because not applicable]	1234-5678-1234-5678 (the credit card account in which payment was made)
Account holder	Gordie Gold	[Field left blank because not applicable]	[Field left blank because not applicable]
Was there any other person or entity involved in the completing action?	No	No	No

Fields	Information provided for completing action 1 of transaction 1	Information provided for completing action 1 of transaction 2	Information provided for completing action 1 of transaction 2
Beneficiary information	Information that Moon Rays Financial has on Gordie Gold. This may include; - name- alias- username- client number- address- telephone number- email address- date of birth- country of residence- occupation- name of employer, and- identification details	Information that Moon Rays Financial has on ABC Electric Company. This may include:- name- username - client number - address - telephone number - email address - nature of entity's principal business (utility) - incorporation and/or registration information- identification details, and- person(s) authorized to bind the entity	Information that Moon Rays Financial has on ABC Credit Card Company. This may include:- name- username - client number - address - telephone number - email address - nature of entity's principal business (credit card company) - incorporation and/or registration information- identification details, and- person(s) authorized to bind the entity

"Completing action" information provided by Moon Rays Financial

Details of suspicion – Scenario B.4

Details of Suspicion
The description of the facts, context and indicators that allowed Moon Rays Financial to establish that there are reasonable grounds to suspect that the transaction(s) are related to the commission of a money laundering offence.

"Details of Suspicion" information provided by Moon Rays Financial

Details of action taken – Scenario B.4

Action Taken
The action that Moon Rays Financial has taken as a result of the suspicious transaction(s).

"Details of Action Taken" information provided by Moon Rays Financial# Guide on harm done assessment for record keeping violations

1. Introduction

This page presents how we assess the harm done and calculate the base penalty amount applied to record keeping violations.

1.1 Purpose of the guide

This guide presents how FINTRAC approaches the harm done criterion and the base penalty amount for violations under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (the Act) and its regulations. According to section 73.11 of the Act, FINTRAC must consider the harm done by a violation, that the purpose of an administrative monetary penalty (AMP) is to encourage compliance rather than to punish, and all other criteria prescribed in the regulations, including a reporting entity's (RE) history of compliance, when determining the amount of a penalty. Considerations for the non-punitive nature of an AMP and an REs' compliance history are assessed in another step in the penalty calculation and are outlined separately in FINTRAC's AMP policy.

1.2 Definition of harm

FINTRAC defines "harm" as the degree to which a violation interferes with achieving the objectives of the ActFootnote 1 or with FINTRAC's ability to carry out its mandateFootnote 2. Therefore, the consequences of non-compliance, when an AMP is imposed, are linked to its effects on Canada's efforts to combat money laundering and terrorist activity financing (ML/TF).

Compliance enforcement activities are undertaken to prevent and correct the harm that comes from non-compliance with the Act and regulations. REs' adherence to requirements such as record keeping and verifying client identity assists in the deterrence of ML/TF and supports investigations and criminal prosecutions. The requirements related to reporting ensure that FINTRAC is supplied with the high-quality, timely financial transaction reports it needs to produce the financial intelligence that helps with the investigation and prosecution of ML/TF offences.

1.3 Considering harm in AMP Calculations

When determining a penalty, FINTRAC considers the harm caused, that is, the degree to which the non-compliance interferes with the purpose of the Act and/or with FINTRAC's mandate. Non-compliance and harm are measured using the standards described in this guide, which outline the benchmark amounts for the corresponding levels of harm for a specific violation. FINTRAC considers the specific circumstances of each case, including the extent of the non-compliance and mitigating factors, which may further reduce the actual amounts applied.

2. Violations related to keeping prescribed records

Record keeping violations directly affect the objective set out in subparagraph 3(a)(i) of the PCMLTFA. Record keeping requirements are important to Canada's anti-money laundering and anti-terrorist financing (AML/ATF) regime because they compel the preservation of the information that is needed to achieve the objectives of the PCMLTFA and FINTRAC's mandate. The information that is required to be kept serves to identify individuals and entities that own or control funds, or conduct, direct or are beneficiaries to transactions. The required information also helps clarify financial transactions and activities for the purposes of following the flow of funds (such as transaction amounts, dates, currency types, etc.); of understanding clients (such as the nature of their business, occupation, intended use of accounts, etc.); of identifying relationships (such as third party information); of providing evidence for law enforcement investigations and prosecutions, and complying with the legislation.

Records that businesses are required to keep serve many purposes for your business as an RE, law enforcement and FINTRAC. Records with missing, incomplete, incorrect or inadequate information may affect your ability to submit high-quality and timely transaction reports to FINTRAC and to conduct effective risk assessments. They may also interfere with law enforcement investigations, and with FINTRAC's ability to ensure compliance with the Act and its regulations.

2.13 Harm done in the case of violations related to keeping prescribed records

Accurate and complete record keeping is fundamental to the detection, prevention, deterrence, investigation and prosecution of ML/TF offences. Without the prescribed records, REs and government agencies would not be able to identify the individual or entity that owns or controls the funds, or conducts, directs or is a beneficiary of the financial transactions. Information could be lacking on individuals or entities involved in the financial transactions, on their relationships, and on the flow of funds. Failing to comply with record keeping requirements could lead to being non-compliant with transaction reporting requirements and having inadequate risk assessments. This could result in FINTRAC missing

key information for its analysis. This could also lead to situations where law enforcement would not be able to collect critical evidence in their investigations and prosecutions of ML/TF offences.

When a record is not kept, or if the information contained in a record is missing, unclear, incomplete or inaccurate, REs, FINTRAC and law enforcement agencies may be prevented from performing their functions effectively and contributing to the objectives of the PCMLTFA.

2.14 Penalty determination for violations related to keeping prescribed records

The Proceeds of Crime (Money Laundering) and Terrorist Activity Financing Administrative Monetary Penalties Regulations (AMP Regulations) allow a penalty ranging from $1 to $1,000 for violations related to record keeping.

FINTRAC has identified four levels of harm related to these violations by considering the intended purpose of the information that must be kept and the consequences of not complying with the requirements on Canada's AML/ATF regime. Levels of harm are also based on our ability to use the information to identify individuals, entities, transactions and the flow of funds, to understand ML/TF risks, and to ensure compliance as described below. The penalty range of $1 to $1,000 is divided into four even intervals. Each level of harm incurs a maximum penalty of either: $1,000, $750, $500 or $250.

The highest level of harm (Level 1), which incurs a penalty of $1,000, is for violations that would have the greatest negative impact on the achievement of the objectives of the PCMLTFA and on FINTRAC's mandate. The lowest of the four levels of harm (Level 4) incurs a penalty of $250. Penalty amounts may be reduced if there are mitigating factors. All factors that may reduce a penalty will be considered, potentially lowering the penalty to the $1 minimum set out in the AMP Regulations.

The information that must be kept under the Act and its regulations can serve one or more purposes. Therefore, non-compliance with one record keeping requirement can cause various harm to the achievement of the objectives of the Act and FINTRAC's mandate. The table below lists the levels of harm, the types of non-compliance and the descriptions of harm along with their corresponding penalty.

Level of harm	Type of non-compliance	Description of harm	Penalty (not considering mitigating factors)
Level 1	Information that identifies individuals or entities that conduct, own, direct, control or benefit from funds and transactions; OR information that identifies the flow of funds/transactions is non-compliant	Prevents the identification of individuals or entities that conduct, own, direct, control, or benefit from funds or financial transactions; OR prevents FINTRAC from iden- tifying the flow of funds/transactions	$1,000
Level 2	Information that identifies relationships or other parties to a transaction is non-compliant	Prevents the identification of relationships	$750
Level 3	Information that can be used to assess ML/TF risks posed by individuals and entities is non-compliant	Prevents the understanding of an individual or entity, including the expected activity, in order to assess ML/TF risk	$500
Level 4	Information to ensure compliance and efficiency in use of records is non-compliant	Reduces the ability to analyze or use the information for risk assessment, intelligence, compliance and investigation purposes in a timely manner	$250

Table 14—Levels of harm and penalties for violations related to keeping pre-

scribed records

2.14.1 Level 1 harm: Information that identifies individuals/entities or the flow of funds/transactions is non-compliant When there is no information on the flow of funds or transactions, it is not possible to pursue ML/TF offences. Those who are responsible for these offences must be held accountable or prevented from committing the crime, so it is equally important to have the information identifying the individuals and entities that conduct, own, direct, control, or benefit from the funds or transactions.

The records that are required for purposes of identifying individuals and entities, transactions and the flow of funds may be the only proof that a transaction was conducted and may be the only way to confirm the involvement of individuals and entities. Without this information, there can be no meaningful risk assessment, no transaction reporting, no analysis, and no investigation and prosecution. If the record is insufficient for use by law enforcement as evidence, the investigation or prosecution of an ML/TF offence may be dropped. Because this poses the highest level of harm, when records that contain information identifying individuals, entities or transactions are not kept, or if the information in the records is unclear, incomplete or inaccurate, the penalty is determined at the maximum of $1,000 per record.

2.14.2 Level 2 harm: Information that identifies relationships or other parties to a transaction is non-compliant The information that identifies the relationships between the individuals and entities that conduct, own, direct, control, or benefit from the funds or transactions can be used for risk assessment, transaction reporting, analysis, and investigations and prosecutions of ML/TF offences. This information indicates to FINTRAC the type and level of involvement of individuals and entities in transactions and is used to prioritize analysis work. When relationship information is missing, FINTRAC's ability to follow the flow of funds can be significantly limited. When the information that serves to identify relationships is not kept, or when the information is unclear, incomplete or inaccurate to the point of being useless, the penalty is $750 per record.

2.14.3 Level 3 harm: Information that can be used to assess ML/TF risks posed by individuals/entities is non-compliant The Act and its regulations require that information on the background of individuals and entities be kept on record. This information helps understand individuals or entities by supplementing identity information, transaction and relationship information. It gives REs more in-depth knowledge of clients which lets them conduct comprehensive assessments of ML/TF risks that go beyond the client identity, transaction and relationship information that must be kept. While this information may not be required in prescribed transaction reports (Large Cash Transaction Reports, Electronic Funds Transfer Reports, Casino Disbursement Reports), it may support the detection of suspicious transactions that must be

reported to FINTRAC, or the identification of activities and areas of higher risk that require enhanced monitoring. If a suspicious transaction report (STR) is submitted, this information could form part of the grounds for suspicion, be included in the report, analyzed by FINTRAC, and disclosed to law enforcement. Therefore, when a record containing this information is not kept, or when the information is unclear, incomplete or inaccurate to the point of being useless, the penalty is $500 per record.

2.14.4 Level 4 harm: Information to ensure compliance and the efficient use of records is non-compliant Certain records are used to verify compliance or to enhance efficiency. They may help support law enforcement investigations, but are not critical for risk assessment or financial analysis. For example, the requirement to record a date could confirm that an RE has carried out a regulatory requirement within the prescribed period. Although this type of information is not critical, it is useful to assess compliance and consequently, the penalty for non-compliance is $250 per record.

2.15 Mitigating factors

In all the cases described above, mitigating factors will be considered and may reduce the penalty. For example, a financial entity that opens an account is required to keep a signature card for each account holder. Failure to keep a signature card poses harm at the highest level (Level 1) because the information that identifies a person is non-compliant. The penalty is $1,000 in this case. However, if the non-compliance is discovered and corrected before transactions are conducted, the penalty could be reduced to $250 (consistent with Level 4), if, considering the circumstances, the non-compliance's only impact is to the use of the record (or the information) for its intended purpose.

2.16 Non-compliance in the case of records that serve more than one purpose

Most of the required records can be useful for more than one of the purposes described above. For this reason, when determining the penalty amount for non-compliant record keeping that results in more than one level of harm, the penalty is determined at the amount corresponding to the highest level of harm. When assessing the level of harm and determining a penalty, FINTRAC takes the entire record into consideration.

3.1 Harm done in the case of violations related to the retention period for prescribed records

Accurate and complete records are fundamental when it comes to supporting the detection, deterrence and prevention of ML/TF offences. Therefore, records must be available when required to assess compliance, or in support of investigations and prosecutions of ML/TF offences. Not keeping a record for the

prescribed retention period poses the same harm as not having kept the record at all. If records are not retained for the required five-year period, they cannot be accessed to conduct risk assessments, reporting and to ensure compliance. Most importantly, missing records may impact law enforcement investigations of ML/TF offences negatively due to lack of evidence.

3.2 Penalty determination for violations related to the retention period for prescribed records

Since not keeping a record for the required five years poses the same harm as not keeping a record, the penalty is the same, $1,000 per instance. Penalty amounts may be reduced if there are mitigating factors.

4.1 Harm done in the case of a violation related to the requirement to provide a record to an authorized person

The Act and its regulations require records to be kept in a format that can be produced within 30 days when FINTRAC requests to examine it.Footnote 5 Failing to comply with this requirement interferes with FINTRAC's ability to efficiently and effectively ensure compliance with Parts 1 and 1.1 of the PCMLTFA, in accordance with paragraph 40(e) of the PCMLTFA.

4.2 Penalty determination for a violation related to the requirement to provide a record to an authorized person

As failing to comply with this obligation would impact FINTRAC's ability to verify compliance with regulatory requirements in a timely manner, the penalty is set at $250 per record produced after the prescribed period. This is consistent with the amount corresponding to "Information to ensure compliance and efficiency in use of records is non-compliant" (Level 4), as shown in Table 14. When a record is not produced after an extensive delay beyond the prescribed 30-day period, FINTRAC may consider that there is a violation for failing to keep a prescribed record. Penalty amounts may be reduced if there are mitigating factors.

5. Repeated instances of a given violation

When a particular violation occurs multiple times, FINTRAC will consider its underlying cause, its type and other relevant facts to assess whether the level of harm should be reduced for the subsequent instances of that violation. For example, should repeated instances of a given violation affect only the efficiency of FINTRAC's analysis, it may be appropriate to assess its recurring instances at the base penalty of $250 each (Level 4 harm), regardless of the level of harm of the first occurrence.# Guide on harm done assessment for "Know your client" requirements violations

1. Introduction

This page presents how we assess the harm done and calculate the base penalty amount applied to "Know your client" violations.

1.1 Purpose of the guide

This guide presents how FINTRAC approaches the harm done criterion and the base penalty amount for violations under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (the Act) and its regulations. According to section 73.11 of the Act, FINTRAC must consider the harm done by a violation, that the purpose of an administrative monetary penalty (AMP) is to encourage compliance rather than to punish, and all other criteria prescribed in the regulations, including a reporting entity's (RE) history of compliance, when determining the amount of a penalty. Considerations for the non-punitive nature of an AMP and an REs' compliance history are assessed in another step in the penalty calculation and are outlined separately in FINTRAC's AMP policy.

1.2 Definition of harm

FINTRAC defines "harm" as the degree to which a violation interferes with achieving the objectives of the Act Footnote 1 or with FINTRAC's ability to carry out its mandateFootnote 2. Therefore, the consequences of non-compliance, when an AMP is imposed, are linked to its effects on Canada's efforts to combat money laundering and terrorist activity financing (ML/TF).

Compliance enforcement activities are undertaken to prevent and correct the harm that comes from non-compliance with the Act and regulations. REs' adherence to requirements such as record keeping and verifying client identity assists in the deterrence of ML/TF and supports investigations and criminal prosecutions. The requirements related to reporting ensure that FINTRAC is supplied with the high-quality, timely financial transaction reports it needs to produce the financial intelligence that helps with the investigation and prosecution of ML/TF offences.

1.3 Considering harm in AMP calculations

When determining a penalty, FINTRAC considers the harm caused, that is, the degree to which the non-compliance interferes with the purpose of the Act and/or with FINTRAC's mandate. Non-compliance and harm are measured using the standards described in this guide, which outline the benchmark amounts for the corresponding levels of harm for a specific violation. FINTRAC considers the specific circumstances of each case, including the extent of the non-compliance and mitigating factors, which may further reduce the actual amounts applied.

2. Violations related to "Know your client" (KYC) requirements

One of the most important things we can do to protect our financial system from being exploited for ML/TF activities is to remove anonymity from financial transactions.

Criminals convert, conceal and transfer their assets without detection by hiding their identities when conducting financial transactions.

Therefore, requirements such as verifying the identity of individuals, confirming the existence of entities, determining whether a person is acting on behalf of a third party or if an account will be used by a third party, and determining the beneficial ownership of an entity have been put in place to make our financial system less anonymous. As a consequence of these requirements, those who are conducting transactions, and those that are directly or indirectly in control of, or benefit from funds and transactions, will be known and this information will be documented. These measures are of utmost importance to detect, prevent and deter the exploitation of Canada's financial system. Violations related to these requirements interfere with the achievement of subparagraph 3(a)(i) of the Act and result in vulnerabilities in Canada's anti-money laundering and anti-terrorist financing (AML/ATF) regime, particularly when it comes to detecting ML/TF activities and deterring those criminals who would use our financial system for these purposes.

3. Violation related to opening an account when client identity cannot be established

3.1 Harm done in the case of a violation related to opening an account when client identity cannot be established

If an account is knowingly opened but the identity of the account holder cannot be verified, then the account holder can control the funds without being directly associated to the funds, and without being detected. Anonymous financial transactions and activities allow criminals to accumulate, transfer, convert and conceal assets from the authorities. In order to protect Canada's financial system from abuse, financial entities, securities dealers and casinos are prohibited from opening an account for a client whose identity cannot be ascertained.

Verifying the identity of the parties to financial transactions and activities removes the anonymity behind the transactions. This requirement deters those who would launder the proceeds of crime or finance terrorist activities, and when combined with record keeping requirements, it also serves as a tool for law enforcement to investigate and prosecute ML/TF-related offences.

3.2 Penalty determination for a violation related to opening an account when client identity cannot be established

When an account has been opened for client and their identity cannot be verified in accordance with the Act and its regulations, and at least one financial transaction has been conducted on the account, the maximum prescribed penalty of $100,000 is applied. If no transaction has been conducted, FINTRAC may consider this to be a mitigating factor and reduce the penalty.

4. Violations related to verifying client identity

This section outlines FINTRAC's approach to the violations related to the requirement to verify client identity in prescribed circumstances, including the harm assessment and penalty calculation.

4.1 Harm done in the case of violations related to verifying client identity

Verifying the identity of the parties to financial transactions and activities removes the anonymity behind them by identifying the individuals and entities responsible for the movement of the funds. The information collected during the process of verifying identity of an individual, or confirming the existence of an entity, must be recorded so that it can later be used to report to FINTRAC, in the RE's risk assessments and ongoing monitoring of business relationships. Verifying identity is necessary not only to meet client identification requirements, but also to meet record keeping requirements.

Verifying the identity of the parties to financial transactions and activities deters those who would launder the proceeds of crime or finance terrorist activities. When combined with the associated record keeping requirements, client identity verification also provides records and evidence for the ML/TF investigations and prosecutions of ML/TF offences.

Ultimately, without knowing the identity of the individuals involved in financial transactions potentially related to ML/TF offences, REs cannot conduct appropriate risk assessments, ongoing monitoring of business relationships or put in place mitigation measures. Furthermore, FINTRAC and its law enforcement partners cannot follow the flow of funds to combat these illegal activities, prevent future illegal activities, and protect the integrity of Canada's financial system and the safety of Canadians.

4.2 Penalty determination for violations related to verifying client identity

The PCMLTFR set out the ways by which individuals must be identified, and the existence of entities confirmed, as well as the timelines for making these verifications. The requirements were developed to make sure that the verification

of identity is done with methods that are accurate and timely, in support of FINTRAC and law enforcement agencies' purposes.

Given the importance of removing anonymity in financial transactions and activities conducted, when an RE has not taken measures to verify client identity, the maximum penalty of $1,000 per instance will apply, as this constitutes a complete violation or disregard for the requirement.

When the methods used to verify identity are not in accordance with the methods set out in the PCMLTFR, the client's identity is considered not to have been verified, therefore the harm to achieving the objectives of the PCMLTFA and FINTRAC's mandate is the same as with not taking steps to verify client identity and the same penalty ($1,000 per instance) will apply. Relevant mitigating factors of each case will be considered and may reduce the actual penalty amount. For example, if the RE did not verify the identity of the client within the prescribed period, but did so subsequently.

When an account is knowingly opened for a client without verifying client identity or confirming the existence of an entity, this is a violation of the prohibition under section 9.2 of the Act, which is a "serious" violation and carries a maximum penalty of $100,000. See *Violation related to opening an account when client identity cannot be established*.

4.3 Violations related to client identification information records

See the guide on harm done assessment for record keeping violations for the harm rationale and penalty calculation for the violations below.

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
6	64.2	Failure of a person or entity that is required to ascertain a person's identity to keep prescribed information	Minor$1-$1,000

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
6	65(3)	Failure of a person or entity who ascertains information in respect of a corporation by referring to an electronic version of a record to keep a prescribed record	Minor$1-$1,000
6	65(4)	Failure of a person or entity who ascertains information in respect of a corporation by referring to a paper copy of a record to retain the record or a copy of it	Minor$1-$1,000
6	66(3)	Failure of a person or entity who ascertains information in respect of an entity by referring to an electronic version of a record to keep a prescribed record	Minor$1-$1,000

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
6	66(4)	Failure of a person or entity who ascertains information in respect of an entity by referring to a paper copy of a record to retain the record or a copy of it	Minor$1-$1,000

Table 4—Violations related to client identification information records

5. Violations related to third party determination

This section outlines FINTRAC's approach to the violations related to the requirement to make a third party determination, including the harm assessment and penalty calculation.

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
6	8(1)	Failure to take reasonable measures to determine if an individual giving cash is acting on behalf of a third party	Minor$1-$1,000
6	9(1)	Failure to take reasonable measures when opening an account to determine if the account is to be used by or on behalf of a third party	Minor$1-$1,000

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
6	10(1)	Failure to take reasonable measures when client information record is created to determine whether the client is acting on behalf of a third party	Minor$1-$1,000
6	44(1)	Failure of a casino to take reasonable measures to determine if a person who receives a prescribed disbursement is acting on behalf of a third party	Minor$1-$1,000

Table 5—Violations related to third party determination

5.1 Harm done in the case of violations related to third party determination

Criminals who would launder the proceeds of crime or finance terrorist activities often resort to third parties to hide their identity. By doing so, they mask their involvement in the financial transactions and activities, maintain their anonymity while giving instructions for the funds and while retaining the benefits of the funds. The PCMLTFR require RE to take reasonable measures to determine whether a transaction is being conducted on behalf of a third party, whether a client is acting on behalf of a third party or whether an account will be used for the benefit of a third party. Failing to make a third party determination may result in financial transactions and activities being directed by unknown individuals and entities. When this occurs, REs cannot properly assess the risks posed by the transactions/activities, or report on all the parties involved in the transactions conducted. The information on third parties involved in transactions is required to be reported so that FINTRAC can properly conduct analysis to establish relationships, determine the individuals or entities directing transactions and the flow of funds, and law enforcement can effectively investigate

and prosecute ML and TF offences.

5.2 Penalty determination for violations related to third party determination

The PCMLTFR require that reasonable measures be taken to make a third party determination. The reasonable measures taken must be in line with those described in FINTRAC's guidance and documented in the RE's compliance policies and procedures. As reasonable measures include simply asking the client if they are acting on someone else's behalf or retrieving information from existing records, an RE who does not take any measures to make a third party determination has fully interfered with the purpose of the requirement, which is to eliminate anonymity and identify the individuals/entities that are giving instructions on transactions/activities conducted. Given the importance of removing anonymity in financial transactions and activities, the maximum prescribed penalty of $1,000 applies. This amount may be reduced in consideration of the relevant mitigating factors of each situation.

5.3 Violations related to third party information records

See the guide on harm done assessment for record keeping violations for the harm rationale and penalty calculation for the violations below.

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
6	8(2)	Failure to keep a record of prescribed information respecting third parties	Minor$1-$1,000
6	9(2)	Failure to keep a record of prescribed information respecting third parties	Minor$1-$1,000
6	10(2)	Failure to keep a record of prescribed information when it is determined that the client is acting on behalf of a third party	Minor$1-$1,000

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
6	44(2)	Failure of a casino to keep a record of prescribed information when it is determined that the client is acting on behalf of a third party	Minor$1-$1,000

Table 6—Violations related to third party information records

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
6	8(3)	Failure to keep a record of prescribed information respecting suspected third parties	Minor$1-$1,000
6	9(3)	Failure to keep a record of prescribed information in respect of suspected third parties	Minor$1-$1,000
6	10(3)	Failure to keep a record of prescribed information when there are reasonable grounds to suspect that the client is acting on behalf of a third party	Minor$1-$1,000

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
6	44(3)	Failure of a casino to keep a record of prescribed information when there are reasonable grounds to suspect that the client is acting on behalf of a third party	Minor$1-$1,000

Table 7—Violations related to suspected third party information records

6. Violation related to inter vivos trust information records

See the guide for harm done assessment for record keeping violations for the harm rationale and penalty calculation for the following violation.

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
6	11	Failure of a trust company to keep a record of prescribed information concerning inter vivos trusts	Minor$1-$1,000

Table 8—Violation related to inter vivos trust information records

7. Violation related to beneficial ownership

7.1 Harm done in the case of a violation related to beneficial ownership

Removing anonymity and identifying the **natural** persons behind transactions and account activities is a key component of Canada's AML/ATF regime. Beneficial owners hiding behind entities, including corporations is a technique used in many ML/TF schemes. An important step in the detection, prevention and deterrence of ML/TF is the collection and verification of beneficial ownership

information, which also support ML/TF investigations, and ultimately protect the integrity of Canada's financial system and the safety of Canadians.

If measures are not taken to obtain this information, there is a risk that transactions and account activities will be conducted without knowing the individuals controlling, benefitting from, or giving the instructions for the transactions. This could completely interfere with the objective of subparagraph 3(a)(i) of the PCMLTFA. This also prevents the RE from properly assessing the risks associated, law enforcement from effectively investigating and prosecuting ML and TF offences, and FINTRAC from using the information in support of its mandate, particularly in cases where the information helps establish reasonable grounds to suspect that a transaction is related to an ML/TF offence.

7.2 Penalty determination for a violation related to beneficial ownership

If an RE fails to obtain the prescribed information on the persons controlling an entity, the detection, prevention and deterrence purpose of this requirement, as described above, is completely impeded. Given the importance of removing anonymity in financial transactions and activities, the prescribed maximum penalty of $1,000 applies. This amount may be reduced in consideration of mitigating factors for each situation.

8. Violation related to confirming the accuracy of information on the control of an entity

8.1 Harm done in the case of a violation related to confirming the accuracy of information on the control of an entity

The requirement to take reasonable measures to confirm the accuracy of the prescribed information is not only to ensure the reliability of the information obtained, but also to deter clients from providing false information regarding the control, ownership or structure of entities. Removing anonymity from transactions is a key component of the detection, prevention and deterrence of ML and TF. Failing to take reasonable measures to confirm the accuracy of the prescribed information may result in unreliable information and in the true identity of the individuals behind transactions remaining unknown. In such situations, law enforcement cannot rely on the information to investigate or prosecute ML/TF offences, the RE cannot conduct proper risk assessments and ongoing monitoring of business relationships. In a worst case scenario, should the accuracy of beneficial ownership information be the only fact for establishing reasonable grounds to suspect that a transaction or attempted transaction is related to an ML/TF offence, it could result in an unreported suspicious transaction as that relevant suspicion would be missing. In the case where a suspicious transaction report (STR) was submitted containing beneficial ownership information in Part G that was not confirmed for accuracy, it could result in FINTRAC analyzing incomplete or inaccurate information and therefore the

true flow of funds or individuals behind suspicious transactions could not be established.

8.2 Penalty determination for a violation related to confirming the accuracy of information on the control of an entity

Given the importance of removing anonymity in financial transactions and account activities, the maximum prescribed penalty of $1,000 applies. This amount may be reduced in consideration of relevant mitigating factors of each situation.

9. Violation related to records on beneficial ownership information

See the guide on harm done assessment for record keeping violations for the harm rationale and penalty calculation for the violation below.

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
6	11.1(3)	Failure to keep a record of the prescribed information and the measures taken to confirm its accuracy	Minor$1-$1,000

Table 11— Violation related to records on beneficial ownership information

10. Violation related to ascertaining the identity of an entity's most senior managing officer

10.1 Harm done in the case of a violation related to ascertaining the identity of an entity's most senior managing officer

One of the most important things we can do to protect our financial system from being exploited for ML/TF purposes is to remove anonymity from financial transactions. It is important, not only to confirm the existence of an entity, but to also take reasonable measures to identify the individuals who are in control of it. When an RE is unable to obtain or confirm the accuracy of beneficial ownership information, individuals could be controlling an entity anonymously. This poses a higher risk for ML/TF offences, as individuals with criminal intent may remain undetected while potentially higher-risk activities are overlooked. Therefore, when the beneficial ownership information of an entity is not clear or cannot be established, an RE must verify the identity of the most senior person

who can control the financial transactions of the entity, and treat the activities of the entity as high risk. Failing to take these additional measures could leave Canada's financial system vulnerable to ML and TF caused by individuals criminally utilizing the entities they control anonymously.

10.2 Penalty determination for a violation related to ascertaining the identity of an entity's most senior managing officer

Failing to take reasonable measures to verify the identity of the most senior managing officer and treat the activities of the entity as high risk will result in the prescribed maximum penalty of $100,000. This amount may be reduced in consideration of relevant mitigating factors each situation.

11. Violations related to politically exposed persons (PEP) and heads of international organizations (HIO) determination

11.1 Harm done in the case of violations related to PEP and HIO determination

A PEP or HIO is a person entrusted with a prominent position that typically comes with the opportunity to influence decisions and the ability to control resources. The influence and control a PEP or HIO puts them in a position to impact policy decisions, institutions and rules of procedure in the allocation of resources and finances, which can make them vulnerable to corruption. It is important to understand that the possibility for corruption exists, and that PEPs and HIOs can be vulnerable to carrying out, or being used for, ML/TF offences.

The requirements concerning PEPs, HIOs and their family members and close associates have been put in place because of concerns about their higher vulnerability to corruption, and related higher risk of money laundering. Canada and the Financial Action Task Force (FATF) attach a great deal of importance to the fight against corruption as it has the potential to bring great harm to economic development, the fight against organized crime and the respect for law and effective governanceFootnote 5.

Therefore, under prescribed circumstances, financial entities; securities dealers; life insurance companies, brokers, and agents; and money services businesses are required to take reasonable measures to identify PEPs, HIOs, family members and persons closely related to them so that prescribed measures can be taken to mitigate risks. If REs fail to make the determination, risk mitigation measures cannot be applied.

11.2 Penalty determination for violations related to PEP and HIO determination

The determination of PEPs, HIOs and their family members and close associates, is the pre-requisite to taking the prescribed measures to mitigate risks. Without first making the determination, no mitigating measures can be applied and potentially higher-risk clients and their activities could remain undetected. As such, this type of violation carries the maximum penalty of $1,000. This amount may be reduced in consideration of the relevant mitigating factors of each situation. For example, should FINTRAC become aware of the violation prior to any transaction being conducted, the penalty may be reduced to the lower end of the penalty range to an amount that is sufficient to encourage compliance with the requirement, while recognizing that the potential harm is reduced considering that no transactions have been conducted.

12. Violations related to source of funds determination

12.1 Harm done in the case of violations related to source of funds determination

Once it has been determined that an individual is a PEP, a HIO, a family member or close associate, REs are required to determine the source of the funds that have been, will be or are expected to be deposited into an account; or to establish the source of the funds used in a prescribed transaction. The requirements concerning PEPs, HIOs, their family members and close associates have been put in place because of concerns over these individuals' higher vulnerability to corruption and related higher risk of money laundering. These requirements mitigate the inherent risks by allowing REs to know their clients, which deters criminal elements, by allowing REs to assess the ML/TF risk through the identification of the source of the funds, and through the detection of transactions that must be reported. Not complying may result in the improper assessment of ML/TF risks, which potentially leads to not applying the required mitigation measures and not reporting to FINTRAC.

12.2 Penalty determination for violations related to source of funds determination

Once it has been determined that a client is a PEP, HIO, family member or close associate, a higher risk situation has been identified. Not taking reasonable measures to determine the source of funds for these higher-risk clients will result in the prescribed maximum penalty of $1,000 per instance. This amount may be reduced in consideration of the relevant mitigating factors of each situation. For example, should FINTRAC become aware of the violation prior to any transaction being conducted, the penalty may be reduced to the lower end of the penalty range to an amount that is sufficient to encourage compliance with the requirement, while recognizing that the potential harm is reduced considering no transactions have been conducted.

13. Violations related to obtaining senior management approval to keep an account open or reviewing a prescribed transaction

13.1 Harm done in the case of violations related to obtaining senior management approval to keep an account open or reviewing a prescribed transaction

The requirements concerning PEPs, HIOs, their family members and close associates have been put in place because of concerns over these individuals' higher vulnerability to corruption and related higher risk of money laundering. Canada and the FATF attach a great deal of importance to the fight against corruption because corruption can harm economic development; interfere with the fight against organized crime, and with respect for the law and effective governance-Footnote 6. When the approval to keep an account open is not obtained, or when a transaction is not reviewed by senior management, higher ML/TF risks may not be properly assessed and understood sufficiently to conduct effective risk assessments and to ensure that the proper mitigation measures are applied.

13.2 Penalty determination for violations related to obtaining senior management approval to keep an account open or reviewing a prescribed transaction

Once it has been determined that a client is a PEP, HIO, family member or close associate, a higher-risk situation has been identified. Failing to obtain senior management's approval to keep the account open or failing to ensure that senior management reviews prescribed transactions in these higher-risk situations will result in the maximum penalty of $1,000 per instance. This amount may be reduced in consideration of the relevant mitigating factors of each situation. For example, should FINTRAC become aware of the violation prior to any transaction being conducted, the penalty may be reduced to the lower end of the penalty range to an amount that is sufficient to encourage compliance with the requirement, while recognizing that the potential harm is reduced considering that no transactions have been conducted.

14. Violations related to records for PEPs and HIOs

14.1 Violation related to enhanced ongoing monitoring of activities in respect of a PEP or HIO's account

This section outlines FINTRAC's approach to the violation related to enhanced ongoing monitoring of the activity on PEP and HIO's accounts, including the harm assessment and penalty calculation.

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
9.3(2)	67.1(1)(c) and (2)	Failure of a financial entity or securities dealer to conduct enhanced ongoing monitoring of the activities in respect of an account	Minor$1-$1,000

14.2 Harm done in the case of a violation related to enhanced ongoing monitoring of activities in respect of a PEP or HIO's account

When there is the potential for an increased risk of ML/TF offence, such as when a client is a politically exposed foreign person, or their family member or close associate, enhanced ongoing monitoring the client's account is a key measure that supports the detection, prevention and deterrence of ML/TF. Without enhanced ongoing monitoring, the level of scrutiny may not be appropriate to detect the transactions that would raise concern, which could result in the failure to detect the suspicious transactions or attempted suspicious transactions that are required to be reported to FINTRAC.

Ongoing monitoring must be conducted for the purposes of 1) detecting suspicious transactions that are required to be reported, 2) keeping client information up to date, 3) reassessing the level of risk, and 4) determining whether the transactions and activities are consistent with the information and risk level associated to a given client. Enhanced ongoing monitoring means that the above listed measures are conducted more frequently. When only some of the prescribed enhanced ongoing monitoring measures are conducted, or when all measures are conducted but not more frequently than for a lower risk situation, the ML/TF risks are only partially mitigated. Therefore, the penalty amount may be reduced based on the circumstances. When not performing enhanced ongoing monitoring results in the failure to report an STR, a separate violation and penalty can be imposed.

14.3 Penalty determination for a violation related to enhanced ongoing monitoring of activities in respect of a PEP or HIO's account

The penalty is set at the prescribed maximum amount of $1,000 for each account where enhanced ongoing monitoring is not conducted. This violation poses a high level of harm to the achievement of the objectives of the PCMLTFA and of FINTRAC's mandate, since the activity on an account held by an individual identified as being vulnerable to ML/TF offences could remain overlooked;

in some cases, this may also result in the failure to report suspicious transactions. This amount may be reduced in consideration of mitigating factors for each situation. For example, if no activity was conducted within the PEP or HIO's accounts prior to FINTRAC identifying the violation.

15. Violation related to ongoing monitoring of business relationships

15.1 Harm done in the case of a violation related to ongoing monitoring of business relationships

The requirement to conduct ongoing monitoring of a business relationship is in place to protect REs and Canada's financial system from ML/TF.

Failing to comply with the ongoing monitoring requirement can impact the objectives of the PCMLTFA which are to detect, prevent and deter ML/TF. When an RE fails to conduct ongoing monitoring of business relationships, it is unaware of changes to the client's transactions, activities, and circumstances; especially those that may pose a higher risk of ML/TF. When the RE is unaware, the client's information and risk assessment are not updated to reflect the true level of risk. This can potentially result in ineffective risk mitigation, and unreported transactions. When a high-risk client or business relationship is undetected because of a lack of ongoing monitoring, the RE's operations and Canada's financial system could be at risk. Should a lack of ongoing monitoring result in the failure to submit STRs, there is also an impact on FINTRAC's mandate which is to analyze and disclose information to assist in the detection, prevention and deterrence of ML/TF.

In addition, the requirement to record the measures taken and the information obtained demonstrates compliance with continuously assessing ML/TF risks, applying appropriate mitigation measures and detecting information that is required to be reported to FINTRAC. These reports support FINTRAC's analysis and disclosure mandate, which provides valuable financial intelligence to law enforcement agencies. Not keeping a record of the information obtained would not only interfere with the purposes listed above, but could also affect law enforcement investigations and prosecutions of ML/TF if client information is not up to date.

15.2 Penalty determination for a violation related to ongoing monitoring of business relationships

The Proceeds of Crime (Money Laundering) and Terrorist Financing Administrative Monetary Penalties Regulations (AMP Regulations) allow for a penalty ranging from $1 to $1,000 for violations of ongoing monitoring requirements.

FINTRAC has identified four levels of harm related to these violations by considering their impact on the objectives of the PCMLTFA or on FINTRAC's mandate. To create a penalty scale based on harm done, the above-mentioned

penalty range is divided in four to correspond with the identified levels of harm: $1,000, $750, $500 and $250.

The highest harm category (Level 1) is assigned the maximum amount of $1,000 as it would have the greatest effect on the objectives of the PCMLTFA or on FINTRAC's mandate. The lowest of the four harm levels (Level 4) has a penalty of $250. Penalty amounts may be reduced if there are mitigating factors, but must be enough to encourage a change in compliance behaviour.

We consider all factors that may reduce a penalty to the $1 minimum set out in the AMP Regulations.

15.2.1 Level 1 harm—No ongoing monitoring measures conducted In situations where no ongoing monitoring measures are taken, the potential impact on the objectives of the PCMLTFA and on FINTRAC's mandate is the greatest; therefore the harm posed is highest. As such, the penalty is determined at the prescribed maximum of $1,000.

15.2.2 Level 2 harm—Reassessment of risk levels and transaction monitoring not conducted In cases where some ongoing monitoring measures are taken and the non-compliance relates to the risk assessment or transaction monitoring, the harm is somewhat reduced compared to Level 1. However, this type of non-compliance could lead to the ineffective mitigation of ML/TF risks posed by the business relationship, or to the ineffective detection of suspicious transactions that need to be reported. This would pose high harm to the achievement of the objectives of the PCMLTFA and FINTRAC's mandate, therefore the penalty is set at $750.

15.2.3 Level 3 harm—Client information not kept up to date In cases where some ongoing monitoring measures are conducted and the non-compliance relates to keeping client information up to date, the harm on the objectives of the PCMLTFA and on FINTRAC's mandate is significant, but less important when non-compliance can affect ML/TF risk mitigation. While incomplete or outdated client information can be used in transaction reports or in law enforcement investigations, higher risk transactions may still be detected, mitigated, and reported to FINTRAC for analysis. As such, the penalty is set at $500.

15.2.4 Level 4 harm—Minor record keeping non-compliance When ongoing monitoring measures are taken and the non-compliance relates to record keeping requirements that do not prevent the use of the information for risk assessments, risk mitigation, transaction reporting, intelligence analysis, compliance and investigations in a timely manner, the harm to the achievement of the objectives of the PCMLTFA and FINTRAC's mandate is reduced. As such, the penalty is set at $250.

16. Violations related to treating the activities of a person or an entity as high-risk

16.1 Harm done in the case of violations related to treating the activities of a person or an entity as high-risk

The PCMLTFR set out specific circumstances under which an RE must treat the activities of clients as high-risk and apply the prescribed special measures to mitigate the heightened risks. The prescribed special measures that are required to be taken are the development and application of written policies and procedures for taking enhanced measures, based on the risk assessment undertaken, to ascertain the identify of clients, and taking any other enhanced measures to mitigate risks including keeping client information up to date and conducting ongoing monitoring of business relationships for the purpose of detecting suspicious transactions that are required to be reported to FINTRAC. Failure to do so would mean that the necessary controls, policies and processes are not in place to for high risk situations and consequently, high-risk transactions and activities could be allowed to proceed without mitigation and reporting. This could result in STRs not being submitted to FINTRAC, and information not being available for analysis and disclosure to police and law enforcement. Ultimately, this could leave Canada's financial system and Canadians vulnerable to abuse for ML/TF purposes.

16.2 Penalty determination for violations related to treating the activities of a person or an entity as high-risk

The AMP Regulations allow for a penalty ranging from $1 to $100,000 for failing to treat prescribed client activities as high-risk and taking the prescribed special measures. FINTRAC has identified five levels of harm related to these violations by considering their impact on the objectives of the PCMLTFA or on FINTRAC's mandate. To create a penalty scale based on harm done, the above-mentioned penalty range is divided in five to correspond with the identified levels of harm: $100,000, $75,000, $50,000, $25,000 and $10,000.

The highest harm category (Level 1) is assigned the prescribed maximum amount of $100,000 as it would have the greatest effect on the objectives of the PCMLTFA or on FINTRAC's mandate. The lowest of the five harm levels (Level 5) has a penalty of $10,000. The rationale for setting this amount as the lowest is based on the notion set out in subsection 4(2) of the AMP Regulations which establishes that a series of "minor" violations amounting to a total penalty of $10,000 or more is considered a "serious" violation.

Penalty amounts may be reduced if there are mitigating factors, but the amount must be enough to encourage a change in compliance behaviour with respect to high-risk activities. We consider all factors that may reduce a penalty to the $1 minimum set out in the AMP Regulations.

16.2.1 Level 1 harm—Specified client activities are not treated as high-risk and there are no policies and procedures on prescribed special measures When an RE fails to treat prescribed activities as high-risk and there are no policies and procedures for taking enhanced measures to mitigate the risks, there is a weakness at the compliance program level which poses the most harm. If there is no system in place to ensure that enhanced measures are applied to mitigate the high risk posed by certain activities, it is more likely that the objectives of the PCMLTFA which are to detect, prevent and deter ML/TF would be hindered. This could leave both the RE's operations and Canada's financial system more vulnerable to ML/TF. An RE in this situation would not have set out the concrete steps to take in order to reduce or prevent those risks. High-risk clients, transactions and activities could go undetected while suspicious transactions are not reported to FINTRAC. Unreported suspicious transactions lead to a loss of intelligence for investigations of ML/TF offences. Therefore the maximum penalty of $100,000 applies under these circumstances.

16.2.2 Level 2 harm—Policies and procedures for taking enhanced measures are developed but not applied The second highest level of harm relates to cases where policies and procedures related to taking enhanced measures for high-risk exist, but they are not being applied in practice. As mitigating measures are not taken, the prescribed activities are in fact not being treated as high-risk according to the requirements set out in the PCMLTFR. Therefore, the impact is nearly the same as in Level 1. However, an RE in this situation could more readily apply the procedures that it has developed in order to mitigate high-risk activities; therefore the harm done is potentially reduced. The penalty is $75,000 which remains at the higher end of the prescribed range but is less than that of Level 1 harm.

16.2.3 Level 3 harm—Enhanced ongoing monitoring, for purposes of detecting suspicious transactions, not conducted In cases where some enhanced measures are taken but the non-compliance relates to the requirement to conduct enhanced ongoing monitoring for the purpose of detecting suspicious transactions to be reported, the harm done is less than in the two previous circumstances. While other prescribed special measures are taken that could mitigate some risks, the potential unreported suspicious transactions can have a significant impact on FINTRAC's intelligence mandate, the investigation or prosecution of ML/TF offences, and other objectives of the PCMLTFA. Therefore, the penalty is set at mid-range, which is $50,000.

16.2.4 Level 4 harm—Enhanced measures are not taken to verify client identification or keep client information, including beneficial ownership information, up to date REs are required to take enhanced measures to ascertain the identity of clients whose activities are deemed high risk. Taking enhanced measures means doing more than what is set out in regular identity verification procedures, to ensure that the identity of the client is

verified and that transactions and activities are not conducted anonymously. If an RE fails to apply these enhanced measures, some risks would not be mitigated and it could leave the RE's operations and Canada's financial system vulnerable to ML/TF. Similarly, if an RE does not take enhanced measures to keep client information up to date in situations of high-risk, outdated or incomplete information could be used in risk assessments, transaction reports, or investigations. The harm posed is less than in Level 3, as some client information is still available although not necessarily complete or up to date. As such, the penalty is set at $25,000.

16.2.5 Level 5 harm—Other enhanced measures not taken to mitigate risks identified When the non-compliance relates to the failure to develop and apply policies and procedures to take any other enhanced measures to mitigate the risks identified (i.e., other than performing enhanced measures to verify client identification, conduct ongoing monitoring and keep client information up to date), effective risk assessment and mitigation, and the timely and efficient availability of information for transaction reporting, analysis, compliance and investigations ML/TF are diminished. The penalty is set at $10,000.

17. Repeated instances of a given violation

When a particular violation occurs multiple times, FINTRAC will consider its underlying cause, its type and other relevant facts to assess whether the level of harm should be reduced for the subsequent instances of that violation. For example, should repeated instances of a given violation only affect the efficiency of FINTRAC's analysis, it may be appropriate to assess its recurring instances at the base penalty of $250 (level 4 harm), regardless of the level of harm of the first occurrence.# Politically exposed persons and heads of international organizations guidance

Overview

All reporting entities (REs) have politically exposed persons (PEPs) and heads of international organizations (HIOs) requirements under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and associated Regulations. However, some requirements and the examples given in this guidance may only apply to certain REs.

References to PEPs in this guidance include both foreign and domestic PEPs, unless otherwise specified.

The access, influence and control that PEPs and HIOs have can make them vulnerable to corruption and the potential targets of criminals who could exploit their status and use them, knowingly or unknowingly, to carry out money laundering (ML) or terrorist activity financing (TF) offences.Footnote 1 The family members and close associates of PEPs and HIOs are potential targets as well because they can more easily avoid detection.

This guidance explains your obligations under the PCMLTFA and associated Regulations in relation to determining who are PEPs, HIOs, and persons related or closely associated to them. It also provides clarity on related terminology and considerations.

1. Who is a domestic PEP?

A **domestic PEP** is a person who currently holds, or has held within the last 5 years, a specific office or position in or on behalf of the Canadian federal government, a Canadian provincial (or territorial) government, or a Canadian municipal government. Specifically, the person has held the office or position of:Footnote 2

- Governor General, lieutenant governor or head of government;
- member of the Senate or House of Commons or member of a legislature;
- deputy minister or equivalent rank;
- ambassador, or attaché or counsellor of an ambassador;
- military officer with a rank of general or above;
- president of a corporation that is wholly owned directly by His Majesty in right of Canada or a province;
- head of a government agency;
- judge of an appellate court in a province, the Federal Court of Appeal or the Supreme Court of Canada;
- leader or president of a political party represented in a legislature; or
- mayor, reeve or other similar chief officer of a municipal or local government**.

****Note**: In line with legislation across Canada, municipal governments include cities, towns, villages and rural (county) or metropolitan municipalities. As such, a mayor is the head of a city, town, village and rural or metropolitan municipality, regardless of the size of the population.

A person **ceases** to be a domestic PEP **5 years** after they have left office or **5 years** after they are deceased.Footnote 3 You must continue to mitigate the risks associated with domestic PEPs until they cease to be domestic PEPs.

2. Who is a foreign PEP?

A **foreign PEP** is a person who holds or has held one of the following offices or positions in or on behalf of a foreign state:Footnote 4

- head of state or head of government;
- member of the executive council of government or member of a legislature;
- deputy minister or equivalent rank;
- ambassador, or attaché or counsellor of an ambassador;
- military officer with a rank of general or above;
- president of a state-owned company or a state-owned bank;
- head of a government agency;

- judge of a supreme court, constitutional court or other court of last resort; or
- leader or president of a political party represented in a legislature.

These persons are foreign PEPs regardless of citizenship, residence status or birthplace.

Once you determine that a person is a foreign PEP, they remain a foreign PEP **forever**(including deceased foreign PEPs). You are not required to determine whether they are a foreign PEP again.Footnote 5

3. Who is a HIO?

A HIO is a person who currently holds or has held within the last 5 years the specific office or position of head of an international organization and the international organization that they head or were head of is either:Footnote 6

1. an international organization established by the governments of states;
2. an institution of an organization referred to in 1 above; or
3. an international sports organization.

An institution established by an international organization does not have to operate internationally and it is possible that an institution only operates domestically, or in one jurisdiction.

The HIO is the primary person who leads the organization. For example, the HIO could be a president or CEO.

A person **ceases** to be a HIO **5 years** after they are no longer the head of the organization or institution or **5 years** after they are deceased.Footnote 7 You must continue to mitigate the risks associated with HIOs until they cease to be HIOs.

4. What is an international organization?

To determine whether a person is a HIO, you must first determine whether you are dealing with an international organization. An international organization is set up by the governments of more than one member country, has activities in several countries, and is bound by a formal agreement among member countries. An international organization has its own legal status, and it is an entity that is distinct from the member countries.

Looking at how an organization was established will help you to determine if it is an international organization. For example, if the organization was established by a formally signed agreement between the governments of more than one country, then it is likely an international organization, and the head of that organization is a HIO.

International organizations are recognized by their member countries, but they are not resident organizations of any country. For examples of international

organizations and institutions established by international organizations, see Annex 1.

5. Who is a family member of a PEP or HIO?

If a person is a PEP or HIO, some of their family members are considered family members of PEPs or HIOs under the PCMLTFA and associated Regulations. These family members are:Footnote 8

- their spouse or common-law partner;
- their biological or adoptive child(ren);
- their mother(s) or father(s);
- the mother(s) or father(s) of their spouse or common-law partner (mother-in-law or father-in-law); and
- the child(ren) of their mother or father (sibling(s)).

Once you determine that a person is a family member of a foreign PEP (including a deceased foreign PEP), they remain a family member of a foreign PEP forever and you are not required to make this determination again.Footnote 9

Once you determine that a person is a family member of a domestic PEP or HIO, they remain a family member of a domestic PEP or HIO until five years after the domestic PEP or HIO has left office.Footnote 10 In the case of a deceased domestic PEP or HIO, persons that are their family members remain a family member of a domestic PEP or HIO for five years after the domestic PEP or HIO ceases to be a domestic PEP or HIO. So, you must continue to mitigate the risks associated with the family members of domestic PEPs or HIOs during that time.

Is a PEP or HIO's ex-spouse or partner considered a family member?

An ex-spouse or partner may continue to have access to a PEP or HIO's funds even when a divorce has taken place or a relationship has ended. Therefore, in the case of:

- the ex-spouse or partner of a **foreign PEP**, they are considered a family member of a foreign PEP forever; and
- the ex-spouse or partner of a **domestic PEP or HIO**, they are considered a family member of a domestic PEP or HIO until the domestic PEP or HIO ceases to be a domestic PEP or HIO.

Is a PEP or HIO's stepchild or step-sibling considered a family member?

A step family relationship does not fall under the definition of a family member unless a child is legally adopted. For example, if Helen is a domestic PEP, and she has legally adopted her stepdaughter, then her stepdaughter is her child under the law and is considered to be the family member of a domestic PEP.

Similarly, if a marriage includes step-siblings, these step-siblings are not considered family members if they are not legally adopted by the stepparent. However, you may want to consider the step family members as close associates of the PEP or HIO, depending on their relationship.

Is the niece or nephew of a PEP or HIO considered a family member?

No. Only the family members of a PEP or HIO listed in this guidance must be regarded as family members of PEPs or HIOs. For example, if John is a PEP, then John's brother, Sam, is considered a family member of a PEP, however, Sam's daughter (John's niece) is not considered a family member of a PEP. However, you may want to consider extended family members as close associates of the PEP or HIO, depending on their relationship.

6. Who is considered a close associate of a PEP or a HIO?

A close associate can be a person who is connected to a PEP or HIO for personal or business reasons. Examples of relationships that could indicate that someone is a close associate (personal or business) could include, but are not limited to, persons who:

- are the business partners of, or who beneficially own or control a business with, a PEP or HIO;
- are in a romantic relationship with a PEP or HIO;
- are involved in financial transactions with a PEP or a HIO;
- serve as prominent members of the same political party or union as a PEP or HIO;
- serve as a member of the same board as a PEP or HIO;
- carry out charitable works closely with a PEP or HIO; or
- are listed as joint on a policy where one of the holders may be a PEP or HIO.

Once you determine that a person is the close associate of a PEP or HIO, they remain a close associate until they lose that connection.

7. What does it mean to "detect a fact" about a PEP or HIO?

Detecting a fact about a PEP or HIO is to discover (proactively or not) information about a person that could lead you to make a PEP or HIO determination or to update information about a known PEP or HIO. You detect a fact when you discover PEP or HIO related information about a person that has an account-based business relationship **or** a non-account-based business relationship with you, outside of your periodic review of existing clients. The information that you detect must be a fact that constitutes **reasonable grounds to suspect** that a person is a PEP, HIO, or family member or close associate of a PEP or HIO.

There is no requirement for you to have proactive processes in place to detect facts about existing clients, but if you do detect information related to a PEP or HIO determination, then you must act on that information. For example, you might detect a fact that would require further action based on information obtained from an existing client, monitoring efforts you may already have in place, knowledge of domestic and world events, or a search run against an open source or third party database.

While a name match is a fact, it is not necessarily a fact that constitutes reasonable grounds to suspect that an existing client is a PEP, HIO, or family member or close associate of a PEP or HIO. As a best practice, you could apply additional criteria (for example, address, date of birth, age, transaction activities, etc.) to a name match, to meet the reasonable grounds to suspect threshold.

8. How do I establish the source of funds, source of virtual currency (VC), or source of a person's wealth?

Once you have determined that a person is a PEP, HIO, or a family member or close associate of a PEP or HIO (in certain circumstances, as applicable), you must take reasonable measures to establish the source of the funds or source of VC used for a transaction or that is expected to be deposited into an account, and the source of a person's wealth. To do this you could take measures such as:

- asking the person; or
- referring to open source information available about the person.

If a transaction or the account activity is inconsistent with the information you have about the source of funds or source of VC, or the source of the person's wealth, then you may want to follow up with the client for clarification. If the information remains inconsistent with what you know about the person, or you are not satisfied with their response and have reasonable grounds to suspect that a transaction or deposit is related to the commission or the attempted commission of an ML or TF offence, you must file a suspicious transaction report.

9. Who can review a transaction or allow an account to stay open?

A member of senior management must review transactions and allow certain accounts to stay open. A member of senior management is a person who has:

- the authority to make management decisions about transactions or accounts and is accountable for them;
- awareness of the ML or TF risks to which you are exposed; and
- awareness and understanding of your obligations related to PEPs, HIOs, and their family members and close associates.

If you are a sole proprietor with no employees, agents or other persons authorized to act on your behalf, you are considered to be the senior manager.

10. Should I treat a PEP or HIO as a high-risk client?

You must treat all persons that you determine to be **foreign PEPs** or **family members or close associates of foreign PEPs** as posing a high risk.

Persons that you determine to be **domestic PEPs**, **HIOs**, or **family members or close associates of domestic PEPs or HIOs** must, be treated as high-risk if you consider, based on your risk assessment, that there is a **high-risk** of an ML or TF offence being committed.

Once you determine that there is a high risk of an ML or TF offence being committed, you must take the measures prescribed in the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations. These measures should be detailed in your written compliance policies and procedures for high-risk clients. For more information about risk assessment considerations for PEPs or HIOs see FINTRAC's Risk assessment guidance.# Methods to verify the identity of persons and entities

From: Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)

Overview

This guidance came into effect on June 1, 2021.

This guidance explains the methods that can be used by reporting entities (REs) to verify the identity of a person or an entity.

Note: For specific information on when to verify the identity of a person or an entity (the timing requirement) for your business sector, refer to the related guidance by business sectors.

Who is this guidance for

The requirement to verify the identity of a person or an entity under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and associated Regulations applies to all reporting entities

1. Meaning of verifying the identity of a person or an entity

It means to use the methods described in this guidance to ensure that the information in an identification document or from other informational sources matches the information that the person or entity provided.

Verifying identity is a foundational element of Canada's anti-money laundering and anti-terrorist financing regime and a key component of an RE's relationship

with clients. It helps you to know your clients and to understand and assess any risk that may be associated to their transactions or activities.

2. How to verify the identity of a person

You can use any of the 5 methods described below to identify a person:

1. 2.1 Government-issued photo identification method
2. 2.2 Credit file method
3. 2.3 Dual-process method
4. 2.4 Affiliate or member method
5. 2.5 Reliance method

2.1 Government-issued photo identification method

You may verify the identity of a person by referring to a government-issued photo identification document.Footnote 1 To do so, the document must:

- be **authentic**, **valid and current**;Footnote 2
- be issued by a federal, provincial or territorial government (or by a foreign government if it is equivalent to a Canadian document);
- indicate the person's name;
- include a photo of the person;
- include a unique identifying number; and
- match the name and appearance of the person being identified.

Photo identification documents issued by municipal governments, Canadian or foreign, are not acceptable. See Annex 4 for examples of acceptable government-issued photo identification documents.

You can determine whether a government-issued photo identification document is **authentic, valid and current** by viewing it **in person**, and by looking at the characteristics of the original physical document and its security features (or markers, as applicable) **in the presence of the person being identified**. This will allow you to be satisfied that the identification document is authentic, as issued by the competent authority (federal, provincial, or territorial government), valid (unaltered, not counterfeit) and current (not expired).

Using the government-issued photo identification method if a person is not physically present You may use the government-issued photo identification method if a person is **not physically present**, but you must have a **process in place to authenticate** the government-issued photo identification document. For instance, you could assess a document by using a technology capable of determining the document's authenticity. For example, you could:

- ask a person to scan their government-issued photo identification document using the camera on their mobile phone or electronic device; and

- use a technology to compare the features of the government-issued photo identification document against known characteristics (for example, size, texture, character spacing, raised lettering, format, design), security features (for example, holograms, barcodes, magnetic strips, watermarks, embedded electronic chips) or markers (for example, logos, symbols) to be satisfied that it is an authentic document as issued by the competent authority (federal, provincial, or territorial government).

When a person **is not physically present,** you must still determine whether the authenticated government-issued photo identification document is **valid** and **current,** and that the name and photo are those of the person providing the document. For example, you could:

- participate in a live video chat session with the person and compare the name and the features of the live video image to the name and photo on the authentic government-issued photo identification document; or
- ask the person to take a "selfie" photo using the camera on their mobile phone or electronic device, and use an application to apply facial recognition technology to compare the features of that "selfie" to the photo on the authentic government-issued photo identification document. You would also need a process to compare the name on the government-issued photo identification document with the name provided by the person.

Note: It is not enough to only view a person and their government-issued photo identification document through a video conference or another type of virtual application.

Your compliance program's policies and procedures must describe the processes you follow to determine whether a government-issued photo identification document is authentic, whether the client is present or not, and how you will confirm that it is valid and current. Your policies and procedures must also describe the steps you use to confirm that the name and photograph are those of the person. Your processes to determine that a government-issued photo identification document is authentic, valid, and current, **and** the verification step (ensuring that the name and photo match the name and appearance of the person), do **not** need to happen at the same time. It is up to you to determine the timing, but you must complete both steps.

Record keeping requirements for the government-issued photo identification method If you use the government-issued photo identification method, you must record:Footnote 3

- the person's name;
- the date on which you verified the person's identity;
- the type of document used (for example, driver's licence, passport, etc.);
- the unique identifying number of the document used;
- the jurisdiction (province or state) and country of issue of the document; and

- the expiry date of the document, if available (if this information appears on the document or card, you must record it).

2.2 Credit file method

You may verify the identity of a person by referring to information that is in their credit file.Footnote 4 To do so, the credit file must:

- contain information that is **valid and current**;Footnote 5
- be from a Canadian credit bureau (credit files from foreign credit bureaus are not acceptable);
- have been in existence for at least three years;
- contain information that is derived from more than one source (i.e. more than one tradeline); and
- match the name, address and date of birth of the person being identified.

A credit file provides a rating on a person's ability to repay loans; however, it is possible to request a credit file to verify a person's identifying information that does not include a credit assessment. You do not need a credit assessment to verify the identity of a person. Equifax Canada and TransUnion Canada are Canadian credit bureaus that provide credit file information for identification purposes.

To use the credit file method, you must conduct the search **at the time** you are verifying the person's identity. A person cannot provide you with a copy of their credit file, nor can a previously obtained credit file be used.

It is acceptable to use an automated system to match the person's information with the information in the person's credit file. You may also refer to a third party vendor to provide you with valid and current information from the person's credit file. A third party vendor is a business that is authorized by a Canadian credit bureau to provide access to Canadian credit information.

If any of the information provided by the person (name, address or date of birth) does not match the information in the credit file, you cannot use that credit file to verify the identity of the person. You will need to use another credit file from a different provider (credit bureau or third party vendor) or use a different method (for example, the government-issued photo identification method or the dual-process method) to verify the person's identity.

On occasion, information found in the credit file may contain a variation on the name or a discrepancy in the address that was provided to you by the person. In these instances, you must determine whether the information in the credit file matches the information provided by the person. For example:

- If there is a slight typo in the address or name, you may determine that the information still matches what the person provided.
- If there is a discrepancy in their date of birth, it is more likely that you will determine that the information does not match.

  - In this case, if this is your determination, you cannot rely on the information in the credit file for identification purposes. You will need to use another credit file from a different provider (credit bureau or third party vendor) or use a different method (for example, the government-issued photo identification method or the dual-process method) to verify the person's identity.
- If there are multiple addresses in the credit file, it is possible that the address the person provided to you is not the primary address in the credit file but it does appear in the credit file as a secondary address. If this is the case, you can still meet your requirements for ensuring that the information matches what the person provided.

Record keeping requirements for the credit file method If you use the credit file method, you must record:Footnote 6

- the person's name;
- the date you consulted or searched the credit file;
- the name of the Canadian credit bureau or third party vendor as the source holding the credit file; and
- the person's credit file number.

Your compliance program's policies and procedures must describe the processes you will follow to verify a person's identity using the credit file method **and** how you will ensure that the information is valid and current. It should also include the steps you will take if the information is not valid and current (for example, search a different credit file, use another method, stop the transaction, etc.).

2.3 Dual-process method

You may verify the identity of a person by using the dual-process method, which consists of doing any **two** of the following:Footnote 7

- referring to information from a reliable source that includes the **person's name and address** and confirming that the name and address are those of the person;
- referring to information from a reliable source that includes the person's **name and date of birth**, and confirming that the name and date of birth are those of the person; or
- referring to information that includes the person's **name and confirms that they have a deposit account, a prepaid payment product account , or a credit card or other loan account with a financial entity**, and confirming that information.

The information you refer to **must** be valid and currentFootnote 8 **and** come from two different reliable sources. This information could be found in **statements, letters, certificates, forms or other information sources** that can be provided through an original version or by another version of the information's original format such as a fax, a photocopy, a scan, or an electronic

image. For example, you can rely on a fax, photocopy, scan or electronic image of a government-issued photo identification document as one of the two pieces of information required to verify a person's identity.

You **cannot** use the same source for the two categories of information you choose to verify a person's identity.Footnote 9 For example, you cannot rely on a bank statement from Bank A that includes the person's name and address and another bank statement from Bank A that includes the person's name and confirms that the person holds a deposit account, as Bank A would be the same source of both categories of information. You can, however, refer to a bank statement from Bank A that contains the person's name and confirms that the person holds a deposit account, and rely on an electronic image of a driver's licence to confirm the person's name and address.

For further precision, the possible combinations for this method include:

Referring to information from one reliable source that includes the person's **name** and **address** and confirming that this matches the information provided by the person, **and** referring to information from a different reliable source that includes the person's **name** and **date of birth** and confirming that this matches the information provided by the person.

OR

Referring to information from one reliable source that includes the person's **name** and **address** and confirming that this matches the information provided by the person, **and** referring to information from a different reliable source that includes the person's **name** and a **financial account**(specifically, a deposit account, a prepaid payment product account, a credit card account or a loan account) and confirming this information.

OR

Referring to information from one reliable source that includes the person's **name** and **date of birth** and confirming that this matches the information provided by the person, **and** referring to information from a different reliable source that includes the person's **name** and a **financial account**(specifically, a deposit account, a prepaid payment product account, a credit card account or a loan account) and confirming this information.

Note: If the information does not match the information provided by the person, you cannot rely on it. For example, it is **not acceptable** to rely on information if the account number or number that is associated with the information is truncated or redacted. On occasion, information from a source may contain a variation on the name of the client or a typo in the client's address. In these instances, you must determine whether the information matches the information provided by the person. If it is a slight typo in the address or a misspelled name, you may determine that the information still matches what the person provided. However, in the case of an incorrect date of birth, it is more likely that you will determine that the information does not match. In this case, you cannot

rely on the information from this source for identification purposes. You must obtain information from a different source under the dual-process method or use a different method (for example, the government-issued photo identification method or the credit file method) to verify the person's identity.

Reliable source of information A reliable source of information is an originator or issuer of information that you trust. To be considered reliable, the source should be well known and considered reputable. For example, a reliable source could be the federal, provincial, territorial or municipal levels of government, Crown corporations, federally regulated financial institutions, or utility providers. Social media is **not** an acceptable source of information to verify a person's identity. Also, the source **cannot** be the person whose identity is being verified, nor you, the RE who is verifying identity.Footnote 10 See Annex 5 for a table of examples of reliable sources of information for the dual-process method.

How to use a credit file under the dual-process method A Canadian credit file can be used as one of the two pieces of information required to verify the identity of a person under the dual-process method. Specifically, it can be used to confirm the person's name and address, name and date of birth, or to confirm the person's name and confirm that the person has a credit card account or a loan account. If you use a credit file as one of the information pieces for the dual-process method, it must have existed for at least six months.Footnote 11

Information from a second source, for example, a property tax assessment, must be used to confirm the second category of information. In this instance, the two reliable sources are the Canadian credit bureau that provided the credit file information and the municipal government that issued the property tax assessment. The information from these two sources must match the information provided by the person.

You can also refer to information from a Canadian credit bureau if it acts as an aggregator that compiles information from different reliable sources (often referred to as tradelines). In this instance, the Canadian credit bureau must provide you with information from **two** independent tradelines where each tradeline confirms one of the two categories of information required to verify the identity of a person under this method. In this instance, **each tradeline is a distinct source; the credit bureau is not the source**.

The tradelines cannot be your own, as the RE verifying the person's identity, and each tradeline must originate from a different reliable source (for example, a federally regulated financial institution, a utility service provider, etc.).

Record keeping requirements for the dual-process method If you use the dual-process method to verify a person's identity, you must record:Footnote 12

- the person's name;
- the date you verified the information;
- the name of the two different reliable sources that were used to verify the identity of the person;
- the type of information referred to (for example, a utility statement, a bank statement, a marriage licence); and
- the number associated with the information (for example, account number or if there is no account number, a number that is associated with the information, which could be a reference number or certificate number, etc.). If you use information aggregated by a Canadian credit bureau and receive information from two distinct sources (tradelines), you must record the account number or number associated to each tradeline, not the aggregator (credit bureau) number.

Your compliance program's policies and procedures must describe the processes you follow when using the dual-process method to verify a person's identity and how you will ensure that the information is valid and current.

2.4 Affiliate or member method

You may verify the identity of a person by confirming that one of the following entities previously verified the person's identity:

- an **affiliate** of yours that is an RE referred to in any of paragraphs 5(a) to (g) of the PCMLTFA;Footnote 13
- a **foreign affiliate** of yours that carries out activities outside of Canada that are similar to the activities of an RE referred to in any of paragraphs 5(a) to (g) of the PCMLTFA;Footnote 14 **or**
- a financial entity that is subject to the PCMLTFA and isa **member** of yourfinancial services cooperative or credit union central.Footnote 15

You must confirm that the name, address, and date of birth in the affiliate or member's records match the information provided by the person whose identity is being verified.Footnote 16

The affiliate or member must have previously verified the person's identity by using the government-issued photo identification method, the credit file method or the dual-process method presented in this Guidance. If the affiliate or member verified the identity of the person prior to June 1, 2021, they must have done so in accordance with the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFR), by using the methods that were in place **at the time**.Footnote 17

If you have any concerns about the methods or information that the affiliate or member used to verify the person's identity, you should re-verify their identity,Footnote 18 as you have the responsibility for ensuring the person's identity has been verified.

Note: Financial services cooperatives or credit union centrals act on behalf of

a membership composed of certain financial entities and can provide financial services to that group.

Record keeping requirements for the affiliate or member method
When you verify the identity of a person by confirming that an **affiliate** or a financial entity that is a **member** of **your** financial services cooperative or credit union central previously verified their identity, you must record:Footnote 19

- the person's name;
- the date on which you verified the identity of the person;
- the name of the affiliate or the member that previously verified the person's identity;
- the method (government-issued photo identification, credit file or dual-process) that the affiliate or the member used to verify the person's identity; and
- the information that the affiliate or the member recorded based on the method used (this includes the name of the person, the date the affiliate or member verified identity, and all the other information required to be kept by them for the method used).

Note: If the affiliate or the member verified the identity of the person in accordance with the methods that were in place prior to June 1, 2021, you must still record the information listed above, but include the method they used in accordance with the PCMLTFR as it read at the time, and the information that was required to be recorded for that method.Footnote 20

Your compliance program's policies and procedures must describe the processes you follow when using the affiliate or member method to verify a person's identity.

2.5 Reliance method

You may verify the identity of a person by relying on measures that were previously taken by:

- **another RE**(person or entity that is referred to in section 5 of the PCMLTFA);Footnote 21 **or**
- an entity that is affiliated with you or with another RE **and** carries out activities outside of Canada that are similar to those of a person or entity referred to in any of paragraphs 5(a) to (g) of the PCMLTFA(an **affiliated foreign entity**).Footnote 22

To rely on measures previously taken by an **affiliated foreign entity**, you must be satisfied, after considering the risk of a money laundering or terrorist activity financing offence in the foreign state in which it carries out its activities, that:Footnote 23

- the **affiliated foreign entity** has policies in place similar to the record keeping, verifying identity, and compliance program requirements under the PCMLTFA, including the requirement to develop and apply policies to assess, in the course of their activities, the risk of a money laundering offence or a terrorist activity financing offence, and the requirement to take enhanced measures where the risk has been identified as high; **and**
- the **affiliated foreign entity's** compliance with those policies is subject to the supervision of a competent authority under the legislation of that foreign state.

To rely on measures previously taken by **another RE** or an **affiliated foreign entity** to verify the identity of a person, you must:Footnote 24

- as soon as feasible, obtain from the **other RE** or **affiliated foreign entity** the information that was confirmed as being that of the person, and be satisfied that:
  - the information is valid and current; and
  - the **other RE** or **affiliated foreign entity** verified the person's identity using the government-issued photo identification method, the credit file method or the dual-process method, or if the **other RE** or **affiliated foreign entity** verified the person's identity prior to June 1, 2021, that they did so in accordance with the PCMLTFR, by using the methods that were in place at the time; **and**
- have a written agreement or arrangement with the **other RE** or **affiliated foreign entity** that upon request requires them to provide you, as soon as feasible, with all of the information that they referred to in order to verify the person's identity.

Record keeping requirements for the reliance method If you rely on **another RE** or an **affiliated foreign entity** to verify the identity of a person, you must keep a record of:Footnote 25

- the person's name;
- the written agreement or arrangement with the **other RE** or **affiliated foreign entity** for the purpose of verifying a person's identity; and
- the information that the **other RE** or **affiliated foreign entity** referred to in order to verify the identity the person.

Your compliance program's policies and procedures must describe the processes you follow when using the reliance method to verify a person's identity and how you will ensure that the information is valid and current.

3. Using an agent or a mandatary to verify the identity of a person on your behalf

You may verify the identity of a person by using an agent or mandatary to carry out the verification on your behalf, in accordance with the government-issued photo identification method, the credit file method, or the dual-process method.Footnote 26

You may rely on the measures that were previously taken by an agent or mandatary to verify the person's identity, if the agent or mandatary was:Footnote 27

- acting in their own capacity at the time, whether or not they were required to use the methods in accordance with the PCMLTFR; or
- acting as an agent or mandatary under a written agreement or arrangement that was entered into with another RE, for the purposes of verifying a person's identity using either the government-issued photo identification method, the credit file method or the dual-process method, or if the measures were taken prior to June 1, 2021, using the methods in accordance with the PCMLTFR that were in place at the time.

To use an agent or mandatary to verify the identity of a person you must:Footnote 28

- have a written agreement or arrangement in place with the agent or mandatary **before** you use them;Footnote 29
- obtain, as soon as feasible, all of the information that the agent or mandatary referred to in order to verify the person's identity, and the information that the agent or mandatory confirmed as being that of the person;Footnote 30 and
- be satisfied that:
  - the information that the agent or mandatary confirmed as being that of the person is valid and current, and
  - the person's identity was verified using the government-issued photo identification method, the credit file method or the dual-process method, or, if the person's identity was verified prior to June 1, 2021, using the methods in accordance with the PCMLTFR in place at the time.Footnote 31

Example 1 — Acceptable

Jane Smith would like to open an account with you. Your agent—with whom you have a written agreement for this purpose—verified Jane Smith's identity in 2019 using the government-issued photo identification method, by referring to her driver's licence, which expired in February 2021. In 2019, Jane Smith's name and appearance matched the name and photograph on the driver's licence, and the document was determined to be authentic, valid and current, therefore, her identity was verified by the agent in accordance with the method. Jane's name and appearance have not changed. When you obtain the information from

the agent, you are satisfied that the information the agent confirmed as being Jane's (her name and photo) is still valid and current and is therefore acceptable. It does not matter that her licence (the identification document used by the agent) has expired, as it is the information that you must be satisfied is valid and current, not the document.

Example 2 — Not acceptable

Jane Smith (maiden name — Jane Rogers) would like to carry out a transaction for which you must verify her identity. Your agent—with whom you have a written agreement for this purpose—verified Jane Rogers' identity in 2019 using the government-issued photo identification method, by referring to her driver's licence, which has not yet expired. In 2019, **Jane Rogers'** name and appearance matched the name and photograph on the driver's licence, and the document was determined to be authentic, valid and current, therefore, her identity was verified by the agent in accordance with the method. However, although the licence has not yet expired, it is not acceptable to rely on the information from the agent now because the agent's information is about Jane Rogers, and this does not match the name of your client who is now Jane Smith, so the information provided by the agent is not valid and current.

Example 3 — Not acceptable

Jane Smith would like to carry out a transaction for which you must verify her identity. Your agent—with whom you have a written agreement for this purpose—verified Jane Smith's identity in 2019 by referring to her driver's licence, which expired in 2018. In 2019, because **Jane Smith's** driver's licence had expired, her identity **was not** verified in accordance with the government-issued photo identification method. As such, it is not acceptable to rely on the information from the agent.

Record keeping requirements when using an agent or a mandatary
When you verify the identity of a person by using an agent or mandatary, you must keep a record of:Footnote 32

- the person's name;
- the written agreement or arrangement with the agent or mandatary for verifying a person's identity; and
- all of the information the agent or mandatary referred to in order to verify the identity of the person, and the information that the agent or mandatary confirmed as being that of the person (this includes, as applicable, information that is required to be kept in the record for the method used).

Note: As an RE it is your responsibility to meet your client identification requirements under the PCMLTFA and associated Regulations, even when you use an agent or mandatary to verify the identity of a person on your behalf, or when you rely on the measures previously taken by an agent or mandatary to verify a person's identity.

For example, if your agent verifies the identity of a person using the government-issued photo identification method but they don't refer to an authentic, valid and current photo identification document issued by a federal, provincial or territorial government, or keep the required records after verifying the person's identity, you are still responsible. Specifically, it is your responsibility to ensure that the agent is verifying client identity and keeping the required records in accordance with the PCMLTFA and associated Regulations.

Your compliance program's policies and procedures must describe the processes you follow when you rely on an agent or mandatary to verify a person's identity and how you will ensure that the information is valid and current.

4. Verifying a person's identity if it has been previously verified

You do **not** need to verify a person's identity for subsequent transactions or activities, as required, **if** you have already verified the identity of the person using:Footnote 33

- one of the methods explained in this guidance; or
- the methods specified in the PCMLTFR prior to June 1, 2021 as it read at the time, and have kept the required record.

You must not have doubts about the information that was previously used to verify the person's identity. If you have doubts, you must verify their identity again using the methods explained in this guidance.Footnote 34

Note: In the context of a business merger or acquisition, you are not required to re-identify the acquired clients if their identities were verified in accordance with the methods in the PCMLTFR at the time the verification took place. As a best practice, you are encouraged to review and update client information (for example, name, address, occupation, etc.), in accordance with your risk assessment process. The acquired clients become the responsibility of the acquiring entity which must ensure compliance with the PCMLTFA and associated Regulations. This includes reviewing any money laundering or terrorist financing risks that may be associated with these clients.

5. How to identify a child

If a child is under 12 years of age, you must verify the identity of one parent, guardian or tutor **and** record the parent, guardian or tutor's information.Footnote 35 You can rely on the information provided by the parent, guardian or tutor in order to record the child's identification details.

If a child is between 12 and 15 years of age, you can verify their identity by using any of the methods. If this is not possible due to a lack of identification information, you may use a variation of the dual-process method that allows you to:

- Refer to one reliable source of information that includes the name and address of the child's parent, guardian, or tutor;Footnote 36 and
- Refer to a second reliable source that includes the child's name and date of birth.

For example, if the child has a passport you may be able to use it to verify their identity under the government-issued photo identification method. If not, you could rely on the parent's driver's licence to verify the parent's name and their common address, and the child's birth certificate to verify the child's name and date of birth.

6. How to verify the identity of a person who does not have any identity verification documentation or information for a retail deposit account Added on February 22, 2023

In the case of opening a retail deposit account, if a bank cannot verify a person's identity in accordance with one of the methods outlined above, they would still be in compliance with their anti-money laudering/anti-terrorist financing obligations if they opened the account in a way that meets the conditions set out in subsections 627.17(1) and (3) of the Bank Act.

Note: The Bank Act applies to banks, authorized foreign banks and federal credit unions, which are defined as banks under the Act.

For reasons beyond a person's control, they may face barriers in meeting requirements where they must provide proper identification documentation or information. This may be the case for vulnerable populations with barriers to obtaining proper identification such as survivors of human trafficking or victims of domestic abuse.

In specific circumstances, where a person does not have the proper identification documentation or information, a bank must:

- follow the measures as defined by the Bank Act and any bulletins published by the Financial Consumer Agency of Canada that further define the measures to be taken
- document in their compliance policies and procedures the types of circumstances where their organization would follow the Bank Act for verification of identification
- ensure that the banking products provided to the individual opening the account are limited to a basic retail deposit account until which time the account holder returns with the proper form of identification as specified in paragraphs 105(1)(a) to (e) of the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations
- verify the person's identity using the appropriate form of identification as specified in paragraphs 105(1)(a) to (e) of the Regulations, within 6 to 12 months, or as described in their risk-based approach and keep appropriate records

- continue to follow their customer due diligence and "know your client" processes, ensure ongoing monitoring activities are conducted as per the bank's risk assessment of the client and monitor transactions to ensure that the financial activity and use of associated products/services aligns with what is known about the person.

Note: The risk-based approach must reflect what is known about the client (i.e., their profile and individual circumstances including the fact that alternate identification was accepted), and that ongoing monitoring should then be commensurate to the risk profile of the client.

When FINTRAC undertakes compliance activities to ensure reporting entities are meeting their obligations, and observes that this process is used, we will:

- verify that you have documented policies and procedures that articulate the steps your organization takes to ensure that they are meeting this requirement
- ensure that the procedures are also followed in practice
- verify that your risk assessment takes into account these circumstances, ensures that these individuals are identified within a reasonable timeframe (i.e., 6 to 12 months) and that you are able to demonstrate that you are fulfilling these requirements.

7. How to verify the identity of an entity

You can use any of the 3 methods described below to verify the identity of an entity:

1. 7.1 Confirmation of existing method
2. 7.2 Reliance method
3. 7.3 Simplified identification method

While an entity can be a corporation, a trust, a partnership, a fund, or an unincorporated association or organization, corporations are subject to different requirements than other entities (as explained below).

7.1 Confirmation of existence method

Corporation To verify the identity of **a corporation**, you may refer to:Footnote 37

- a certificate of incorporation;
- a record that has to be filed annually under provincial securities legislation; **or**
- the most recent version of any other record that confirms the corporation's existence and contains its name and address and the names of its directors, such as a certificate of active corporate status, the corporation's published annual report signed by an audit firm, or a letter or notice of

assessment for the corporation from a municipal, provincial, territorial or federal government.

The record you refer to must be authentic, valid and current.Footnote 38

You may obtain a corporation's name and address and the names of its directors from a publicly accessible database, such as a provincial or federal database like the Corporations Canada database, or a corporation search and registration service through subscription.

When a corporation is a securities dealer, you do not need to confirm the names of its directors when you confirm its existence.Footnote 39

Entity To verify the identity of an **entity other than a corporation,** you may refer to:Footnote 40

- a partnership agreement;
- articles of association; **or**
- the most recent version of any other record that confirms its existence and contains its name and address.

The record you refer to must be authentic, valid and current.Footnote 41

Record keeping requirements when verifying the identity of a corporation or other entity If you refer to a paper record or an electronic version of a record, you must keep the record or a copy of it.

If the electronic version of the record that you refer to is contained in a database that is accessible to the public, you must keep a record that includes the corporation or other entity's registration number, the type of record referred to and the source of the electronic version of the record.Footnote 42

Your compliance program's policies and procedures must describe the processes you follow when using the confirmation of existence method to verify the identity of corporations and other entities, and how you will ensure that the information is authentic, valid and current.

7.2 Reliance method

You may verify the identity of a **corporation** or other **entity** by relying on the measures that were previously taken by:

- another **RE**(a person or entity that is referred to in section 5 of the PCMLTFA);Footnote 43 **or**
- an entity that is affiliated with you **or** with another RE **and** carries out activities outside of Canada that are similar to those of a person or entity referred to in any of paragraphs 5(a) to (g) of the PCMLTFA (an **affiliated foreign entity**).Footnote 44

Measures previously taken by an affiliated foreign entity To rely on measures previously taken by an **affiliated foreign entity**, you must be satisfied, after considering the risk of a money laundering or terrorist activity financing offence in the foreign state in which it carries out its activities, that:Footnote 45

- the **affiliated foreign entity** has policies in place similar to the record keeping, verifying identity, and compliance program requirements under the PCMLTFA, including the requirement to develop and apply policies to assess, in the course of their activities, the risk of a money laundering offence or a terrorist activity financing offence, and the requirement to take enhanced measures where the risk has been identified as high; **and**
- the **affiliated foreign entity's** compliance with those policies is subject to the supervision of a competent authority under the legislation of that foreign state.

Measures previously taken by another reporting entity or an affiliated foreign entity To rely on the measures previously taken by **another RE** or an **affiliated foreign entity** to verify the identity of a corporation or other entity, you must:Footnote 46

- as soon as feasible, obtain from the **other RE** or **affiliated foreign entity** the information that was used to confirm the identity of the corporation or other entity, as the case may be, and be satisfied that:
  - the information is valid and current; and
  - **for a corporation**, its identity was verified by the **other RE** or **affiliated foreign entity** by referring to a record as described in the confirmation of existence method above, **or** if the measures to verify the corporation's identity were performed prior to June 1, 2021, that the **other RE** or **affiliated foreign entity** confirmed the corporation's existence and ascertained its name, address, and the names of its directors in accordance with the methods in the PCMLTFR as they read at that time;Footnote 47 and
  - **for an entity other than a corporation**, its identity was verified by the **other RE** or **affiliated foreign entity** by referring to a record as described in the confirmation of existence method above, **or** if the measures to verify the entity's identity were performed prior to June 1, 2021, the **other RE** or **affiliated foreign entity** confirmed the entity's existence in accordance with the methods in the PCMLTFR as they read at that time;Footnote 48 **and**
- have a written agreement or arrangement in place with the **other RE** or **affiliated foreign entity** that upon request requires them to provide you, as soon as feasible, with all of the information that they referred to in order to verify the identity of the **corporation** or other **entity,** as the case may be.Footnote 49

Your compliance program's policies and procedures must describe the processes you will follow when using the reliance method to verify the identity of corporations and other entities and how you will ensure that the information is valid and current.

7.3 Simplified identification method

If you are an **RE** that isreferred to in any of paragraphs 5(a) to (g) of the PCMLTFA, you may use the simplified identification method to meet your obligation to verify the identity of a **corporation** or other **entity**. Specifically, you are deemed to comply with your requirement to verify the identity of a **corporation** or other **entity** if, based on your risk assessment, you consider there is a low risk of a money laundering offence or terrorist activity financing offence, **and** if:Footnote 50

- the **corporation** or other **entity** whose identity is being verified:
    1. is referred to in any of paragraphs 5(a) to (g) of the PCMLTFA;
    2. is a foreign corporation or entity that carries out activities that are similar to those of an entity referred to in any of paragraph 5(a) to (g) of the PCMLTFA;
    3. administers a pension or investment fund that is regulated under the legislation of a foreign state and that either is created by a foreign government or is subject to the supervision of a competent authority under the legislation of that foreign state;
    4. is one whose shares are traded on a Canadian stock exchange or a stock exchange designated under subsection 262(1) of the Income Tax Act;
    5. is a subsidiary of a **corporation** or an **entity** that is referred to in paragraphs a. to d. in this section, and is one whose financial statements are consolidated with the financial statements of that corporation or entity;
    6. is an institution or agency of, or in the case of a corporation, is owned by, the government of a foreign state; **or**
    7. is a public service body, as defined in subsection 123(1) of the Excise Tax Act; **and**
- you are satisfied that, within the applicable time period for which you had to verify identity, as explained in the sector-specific guidance on When to verify the identity of persons and entities, the corporation or other entity exists **and** that every person who deals with you on behalf of the corporation or other entity is authorized by it to do so.

If you subsequently consider, based on your risk assessment, that the risk of a money laundering offence or terrorist activity financing offence has increased and is no longer low then you **must**, as soon as feasible, verify the identity of the corporation or other entity, as the case may be, by referring to the appropriate records, as explained in **section 7.1, Confirmation of existence method**.

Record keeping requirements for the simplified identification method
If you use the simplified identification method to verify the identity of a corporation or other entity, you must keep a record that sets out:

- the grounds for considering there is a low risk of a money laundering offence or terrorist activity financing offence; and
- the information obtained about the corporation or other entity, as the case may be, and about the persons that assure you that the corporation or other entity exists and that the persons you deal with are authorized to act on behalf of the corporation or the entity.Footnote 52

Your compliance program's policies and procedures must describe the processes you follow when using the simplified identification method to verify the identity of corporations and other entities.

8. Verifying the identity of an entity if it has been previously verified

You do **not** need to verifythe identity of a corporation or other entity for subsequent transactions or activities, as required, if you have already verified their identity by using:

- One of the methods explained in this guidance; or
- in the case of an **entity**, you confirmed the entity's existence in accordance with the PCMLTFR, and you complied with the related record keeping provisions, as they read at the time prior to June 1, 2021; **or**
- in the case of a **corporation**, you confirmed the corporation's existence and ascertained its name and address and the names of its directors in accordance with PCMLTFR, and you complied with the related record keeping provisions, as they read at the time prior to June 1, 2021

You must not have doubts about the information that was previously used to verify the identity of the corporation or other entity. If you have doubts, you must verify identity again using the methods explained in this guidance.Footnote 54

9. Restrictions on the use of personal information

The use of personal information in Canadian commercial activities is protected by the Personal Information Protection and Electronic Documents Act (PIPEDA), or by similar provincial legislation. You have to inform clients about the collection of their personal information. However, you do not have to inform them when you include their personal information in the reports you are required to submit to FINTRAC.

The Office of the Privacy Commissioner of Canada can provide further guidance, and has created a Question and Answer document about PIPEDA and the

Proceeds of Crime (Money Laundering) and Terrorist Financing Act, to help clarify your responsibilities under PIPEDA.# Beneficial ownership requirements

Overview

This guidance came into force on June 1, 2021.

Beneficial ownership requirements under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and associated Regulations apply to all reporting entities (REs).

The concealment of beneficial ownership information is a technique used in money laundering and terrorist activity financing schemes. Identifying beneficial ownership removes the anonymity of the individuals behind the transactions and account activities, which is a key component of Canada's anti-money laundering and anti-terrorist financing regime. By collecting beneficial ownership information and confirming its accuracy, REs are performing an important step to mitigate the risk of money laundering and terrorist activity financing, and ultimately, to protect the integrity of Canada's financial system.

1. Who are beneficial owners?

Beneficial owners are the individuals who directly or indirectly own or control 25% or more of a corporation or an entity other than a corporation. In the case of a trust, they are the trustees, the known beneficiaries and the settlors of the trust. If the trust is a widely held trust or a publicly traded trust, they are the trustees and all persons who own or control, directly or indirectly, 25% or more of the units of the trust.

Beneficial owners cannot be other corporations, trusts or other entities. They must be the individuals who are the owners or controllers of the entity. It is important to consider and review the names found on official documentation in order to confirm the accuracy of the beneficial ownership information. It may be necessary to search through many layers of information in order to confirm who are the beneficial owners, as the names found on official documentation may not always reflect the actual beneficial owners.

2. When must I obtain beneficial ownership information?

You must obtain beneficial ownership information when you verify the identity of an entity in accordance with the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFR).Footnote 2 For more information about when you are required to verify the identity of entities, see your sector's guidance on When to identify persons and entities.

The beneficial ownership information that you must obtain varies depending on whether the entity is a corporation, an entity other than a corporation (such as a partnership), a trust, or a widely held or publicly traded trust. The specific

beneficial ownership information that you must obtain for each type of entity is detailed in section " 5. What beneficial ownership information do I need to obtain and confirm the accuracy of?".

3. When must I confirm the accuracy of beneficial ownership information?

You must take reasonable measures to confirm the accuracy of the beneficial ownership information when you first obtain it **and** in the course of conducting ongoing monitoring of your business relationships.

4. Are there circumstances where I do not have to obtain beneficial ownership information and confirm its accuracy?

You do not have to obtain beneficial ownership information and take reasonable measures to confirm its accuracy in the following situations:

1. For a group plan account held within a dividend or a distribution reinvestment plan. This includes plans that permits purchases of additional shares or units by the member with contributions other than the dividends or distributions paid by the plan sponsor, if the sponsor is an entity:
   - whose shares or units are traded on a Canadian stock exchange; and
   - that operates in a country that is a member of the Financial Action Task Force.
2. If you are a **financial entity**, beneficial ownership requirements do not apply to your activities in respect of the processing of payments by credit card or prepaid payment product for a merchant.Footnote 5
3. If you are a **life insurance company, broker or agent**, and you deal in reinsurance, beneficial ownership requirements do not apply to you for those dealings.Footnote 6

All RE sectors

The beneficial ownership requirements do not apply if you are not required to verify the identity of an entity under the Regulations because of a related exception. This is because your obligation to verify identity for a particular transaction, activity, or client does not apply in that circumstance.

5. What beneficial ownership information do I need to obtain and confirm the accuracy of?

When you verify an entity's identity in accordance with the PCMLTFR, you **must obtain** the following information about beneficial owners:Footnote 7

Corporations

- the names of all directors of the corporation and the names and addresses of all persons who directly or indirectly own or control 25% or more of the shares of the corporation.

Trusts

- the names and addresses of all trustees and all known beneficiaries and settlors of the trust.

Widely held or publicly traded trusts

- the names of all trustees of the trust and the names and addresses of all persons who directly or indirectly own or control 25% or more of the units of the trust.

Entities other than corporations or trusts

- the names and addresses of all persons who directly or indirectly own or control 25% or more of the entity.

In all cases, you must obtain information establishing the ownership, control and structure of the entity.Footnote 8

You **must also take reasonable measures to confirm** the accuracy of the information when you first obtain it and in the course of the ongoing monitoring of your business relationships.Footnote 9

If you verify the identity of a **not-for-profit organization**, you must also determine if the entity is:Footnote 10

- a charity registered with the Canada Revenue Agency under the Income Tax Act; or
- an organization, other than one referred to above, that solicits charitable donations from the public.

6. How do I obtain the required beneficial ownership information?

To obtain beneficial ownership information, which includes information on the ownership, control and structure, you could have the entity provide it, either verbally or in writing, or you could search for publicly available information.

For example:

- the entity can provide you with official documentation;
- the entity can tell you the beneficial ownership information and you can write it down for record keeping purposes; or
- the entity can fill out a document to provide you with the information.

7. How do I confirm the accuracy of beneficial ownership information?

You must take reasonable measures to confirm the accuracy of the beneficial ownership information that you obtain.Footnote 11 These reasonable measures cannot be the same as the measures you used to obtain the information.

Your reasonable measures could include referring to official documentation or records. For example, for a corporation or other entity, you could refer to records such as, but not limited to, the:

- minute book;
- securities register;
- shareholders register;
- articles of incorporation;
- annual returns;
- certificate of corporate status;
- shareholder agreements;
- partnership agreements; or
- board of directors' meeting records of decisions.

It is also acceptable to have a client sign a document to confirm the accuracy of the beneficial ownership information you obtained, which includes information on ownership, control and structure. In this case, it is possible for one document to be used to satisfy the two steps—namely to obtain the information and to confirm its accuracy by means of the signature.

In the case of a trust, you could confirm the accuracy of the information by reviewing the trust deed, which should provide you with the information needed.

Other reasonable measures can include:

- asking the client to provide supporting official documentation;
- conducting an open-source search; or
- consulting commercially available information.

As a best practice, you should also confirm whether a not-for-profit organization is a charity registered with the Canada Revenue Agency by consulting the charities listing on the Canada Revenue Agency website.

The reasonable measures that you take to confirm the accuracy of beneficial ownership information, which includes ownership, control, and structure information, must align with your risk assessment of the entity's risk for money laundering or terrorist activity financing offences. The reasonable measures you take with entities assessed to pose a high risk must go further to help you understand and confirm the beneficial ownership, as well as establish the overall ownership, control, and structure of that entity.

The reasonable measures that you take with entities that have a complex business structures must go further to ensure that you are able to understand and

confirm the accuracy of beneficial ownership, which includes establishing the ownership, control and structure of that entity. This does not mean, however, that you need to consider or treat a complex entity as posing a high risk. You need to choose reasonable measures that are appropriate to the situation.

8. What if I cannot obtain beneficial ownership information or confirm its accuracy?

If you are unable to obtain the beneficial ownership information, to keep it up to date in the course of the ongoing monitoring of business relationships, or to confirm its accuracy, when it is first obtained, or during the course of ongoing monitoring then you must:Footnote 12

- take reasonable measures to verify the identity of the entity's chief executive officer or of the person who performs that function; and
- apply the special measures for high-risk clients, including enhanced ongoing monitoring.

For more information on enhanced ongoing monitoring, see FINTRAC's Ongoing monitoring requirements guidance.

9. How do I verify the identity of an entity's chief executive officer or of the person who performs that function?

The PCMLTFR does not require that you verify the identity of the chief executive officer or of the person who performs that function in accordance with the prescribed methods. However, you could use one of the methods outlined in the Methods to verify the identity of persons and entities guidance to meet this obligation.

Additionally, there is no record keeping obligation if you have identified the chief executive officer or a person who performs that function using the prescribed methods to verify identity. However, during a FINTRAC examination, you could be asked to demonstrate the reasonable measures that you took to identify the chief executive officer or person who performs that function.

10. What if there are no beneficial owners?

You may obtain information confirming that there is no individual who directly or indirectly owns or controls 25% or more of a corporation, a widely held or publicly traded trust, or an entity other than a corporation or trust. This is not the same thing as being **unable to obtain** the beneficial ownership information.

If **you determine that there is no individual** who directly or indirectly owns or controls 25% or more of a corporation, a widely held or publicly traded trust, or an entity other than a corporation or trust, you must keep a record of the measures you took and the information you obtained in order to reach

that conclusion.Footnote 13 However, you are still required to obtain and take reasonable measures to confirm information about the ownership, control and structure of the entity.

11. What beneficial ownership records do I need to keep?

You must keep a record of the beneficial ownership information you obtain and of the measures you take to confirm the accuracy of the information.

The measures that you take to confirm beneficial ownership information can be part of your overall policies and procedures, so a separate record may not be needed. You only need to keep an individual record of the specific measures you take to confirm the accuracy of beneficial ownership information in situations where the measures differ from those that are documented in your policies and procedures.

For a **corporation**, you must record:

- the names of all directors of the corporation;
- the names and addresses of all persons who directly or indirectly own or control 25% or more of the shares of the corporation; and
- information establishing the ownership, control and structure of the corporation.

For a **trust**, you must record:

- the names and addresses of all trustees, known beneficiaries and known settlors of the trust; and
- information establishing the ownership, control and structure of the trust.

For a **widely held or publicly traded trust**, you must record:

- the names of all trustees of the trust;
- the names and addresses of all persons who directly or indirectly own or control 25% or more of the units of the trust; and
- information establishing the ownership, control and structure of the trust.

For an **entity other than a corporation or trust**, you must record:

- the names and addresses of all persons who directly or indirectly own or control 25% or more of the entity; and
- information establishing the ownership, control and structure of the entity.

If you verify the identity of a **not-for-profit organization**, you must also keep a record that indicates whether the entity is:

- a charity registered with the Canada Revenue Agency under the Income Tax Act; or
- an organization, other than a registered charity, that solicits charitable donations from the public.

In situations where no individual directly or indirectly owns or controls 25% or more of a corporation, a widely held or publicly traded trust, or an entity other than a corporation or trust, you must keep a record of the measures you took to confirm the accuracy of the information, as well as the information you obtained in order to reach that conclusion. The date you took the measures should also be included as a best practice.

Retention: You must keep these records for at least five years from the day the last business transaction is conducted.# Ongoing monitoring requirements

Overview

1. What is ongoing monitoring?

Ongoing monitoring is a process that you must develop and use to review all the information you have obtained about the clients with whom you have a business relationship, in order to:

- detect any suspicious transactions that you are required to report to FINTRAC;
- keep client identification information, beneficial ownership information, and the purpose and intended nature of the business relationship record up to date;
- reassess the level of risk associated with your client's transactions and activities; and
- determine whether transactions or activities are consistent with the client information you obtained and your risk assessment of the client.

For more information about when you enter into a business relationship with a client see FINTRAC's Business relationship requirements guidance.

Your process for conducting ongoing monitoring could include the monitoring of an individual client or of groups of clients. References to the ongoing monitoring of a client in this guidance refers to both an individual client and groups of clients, depending on your processes.

2. When must I conduct ongoing monitoring?

When you enter into a business relationship with a client you must **periodically conduct** ongoing monitoring of that business relationship, based on your risk assessment.Footnote 2

The frequency at which you conduct ongoing monitoring will depend on the risk level assigned to clients in your risk assessment. For example, clients identified as posing a low risk may require less frequent ongoing monitoring whereas those in your high-risk category will require that you take enhanced measures. For more information on risk assessment requirements and enhanced measures, see FINTRAC's Compliance program requirements guidance.

FINTRAC expects that your policies and procedures will include the frequency at which you will conduct ongoing monitoring of your clients, based on your risk assessment for a client or group of clients.

3. When must I conduct enhanced ongoing monitoring?

You must take enhanced measures and conduct enhanced ongoing monitoring of a client that you have identified as posing a high risk in your risk assessment. This means that you must take extra measures in addition to what is required, as appropriate for the level of client risk.Footnote 3

You could consider the following methods to conduct enhanced ongoing monitoring of your high-risk clients:

- reviewing transactions based on an approved schedule that involves management sign-off;
- developing reports and reviewing these reports of high-risk transactions more frequently;
- flagging certain activities or those that deviate from your expectations and raise concerns, as necessary;
- setting business limits or parameters on accounts or transactions that would trigger early warning signals and require a mandatory review; or
- reviewing transactions more frequently against suspicious transaction indicators relevant to business relationships.

4. What are the exceptions to ongoing monitoring?

You do not have to conduct ongoing monitoring in the following situations:

1. **Financial entities**:You do not have toconduct ongoing monitoring for a group plan account held within a dividend or a distribution reinvestment plan (including a plan that allows members to purchase additional shares or units with contributions other than the dividends or distributions paid by the sponsor of the plan), if the sponsor of the plan:Footnote 4
    - is an entity whose shares or units are traded on a Canadian stock exchange; **and**
    - operates in a country that is a member of the Financial Action Task Force.
2. **Insurance companies, brokers or agents**:You do not have to conduct ongoing monitoring when you are dealing in reinsurance.Footnote 5

5. What records do I need to keep for ongoing monitoring?

You must keep records of the measures you take **and** of the information obtained from the ongoing monitoring of your clients with whom you have a business relationship.Footnote 6 This includes:

- your processes in place to perform ongoing monitoring;

- your processes in place to perform the enhanced ongoing monitoring of high-risk clients;
- your processes for recording the information obtained as a result of your ongoing monitoring;
- your processes for recording the information obtained as a result of your enhanced ongoing monitoring of high-risk clients; and
- the information obtained as a result of your ongoing monitoring and enhanced ongoing monitoring of high-risk clients.

You must outline the measures you use to conduct the ongoing monitoring of your business relationships in your policies and procedures, which can form part of your ongoing monitoring records. However, the information you obtain as a result of your ongoing monitoring is likely to be specific to a particular business relationship and not captured in your policies and procedures, so it should be documented separately. You can document and update the information you obtain through your ongoing monitoring activities across several records. For example, updates to the client identification, beneficial ownership or business relationship information you have, could be recorded in any file you maintain on a client.

Retention: You must keep a record of the ongoing monitoring measures taken and the information obtained from that ongoing monitoring for at least five years from the date the record was created.Footnote 7

6. When does the requirement for ongoing monitoring end?

You are no longer required to conduct ongoing monitoring when your business relationship with a client ends. For more information about when a business relationship ends, see FINTRAC's Business relationship requirements guidance.

7. When does the requirement for enhanced ongoing monitoring end?

You are no longer required to conduct enhanced ongoing monitoring when your business relationship ends **or** when, based on your risk assessment, you no longer consider a client to pose a high risk. When you no longer consider a client high-risk, you are still required to conduct ongoing monitoring of the client at the frequency determined by the client's new risk rating. For more information about when a business relationship ends, see FINTRAC's Business relationship requirements guidance.# Third party determination requirements : FINTRAC's compliance guidance

This guidance explains the third party determination requirements under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (the Act) and associated Regulations.

2. Who is a third party and how to make a determination

A third party is the person or entity that instructs another person or entity to conduct a transaction or activity on their behalf. As such, the third party is the instructing party to the transaction or activity, and is also understood to be the party that the transaction occurs on behalf of (the "on behalf of" party).

Note: The Financial Action Task Force, the Egmont Group and other anti-money laundering and anti-terrorist financing authoritative bodies have observed that third parties have been used in several money laundering and terrorist financing cases. It is not uncommon for criminals to use third parties as a method to evade detection by distancing themselves from the proceeds of crime.

You must take reasonable measures to determine whether a third party is involved when you carry out certain transactions or activities, as explained in this guidance.

Reasonable measures for third party determination could include asking the client if they are acting at the instruction of another person or entity, or asking whether another person or entity will be instructing on the account. The steps you take as reasonable measures to make a third party determination must be documented in your compliance program's policies and procedures.

3. When to make a determination

You must take reasonable measures to make a third party determination when you are required to:

- report a large cash transaction or keep a large cash transaction record
- report a large virtual currency transaction or keep a large virtual currency transaction record
- keep a signature card or an account operating agreement
- keep an information record, or
- submit a Casino Disbursement Report

You must also provide information in an electronic funds transfer report (**casinos, money services businesses, foreign money services businesses, and financial entities only**) for any person or entity on whose behalf an electronic funds transfer is requested or received.

Large Cash Transaction Report or large cash transaction record

When you receive cash in an amount of $10,000 or more, and are required to submit a Large Cash Transaction Report to FINTRAC **or** to keep a large cash transaction record, you must take reasonable measures to determine whether **the** person **from whom you receive the cash** is acting on behalf of a third party.

This is the case even if you receive cash from an armoured car.

Note: This requirement applies to the 24-hour rule.

Large Virtual Currency Transaction Report or large virtual currency transaction record

When you receive an amount of virtual currency equivalent to $10,000 or more, and are required to submit a Large Virtual Currency Transaction Report to FINTRAC **or** to keep a large virtual currency transaction record, you must take reasonable measures to determine whether **the person from whom you receive the virtual currency** is acting on behalf of a third party.

Note: This requirement applies to the 24-hour rule.

Signature card or account operating agreement

As a **financial entity**, a **securities dealer** or a **casino**, you must take reasonable measures to determine whether an account will be used by or on behalf of a third party, **when you open an account** and are required to keep a signature card or an account operating agreement.

When you open a **credit card account** or a prepaid payment product account, you do not need to make a third party determination because you are not required to keep a signature card or an account operating agreement for these account types.

Information record

If you are required to keep an information record for certain transactions or activities, you must take reasonable measures to determine whether the person or entity for which the information record is kept on, is acting on behalf of a third party. This must be done at the time you create the information record.

This requirement applies to the following sectors:

- **money services business**
- **foreign money services business**
- **an agent of the Crown**
- **life insurance company broker or agent**
- **mortgage administrator, broker or lender**
- **real estate developer, broker or sales representative**,

Casino Disbursement Report

As a **casino,** when you are required to report a disbursement of $10,000 or more, you must take reasonable measures, at the time of the disbursement, to determine whether:

- the requester of the casino disbursement is acting on behalf of a third party

Note: This requirement applies to the 24-hour rule.

4. What measures to take

If you determine that there is a third party involved, you must take reasonable measures to obtain the following information about the third party:

- If the third party is a **person**—their name, address, telephone number (not required if the third party determination is made for a large cash transaction or large virtual currency transaction), date of birth and occupation, or in the case of a sole proprietor, the nature of their principal business
- If the third party is a **corporation or an other entity**—its name, address, telephone number (not required if the third party determination is made for a large cash transaction or large virtual currency transaction), the nature of its principal business, its registration or incorporation number and the jurisdiction (province or state) and country of issue of that number, and
- the **relationship** between the third party and the following person or entity, as applicable:
  - the person who conducts the large cash transaction
  - the person who conducts the large virtual currency transaction
  - the account holder(s)
  - the person or entity that the information record is kept on, or
  - the person or entity that requests the casino disbursement.

The relationship between the person or entity and the third party can be for example, an accountant, broker, customer, employee, friend or relative.

- A record must be kept of the information obtained.
- If you receive cash or virtual currency from an armoured car on behalf of another party (such as your client), you must obtain and keep a record of the information detailed above at the time the cash or virtual currency is received.

Retention: At least 5 years from the date the third party determination record was created

5. What if I am not able to make a determination, but I suspect that a third party is involved

If you are not able to make a third party determination, but have reasonable grounds to suspect that a third party is involved, you must keep a record that:

- describes the reason(s) why you suspect that the person or entity is acting on behalf of a third party, and

- as applicable, your record must also indicate:
  - When you receive cash in an amount of $10,000 or more, and are required to submit a Large Cash Transaction Report to FINTRAC **or** to keep a large cash transaction record—whether according to the person who gave you the cash, they are acting on their own behalf only
  - When you receive an amount of virtual currency equivalent to $10,000 or more, and are required to submit a Large Virtual Currency Transaction Report to FINTRAC **or** to keep a large virtual currency transaction record—whether according to the person from whom you received the virtual currency, they are acting on their own behalf only
  - When you open an account and are required to keep a signature card or an account operating agreement— whether according to a person who is authorized to act in respect of the account, the account will only be used by or on behalf of an account holder
  - When you create an information record—whether, according to the person or entity for which the information record is kept, they are acting on their own behalf only, and
  - When you are required to report a casino disbursement of $10,000 or more— whether, according to the person or entity that makes the request for the disbursement, they are acting on their own behalf only.

Retention: At least 5 years from the date the record was created.

6. What are the exceptions to making a third party determination

As a financial entity, you do **not** need to make a third party determination when you open an account and are required to keep a signature card or an account operating agreement, if the account is for the processing of payments by credit card or prepaid payment product for a merchant.

If you are a financial entity, securities dealer or casino, you do **not** need to make a third party determination when you open an account and are required to keep a signature card or an account operating agreement, if every account holder is a financial entity or a securities dealer that is engaged in the business of dealing in securities in Canada.

If you are a life insurance company, broker or agent, you do **not** need to make a third party determination when you keep an information record on a beneficiary in connection with the sale of a life insurance policy under which you are to remit an amount of $10,000 or more to the beneficiary over the duration of the policy, regardless of the means of payment.

7. What are the exceptions to keeping a record of a third party determination

If you are a **financial entity**, a **securities dealer** or a **casino**, you do not have to take reasonable measures to obtain information and keep a record of that information for a third party determination if an account is opened by a legal counsel, an accountant or a real estate broker or sales representative, and you have reasonable grounds to believe that the account is to be used only for clients of the legal counsel, accountant or real estate broker or sales representative, as the case may be.

If you are a **securities dealer,** you do not have to take reasonable measures to obtain information and keep a record of that information for a third party determination when an account operating agreement is kept for the account of a person or entity that is engaged in the business of dealing in securities only outside of Canada, and when:

- the account is in a country that is a member of the Financial Action Task Force
- the account is in a country that is not a member of the Financial Action Task Force but has implemented the recommendations of the Financial Action Task Force relating to client identification and, at the time that the account is opened, the securities dealer has obtained written assurance from the account holder that the country has implemented those recommendations, or
- the account is in a country that is not a member of the Financial Action Task Force and has not implemented the recommendations of the Financial Action Task Force relating to client identification but, at the time that the account is opened, the securities dealer has verified the identity of all third parties in accordance with the methods to verify the identity of persons and entities under the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations.# Business relationship requirements : FINTRAC's compliance guidance

From: Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)

This guidance explains when reporting entities enter into a business relationship with a client and related obligations under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (the Act) and associated Regulations.

1. Who must comply

This guidance applies to all reporting entities, however, some requirements and examples may only apply to certain reporting entities.

If you are a life insurance company, or an entity that is a broker or agent, that offers loans or prepaid payment products to the public, or maintains accounts

related to these products, other than the excluded types in the Regulations, then you are considered a financial entity **for those activities** and you can find your business relationship obligations as a financial entity in the guidance below.

2. What is a business relationship

A business relationship is a relationship established between a reporting entity and a client to conduct financial transactions or provide services related to financial transactions.

3. When do I enter into a business relationship with a client

When you enter into a business relationship varies by reporting entity sector, and depends on the activities and transactions that a client conducts with you. For more information on when you enter into a business relationship with a client, see your sector-specific obligations below.

In this section

- Financial entities, securities dealers and casinos
- Accountants, agents of the Crown, British Columbia notaries, dealers in precious metals and precious stones, and life insurance companies, brokers and agents
- Real estate developers, brokers, or sales representatives, and mortgage administrators, mortgage brokers or mortgage lenders
- Money services businesses and foreign money services businesses

Financial entities, securities dealers and casinos

You enter into a business relationship with a client when 1 of the following occurs:

- **you open an account for a client**(except in certain circumstances, consult: Circumstances when a business relationship is not created), or
- when a client does not hold an account with you, the **second time, within a 5-year period,** that the client engages in a financial transaction **for which you are required to verify their identity**

Accountants, agents of the Crown, British Columbia notaries, dealers in precious metals and precious stones, and life insurance companies, brokers and agents

You enter into a business relationship with a client the second time that you are required to verify their identity **within a 5-year period**.

Real estate developers, brokers, or sales representatives, and mortgage administrators, mortgage brokers or mortgage lenders

You enter into a business relationship with a client the first time that you are required to verify their identity.

Money services businesses and foreign money services businesses

You enter into a business relationship with a client:

- the second time you are required to verify their identity within a **5-year period, or**
- when you enter into a service agreement with an entity (the entity must be in Canada if you are a Foreign Money Services Business)

4. Circumstances where a business relationship is not created

Financial entities, securities dealers, and casinos

You do **not** enter into a business relationship when opening an account, for the following circumstances, when you:

- open a business account, if you have already verified the identity of at least 3 persons authorized to give instructions for the account
- open a second account for a person who already has an account with you
- open an account at the request of an entity, for a life insurance company affiliated with the entity to deposit a death benefit under a life insurance policy or annuity, if:
  - the account is opened in the name of a beneficiary that is a person
  - only that death benefit may be deposited into the account, and
  - the policy or annuity contract under which the claim for the death benefit is made has been in existence for a period of at least 2 years before the day on which the claim is made
- open an account for the sale of mutual funds if there are reasonable grounds to believe that the client's identity has been verified by a securities dealer in respect of:
  - the sale of the mutual funds for which the account was opened, or
  - a transaction that is part of a series of transactions that includes that sale
- sell an exempt policy as defined in subsection 306(1) of the Income Tax Regulations
- sell a group life insurance policy that does not provide for a cash surrender value or a savings component

- sell an immediate or deferred annuity that is paid for entirely with funds that are directly transferred from a registered pension plan or from a pension plan that is required to be registered under the Pension Benefits Standards Act, 1985, or similar provincial legislation
- sell a registered annuity policy or a registered retirement income fund
- sell an immediate or deferred annuity that is paid for entirely with the proceeds of a group life insurance policy
- conduct atransaction that is part of a reverse mortgage or structured settlement
- open an account for the deposit and sale of shares from a corporate demutualization or the privatization of a Crown corporation
- open an account in the name of an affiliate of a financial entity, if the affiliate carries out activities that are similar to those of persons and entities referred to in paragraphs 5(a) to (g) of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act
- open a registered plan account, including a locked-in retirement plan account, a registered retirement savings plan account and a group registered retirement savings plan account
- open an account that is established in accordance with the escrow requirements of a Canadian securities regulator or Canadian stock exchange or provincial legislation
- open an account, if the account holder or settlor is a pension fund that is regulated under federal or provincial legislation
- open an account in the name of, or in respect of which instructions are authorized to be given by, a financial entity, a securities dealer, a life insurance company or an investment fund that is regulated under provincial securities legislation
- open an account solely in the course of providing accounting services to a securities dealer, and
- open an account, if you are a **financial entity** or **securities dealer** that is not required to verify the identity of, or to keep a signature card for a person who is a member of a group plan account if:
  - the member's contributions are made by the sponsor of the plan or by means of payroll deductions, and
  - the identity of the plan sponsor has been verified

All reporting entity sectors

You do not enter into a business relationship that would otherwise have been formed after the first or second time you are required to verify identity (as

applicable to your reporting entity sector), if you are not required to verify the identity of a client under the Regulations because of a related exception. This is because your obligation to verify identity for a particular transaction, activity, or client does not apply in that circumstance. For example, if your requirement to verify identity does not apply because your client is a public body, a very large corporation, or a subsidiary of either of those, whose financial statements are consolidated, then a business relationship would not be formed.

However, a business relationship would be formed in instances where you have the obligation to verify identity, but the Regulations allow you to not do so for a particular reason. This is because the underlying obligation to verify a client's identity still exists, even if you relied upon the applicable reasoning for not verifying identity. This could occur as the result of a suspicious transaction or attempted transaction, or as the result of not having to re-verify the identity of a client.

- **Suspicious transaction reporting:**

When you are required to report a Suspicious Transaction Report to FINTRAC, you are required to take reasonable measures to verify the identity of the person or entity that conducts or attempts to conduct the transaction. Despite whether your reasonable measures are unsuccessful, or if you believe taking reasonable measures would inform the person or entity that you are filing a Suspicious Transaction Report, this transaction must factor into your business relationship requirements, as either the first or second time you are required to verify the identity of a client.

- **Re-verifying identity:**

Your business relationship requirements must still factor in a transaction or activity for which you have the requirement to verify identity but choose not to because the Regulations allow it. The Regulations allow you to choose not to re-verify the identity of a client if:

- you previously did so using the methods specified in the Regulations in place at the time
- you have kept the associated records, and
- you have no doubts about the information used

5. When to determine if I have entered into a business relationship with a client

You should determine that you have entered into a business relationship as soon as possible after opening an account **or** after verifying your client's identity for either the first or second transaction or activity (as applicable to your reporting entity sector) where you had the obligation to do so. As a best practice, you should make a business relationship determination within 30 calendar days of opening the account **or** of the first or second transaction or activity (as applicable).

6. Business relationship records to keep

Once you enter into a business relationship with a client, you must keep a record of the purpose and intended nature of the business relationship. For sector-specific examples of the purpose and intended nature of a business relationship, see Annex A.

As a best practice, to help you meet your know your client requirements and conduct ongoing monitoring of your business relationships, this record should also:

- describe your business dealings with the client, and
- include information that would help you anticipate the types of transactions and activities that the client may conduct. You could then use this information to identify unusual or suspicious transactions while conducting your ongoing monitoring.

If you already have a record of this information that is readily available in other records that you are required to keep, you are not required to keep an additional record. For example, for clients who already hold accounts, you may use the information found in the intended use of the account record, client credit file, credit card account record or a service agreement to satisfy this obligation.

Retention: You must keep these records for 5 years from the day they were created.

7. When a business relationship ends

Account-based business relationships

A business relationship ends 5 years after the day on which a client closes their last account with you.

Non-account-based business relationships

A business relationship ends when a period of at least 5 years has passed since the day of the last transaction that required you to verify the identity of the client.# Guide on harm done assessment for compliance program violations

1. Introduction

This page presents how we assess the harm done and calculate the base penalty amount applied to compliance program violations.

1.1 Purpose of this guide

This guide presents how FINTRAC approaches the harm done criterion and the base penalty amount for violations under the *Proceeds of Crime (Money*

Laundering) and Terrorist Financing Act (the Act) and its regulations. According to section 73.11 of the Act, FINTRAC must consider the harm done by a violation, that the purpose of an administrative monetary penalty (AMP) is to encourage compliance rather than to punish, and all other criteria prescribed in the regulations, including a reporting entity's (RE) history of compliance, when determining the amount of a penalty. Considerations for the non-punitive nature of an AMP and an RE's compliance history are assessed in another step in the penalty calculation and are outlined separately in FINTRAC's AMP policy.

1.2 Definition of harm

FINTRAC defines "harm" as the degree to which a violation interferes with achieving the objectives of the ActFootnote 1 or with FINTRAC's ability to carry out its mandateFootnote 2. Therefore, the consequences of non-compliance, when an AMP is imposed, are linked to its effects on Canada's efforts to combat money laundering and terrorist activity financing (ML/TF).

Compliance enforcement activities are undertaken to prevent and correct the harm that comes from non-compliance with the Act and regulations. REs' adherence to requirements such as record keeping and verifying client identity assists in the deterrence of ML/TF and supports police investigations and criminal prosecutions. The requirements related to reporting ensure that FINTRAC is supplied with the high-quality, timely financial transaction reports it needs to produce the financial intelligence that helps with the investigation and prosecution of ML/TF offences.

1.3 Considering harm in AMP calculations

When determining a penalty, FINTRAC considers the harm caused, that is, the degree to which the non-compliance interferes with the objectives of the Act and/or with FINTRAC's mandate. Non-compliance and harm are measured using the standards described in this guide, which outline the benchmark amounts for the corresponding levels of harm for a specific violation. FINTRAC considers the specific circumstances of each case, including the extent of the non-compliance and mitigating factors, which may further reduce the actual amounts applied.

2. Violations related to compliance program requirements

The fulfillment of the objectives of the Act and FINTRAC's ability to carry out its mandate depend upon REs successfully implementing a compliance program that allows them to identify clients, monitor business relationships, keep records and report certain financial transactions. The compliance program itself requires the appointment of a compliance officer, the development of policies and procedures, the assessment of ML/TF risks, the maintenance of a training program, and a review of the program's effectiveness every two years. These requirements not only ensure that REs have the structure in place to comply with

the Act and its regulations, but they also establish a framework that helps facilitate the detection, prevention and deterrence of ML/TF offences in the normal course of business, which serves the objectives of the Act under paragraph 3(a).

Failing to establish and implement a compliance program can signify a serious deficit in anti-money laundering/anti-terrorist activity financing (AML/ATF) measures, leaving REs vulnerable to ML/TF offences, and ultimately impeding achievement of the Act's objectives under paragraph 3(a), or impacting FINTRAC's ability to carry out its mandate under section 40 of the Act. A compliance program requirement violation can signify gaps and weaknesses that result in not meeting other requirements such as reporting, record keeping or verifying client identity.

Therefore, FINTRAC assesses the potential harm that a compliance program violation may cause.

For example:

In situations where the absence of policies and procedures to report the receipt of $10,000 or more in cash also results in the failure to submit Large Cash Transactions Reports (LCTRs), FINTRAC may assess two distinct violations. The total penalty would be comprised of two amounts: the amount levied for the incomplete policies and procedures and the amount levied for the failure to submit LCTRs to FINTRAC. The penalty amount for incomplete policies and procedures represent the potential harm, while the actual failure to submit the LCTRs represents the concrete harm.

For guidance on how to calculate the penalty amount for other compliance requirements such as reporting, verifying client identity and record keeping, please refer to the Penalties for non-compliance page which lists all the harm done guides by violation.

2.1 Harm consideration framework for violations related to the compliance program

FINTRAC assesses the potential harm caused by a violation and takes into account the relative importance of the requirement to achieving the objectives of the Act or FINTRAC's mandate when it considers the harm done by a compliance program violation. FINTRAC also considers the extent of the non-compliance and mitigating factors.

When assessing the extent of the non-compliance of compliance program violations, FINTRAC considers the degree to which the documentation and application of a requirement meet the Act and its regulations. More importance (weight) is given to the application of a requirement because it is the action of putting something into practice that is most effective to achieve the objectives of the Act and FINTRAC's mandate. For example, when compliance policies and procedures, documented in a comprehensive manner, are not put into practice,

there is a big risk of non-compliance, which prevents the objectives of the Act and FINTRAC's mandate from being achieved.

2.1.1 Types of non-compliance for violations related to the compliance program There are two types of compliance program violations: complete or widespread non-compliance and partial non-compliance.

"Complete" or "widespread" non-compliance is when a requirement has not been met because an RE has not put in place measures to meet the requirement to any degree, or what is in place is too rudimentary. This poses the highest harm to the achievement of the objectives of the Act and FINTRAC's mandate. For example, an RE is in complete violation of the requirement under paragraph 71(1)(b) the Proceeds of Crime Money Laundering and Terrorist Financing Regulations (PCMLTFR) if there are no policies and procedures whatsoever documented or put into practice. This poses the highest harm because there would be no measures in place to comply with any of the requirements under the Act and its regulations.

"Partial" non-compliance is when only parts, or elements, of a requirement have not been met. For example, an RE that has incomplete policies and procedures when it comes to the detection and reporting of suspicious transactions would be in partial violation of the requirement under PCMLTFR 71(1)(b). This poses less harm than the previous example and poses varying levels of harm, depending on the issue.

Penalty amounts for complete or widespread violations and partial violations are calculated based on their associated levels of harm, as described below.

2.2 Levels of harm and penalty amounts for violations related to the compliance program

Compliance program violations are classified as a "serious" under the Proceeds of Crime (Money Laundering) and Terrorist Financing Administrative Monetary Penalties Regulations(AMP Regulations) with penalties ranging from $1—$100,000.

For these violations, FINTRAC has identified four levels of harm. Each level of harm incurs a penalty of either $100,000, $75,000, $50,000 or $25,000.

The table below lists the four levels of harm in descending order, the types of non-compliance and the descriptions of harm along with their corresponding penalty.

Level of harm	Type of non-compliance	Description of harm	Penalty (not considering mitigating factors)
Level 1	The requirement is not met, to any degree, or what is in place is not functional, causing widespread non-compliance. This is complete or widespread non-compliance.	Prevents the achievement of the objectives of the Act and of FINTRAC's mandate because a core AML/ATF measure is absent or non-functional.	$100,000
Level 2	An element that is priority for achieving the objectives of the Act or FINTRAC's mandate is not met. This is partial non-compliance with important weaknesses.	Prevents the achievement of results that are priority for meeting the objectives of the Act and FINTRAC's mandate.	$75,000
Level 3	An element that forms the basis for achieving the objectives of the Act or FINTRAC's mandate is not met.This is partial non-compliance with moderate weaknesses.	Prevents the achievement of results that form the basis for meeting the objectives of the Act and FINTRAC's mandate.	$50,000

Level of harm	Type of non-compliance	Description of harm	Penalty (not considering mitigating factors)
Level 4	An element that enables the efficient achievement of the objectives of the Act or FINTRAC's mandate is not met. This is partial non-compliance with lesser weaknesses.	Diminishes the efficient achievement of the objectives of the Act and FINTRAC's mandate.	$25,000

Table 1—Levels of harm and penalties for violations related to compliance program

The highest level of harm (Level 1) applies to situations of complete or widespread non-compliance because they have the greatest potential impact on the Act's objectives or FINTRAC's mandate. As such, they incur the prescribed maximum penalty which is $100,000.

Levels of harm 2, 3 and 4 apply to situations of partial non-compliance and incur penalty amounts decreasing in intervals from $75,000 to $50,000 and to $25,000 respectively.

FINTRAC will consider relevant mitigating factors that could reduce the penalty down to the prescribed minimum penalty amount of $1, regardless of the violation's level of harm.

The remainder of this guide describes how FINTRAC applies the levels of harm to the compliance program violations.

3. Violation related to the appointment of a compliance officer

This section outlines FINTRAC's approach for failing to appoint a compliance officer, including the harm assessment and penalty calculation.

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
9.6(1)	71(1)(a)	Failure of a person or entity to appoint a person to be responsible for the implementation of a compliance program	Serious$1-$100,000

Table 2— Violation related to the appointment of a compliance officer

3.1 Harm done in the case of a violation related to the appointment of a compliance officer

The purpose of appointing a person responsible for the implementation of a compliance program is to ensure that an RE has the necessary oversight to effectively comply with the requirements of the Act. The person in this role, typically referred to as the compliance officer, is responsible for putting into practice the compliance policies and procedures, ML/TF risk assessment, ongoing compliance training program and the prescribed review of the compliance program.

An effective compliance program begins with the appointment of a compliance officer; but simply appointing a person to this position is not sufficient to meet the objectives of the Act. In order for an RE to meet the requirement, it must ensure that the compliance officer has adequate knowledge of the Act and its regulations, possesses the authority and has access to adequate resources to implement the compliance program.

Failing to appoint a person responsible for the implementation of the compliance program may result in the RE not meeting the reporting, record keeping, verifying identity, and applying other compliance measures requirements. This could result in structural gaps that leave the RE vulnerable to ML/TF offences, which affects the achievement of the objectives of the Act and FINTRAC's ability to carry out its mandate, which potentially exposes Canada's financial system and Canadians to ML/TF risks.

Deficiencies in other compliance requirements, such as reporting, record keeping and verifying identity, may be the result of the deficient implementation of a compliance program. FINTRAC will consider the overall effectiveness of the compliance program and the fulfillment of other compliance requirements when it assesses an RE's compliance with the requirement to appoint a compliance officer.

3.2 Penalty determination for a violation related to the appointment of a compliance officer

FINTRAC will assess the level of harm and penalty for failing to appoint a compliance officer using the criteria listed below.

Level of harm	Type of non-compliance	Description of non-compliance with the compliance officer requirement	Penalty (not considering mitigating factors)
Level 1	The requirement is not met to any degree, or what is in place is not functional, causing widespread non-compliance. This is complete or widespread non-compliance.	No one is carrying out the duties of implementing any part of the compliance program. As such, there is widespread and serious non-compliance.	$100,000

Level of harm	Type of non-compliance	Description of non-compliance with the compliance officer requirement	Penalty (not considering mitigating factors)
Level 2	An element that is priority to achieving the objectives of the Act or FINTRAC's mandate is not met. This is partial non-compliance with important weaknesses.	The RE has not ensured that the appointed person performs all the necessary duties related to the: 1. Implementation of the compliance policies and procedures;2. Implementation of the policies and procedures related to mitigating high risks3. Implementation of the risk-based approach in accordance with the risk assessment; 4. Implementation of the ongoing training program;5. Implementation of the prescribed review of the compliance program every 2 years; and6. Implementation of other applicable requirements under the Act and its regulations.	$75,000

Level of harm	Type of non-compliance	Description of non-compliance with the compliance officer requirement	Penalty (not considering mitigating factors)
Level 3	An element that forms the basis for achieving the objectives of the Act or FINTRAC's mandate is not met.This is partial non-compliance with moderate weaknesses.	The RE has not provided the appointed person with the authority to implement the compliance program, including the authority to make any necessary changes. The RE has not provided the appointed person with adequate resources to implement the compliance program.	$50,000
Level 4	An element that enables the efficient achievement of the objectives of the Act or FINTRAC's mandate is not met. This is to partial non-compliance with lesser weaknesses.	The RE has not ensured that the appointed person has adequate knowledge of the Act and its regulations, and how the requirements apply to the business.	$25,000

Table 3—Levels of harm and penalties for a violation related to the appointment of a compliance officer

3.2.1 Level 1 harm: Failure to appoint a person responsible for the implementation of the compliance program When an RE fails to assign the duties related to the implementation of the compliance program to a person, the objectives of the Act and FINTRAC's mandate suffer from the highest level of harm. This is because there would be no oversight to ensure that, for example, policies and procedures are followed, or that ongoing training is provided. This lack of oversight means that there is a high risk that the existing compliance program will become out-of-date or ineffective. Over time, this would likely have an important impact on an RE's compliance with the Act and its regulations, and would likely result in other requirements not being met, such as reporting, record keeping and verifying client identity. As a result, the associated penalty is the prescribed maximum of $100,000.

3.2.2 Level 2 harm: Failure to ensure that the appointed person performs all the necessary duties The second-highest level of risk is attributed when an RE has appointed a compliance officer with the proper authorities and resources but it has not made sure that this person performs all the duties related to the implementation of the compliance program. As a result, the associated penalty is $75,000.

3.2.3 Level 3 harm: Failure to provide the appointed person with authority and resources When the appointed person lacks the authority and resources to carry out the duties and measures that are necessary for the implementation and maintenance of the compliance program, this can result in inefficiencies in detecting and correcting non-compliance with the requirements of the Act and its regulations. As a result, the associated penalty is $50,000.

3.2.4 Level 4 harm: Failure to ensure that the appointed person has adequate knowledge At a minimum, the RE must ensure that the compliance officer has sufficient knowledge of the Act and its regulations, of ML/TF concepts and risks and of how they relate to the business. The compliance officer must have a good understanding of the risks most relevant to the RE and frequently encountered by the industry. Without this knowledge, the measures adopted may not be the most effective or efficient to addressing the RE's compliance needs, thereby affecting the implementation of the compliance program. As a result, the associated penalty is $25,000.

4. Violations related to compliance policies and procedures, including policies and procedures in respect of prescribed special measures for high risks

This section outlines FINTRAC's approach for failing to develop and apply compliance policies and procedures, including the harm assessment and penalty calculation.

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
9.6(1)	71(1)(b)	Failure of a person or entity to develop and apply written compliance policies and procedures that are kept up to date and, in the case of an entity, are approved by a senior officer	Serious$1-$100,000
9.6(3)	71.1	Failure of a person or entity to take the prescribed special measures	Serious$1-$100,000

Table 4— Violations related to compliance policies and procedures, including policies and procedures in respect of prescribed special measures for high risks

4.1 Harm done in the case of violations related to compliance policies and procedures

The development, documentation and application of compliance policies and procedures, including those for enhanced measures to mitigate high risk, ensure that a comprehensive framework and robust controls are in place to comply with the Act and its regulations.

Policies guide REs' decisions and actions with respect to AML/ATF requirements, and ensure that all activities take place within set boundaries. Procedures are the specific methods employed to put policies in action in day-to-day operations.

Policies and procedures are critical because they set out important principles and standards that staff and delegated persons with compliance responsibilities must meet in a consistent manner. Documented policies and procedures also serve to ensure clarity and consistency in business operations for instance, when there are changes in personnel. For each requirement under the Act and its regulations, the policies and procedures documents must include a description of when the requirement is triggered; the information that must be reported, recorded or considered; the step-by-step procedures to ensure that the requirement is fulfilled; and where applicable, the timelines associated to the requirement.

Failing to develop, apply, and keep written policies and procedures up to date can result in not meeting other requirements under the Act and its regulations, and undervalues sound business practices designed to minimize ML/TF.

4.2 Penalty determination for a violation related to compliance policies and procedures

FINTRAC will assess the level of harm and penalty for failing to develop, document and apply written compliance policies and procedures using the criteria listed below.

Level of harm	Type of non-compliance	Description of the non-compliance with the compliance policies and procedures requirement	Penalty (not considering mitigating factors)
Level 1	The requirement is not met to any degree, or what is in place is not functional, causing widespread non-compliance. This is complete or widespread non-compliance.	Policies and procedures for all, or most, of the requirements are not developed or applied.	$100,000

Level of harm	Type of non-compliance	Description of the non-compliance with the compliance policies and procedures requirement	Penalty (not considering mitigating factors)
Level 2	An element that is priority for achieving the objectives of the Act or FINTRAC's mandate is not met. This is partial non-compliance with important weaknesses.	Policies and procedures for priority requirements are not developed or applied, including:1. Know your client requirements: 1. verifying client identity 2. determination of politically exposed persons and heads of international organizations, and their family members and close associates 3. obtaining beneficial ownership information 4. third party determination2. Suspicious transaction and terrorist property reporting; and3. Compliance with Ministerial Directives.	$75,000

Level of harm	Type of non-compliance	Description of the non-compliance with the compliance policies and procedures requirement	Penalty (not considering mitigating factors)
Level 3	An element that forms the basis for achieving the objectives of the Act or FINTRAC's mandate is not met.This is partial non-compliance with moderate weaknesses.	Policies and procedures for basic requirements are not developed or applied, including:1. Reporting large cash transactions, and if applicable electronic funds transfers, and casino disbursements; 2. Ongoing monitoring of business relationships 3. Keeping prescribed records, **except** copies of submitted Suspicious Transaction Reports (STRs) and Casino Disbursement Reports (CDRs); and4. Performing the prescribed risk assessment and the prescribed review every 2 years.	$50,000

Level of harm	Type of non-compliance	Description of the non-compliance with the compliance policies and procedures requirement	Penalty (not considering mitigating factors)
Level 4	An element that enables the efficient achievement of the objectives of the Act or FINTRAC's mandate is not met. This is partial non-compliance with lesser weaknesses.	Policies and procedures for requirements that enable efficiency are not developed or applied, including keeping copies of submitted STRs and CDRs.	$25,000

Table 5—Levels of harm and penalties for violations related to compliance policies and procedures

4.2.1 Level 1 harm: Policies and procedures are not developed or applied When policies and procedures have not been developed or are not applied, the foundational framework and controls that are required to comply with the requirements of the Act and its regulations are absent. This creates an environment where widespread non-compliance and systemic weaknesses in detecting, preventing and deterring ML/TF is possible, and therefore poses the most harm to the objectives of the Act and FINTRAC's mandate. As a result, the associated penalty is the prescribed maximum of $100,000.

4.2.2 Level 2 harm: Policies and procedures for priority requirements are not developed or applied Reporting suspicious transactions and terrorist property, performing know your client procedures and complying with the minister's directives are priority requirements for Canada's AML/ATF efforts, because they are essential for the detection, prevention and deterrence of ML/TF offences. Non-compliance with these requirements is assessed as posing Level 2 harm because, while other measures may be in place, failing to meet priority requirements can pose high levels of harm to the objectives of the Act and FINTRAC's ability to fulfill its mandate. As a result, the associated penalty is $75,000.

The detection and reporting of transactions that are suspected of being related to ML/TF is therefore critical for FINTRAC's analysis and disclosure of financial intelligence that supports the investigation and prosecution of the crimes. Performing know your client procedures such as identifying clients and obtaining information on those controlling or benefitting from the movement of funds deter criminals from using Canada's financial system for ML/TF; they are also necessary to identify high-risk clients, business relationships and transactions for the purpose of reporting to FINTRAC. When proper client identification, and information on the individuals owning or controlling entities measures are not taken by REs, the objectives of the Act and FINTRAC's mandate are harmed significantly since it is then not possible for the RE to mitigate risks; for FINTRAC to conduct analysis on particular subjects; for law enforcement to investigate individuals for ML/TF offences.

Ministerial directives are targeted measures to protect Canada's financial system from being used as a vehicle for ML/TF. Compliance policies and procedures that do not meet the measures set out in a ministerial directive can result in the failure to comply with priority areas intended to detect, prevent and deter specific threats to Canada's financial system and the safety of Canadians. As a result, such a failure represents very significant harm to the achievement of the objectives set out in paragraph 3(d) of the Act.

4.2.3 Level 3 harm: Policies and procedures for basic requirements are not developed or applied Requirements that form the basis for the detection, prevention and deterrence of ML/TF are: reporting large cash transactions, reporting electronic funds transfers and casino disbursements (as required), monitoring business relationships, record keeping, assessing risk, and reviewing the effectiveness of the compliance program. Record keeping requirements are in place to ensure that the information necessary to meet other requirements of the Act and its regulations is kept. Ultimately, the information can serve as evidence in support of investigations and prosecutions of ML/TF offences.

The measures to implement these requirements are fundamental because they support Canada's AML/ATF regime by identifying and mitigating the risks related to transactions at risk of being used for ML/TF, and by helping to detect and deter those inclined to abuse the financial system for ML/TF purposes. Non-compliance with these requirements is assessed as Level 3 harm because it can pose moderate harm to the objectives of the Act and FINTRAC's mandate. Therefore, the associated penalty is $50,000.

4.2.4 Level 4 harm: Policies and procedures for requirements that enable efficiency are not developed or applied Efficiency in the fight against ML/TF is found in those elements that assist in achieving the objectives of the Act and FINTRAC's mandate and support Canada's AML/ATF regime by maximizing its performance. Non-compliance with these elements poses Level 4 harm because it diminishes the efficiency of Canada's AML/ATF

regime, but does not affect priority or basic elements. Therefore, the associated penalty is $25,000.

Keeping complete and accurate records, including copies of STRs, and CDRs (as required), ensures that REs, police, law enforcement and FINTRAC have quick and easy access to reports related to transactions or financial activities. The information captured in STRs and CDRs is required in other records under the Act. Since the information in these copies is likely kept elsewhere, failing to keep these records poses lower harm to the objective of the Act and FINTRAC's mandate.

4.3 Penalty determination for a violation related to compliance policies and procedures for taking enhanced measures to mitigate high risks

FINTRAC will assess the level of harm and penalty for failing to develop, document and apply compliance policies and procedures on taking enhanced measures to mitigate high risks using the criteria listed below.

Level of harm	Type of non-compliance	Description of the non-compliance with the policies and procedures for taking enhanced measures to mitigate high risks requirement	Penalty (not considering mitigating factors)
Level 1	The requirement is not met to any degree, or what is in place is not functional, causing widespread non-compliance. This is complete or widespread non-compliance.	Policies and procedures for taking enhanced measures for high risk are not developed or applied for any, or most, of the prescribed elements.	$100,000

Level of harm	Type of non-compliance	Description of the non-compliance with the policies and procedures for taking enhanced measures to mitigate high risks requirement	Penalty (not considering mitigating factors)
Level 2	An element that is priority for achieving the objectives of the Act or FINTRAC's mandate is not met. This is partial non-compliance with important weaknesses.	Policies and procedures relating to priority requirements for enhanced measures are not developed or applied for:1. Verifying client identity;2. Keeping client and beneficial ownership information up to date; and;3. Conducting ongoing monitoring of business relationships to identify suspicious transactions.	$75,000

Level of harm	Type of non-compliance	Description of the non-compliance with the policies and procedures for taking enhanced measures to mitigate high risks requirement	Penalty (not considering mitigating factors)
Level 3	An element that forms the basis for achieving the objectives of the Act or FINTRAC's mandate is not met.This is partial non-compliance with moderate weaknesses.	Policies and procedures relating to basic requirements for enhanced measures are not developed or applied, which includes any other measures needed to mitigate high risk.	$50,000

Table 6—Levels of harm and penalties for a violation related to compliance policies and procedures for taking enhanced measures to mitigate high risks violations

Note: Level 4 harm is not applicable in the case of this violation, as the measures related to addressing high-risk situations do not play a supporting role; they are either priority or basic elements to mitigate the risks of ML/TF.

4.3.1 Level 1 harm: Policies and procedures for taking enhanced measures to mitigate high risks are not developed or applied for any, or most, of the prescribed elements The development and application of policies and procedures for taking prescribed enhanced measures to mitigate high risk is critical to the AML/ATF regime in the detection, prevention and deterrence of ML/TF offences. These enhanced measures are meant to address the risks posed by those elements that have been expressly identified as being the most vulnerable to ML/TF. When policies and procedures for taking enhanced measures to mitigate high risks have not been developed for any, or most of the prescribed requirements, the controls and framework that are required to mitigate high risks are absent. There is a high likelihood that the highest-risk situations are not being mitigated and identified for reporting to FINTRAC,

leaving the RE and Canada's financial system vulnerable to ML/TF offences. This poses the highest harm and incurs a penalty of $100,000.

4.3.2 Level 2 harm: Policies and procedures related to priority enhanced measures are not developed or applied Taking enhanced measures to identify persons and entities controlling and benefitting from the movement of funds, keep their information up to date, and conduct ongoing monitoring to detect suspicious transactions are priority measures for ML/TF risk mitigation as they help make the most current information available in situations of high risk. Policies and procedures that do not address these elements are incomplete and can result in inadequate risk mitigation; and have a substantial impact on the detection and mitigation of high risks, including reporting related to high-risk transactions. This represents an important weakness in an RE's compliance program, which could have an important impact on the objectives of the Act and FINTRAC's mandate; and therefore poses Level 2 harm, which incurs a penalty of $75,000.

4.3.3 Level 3 harm: Policies and procedures relating to any other enhanced measures needed to mitigate high risks are not developed or applied In addition to the specific enhanced measures prescribed for high-risk mitigation, other mitigation measures may also be necessary to reduce ML/TF vulnerabilities. Policies and procedures that do not consider other measures specific to the RE's assessment of risks can result in ineffective or incomplete strategies to reduce ML/TF vulnerabilities. Depending on the nature of the risk and the RE's size and complexity, this type of non-compliance could have an impact on the objectives of the Act and FINTRAC's mandate. This type of non-compliance poses Level 3 harm and incurs a penalty of $50,000.

5. Violation related to assessing and documenting the risks of ML/TF

This section outlines FINTRAC's approach to failing to assess and document the risks of ML/TF, including the harm assessment and penalty calculation.

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
9.6(1)	71(1)(c)	Failure of a person or entity to assess and document the risk referred to in subsection 9.6(2) of the Act, taking into consideration prescribed factors	Serious$1-$100,000

Table 7— Violation related to assessing and documenting the risks of ML/TF

5.1 Harm done in the case of a violation related to assessing and documenting the risks of ML/TF

Assessing and documenting ML/TF risks ensures that REs are aware of their potential exposure and vulnerability to ML/TF. By identifying areas and levels of risk, REs may apply appropriate mitigation measures to reduce those risks. REs are able to turn more attention to higher-risk areas, thereby effectively contributing to the objectives of the Act and FINTRAC's ability to carry out its mandate.

Failing to assess and document the risks of ML/TF prevents REs from identifying areas of its operations that are vulnerable to being exploited for ML/TF purposes, and prevents appropriate mitigation measures from being put in place. This can also lead to failing to identify high-risk clients and business relationships for which enhanced risk mitigation measures must be applied. This can further result in the failure to detect and report suspicious transactions to FINTRAC.

5.2 Penalty determination for a violation related to assessing and documenting the risks of ML/TF

FINTRAC will assess the level of harm and penalty for failing to assess and document the risks of ML/TF offences using the criteria listed below.

Level of harm	Type of non-compliance	Description of the non-compliance for the risk assessment requirement	Penalty (not considering mitigating factors)
Level 1	The requirement is not met, to any degree, or what is in place is not functional, causing widespread non-compliance. This is complete or widespread non-compliance	An assessment of ML/TF risks has not been conducted or documented for any, or most, of the prescribed factors.	$100,000

Level of harm	Type of non-compliance	Description of the non-compliance for the risk assessment requirement	Penalty (not considering mitigating factors)
Level 2	An element that is priority for achieving the objectives of the Act or FINTRAC's mandate is not met. This is partial non-compliance with important weaknesses.	The risk assessment does not include priority elements, including those for high-risk situations, such as: 1. Politically exposed foreign persons, their family members and close associates;2. Entities for which beneficial ownership information cannot be obtained or confirmed;3. Clients who are mentioned in a submitted TPR; and4. Products, services, delivery channels, geographic locations or types of persons or entities, that are identified as posing a high risk by a ministerial directive, by FINTRAC, or by criteria established by the RE.	$75,000

Level of harm	Type of non-compliance	Description of the non-compliance for the risk assessment requirement	Penalty (not considering mitigating factors)
Level 3	An element that forms the basis for achieving the objectives of the Act or FINTRAC's mandate is not met.This is partial non-compliance with moderate weaknesses.	The risk assessment does not include basic elements such as:1. Products, services and delivery channels offered;2. Clients and business relationships;3. Geographic locations, (including foreign and domestic activities, clients, and business relationships); and4. New technologies.	$50,000
Level 4	An element that enables the efficient achievement of the objectives of the Act or FINTRAC's mandate is not met. This is to partial non-compliance with lesser weaknesses.	The risk assessment does not include other relevant factors that could impact ML/TF risks.	$25,000

Table 8—Levels of harm and penalties for a violation related to assessing and documenting the risks of ML/TF

5.2.1 Level 1 harm: An assessment of ML/TF risks has not been conducted or documented for any, or most, of the prescribed factors

When an assessment of ML/TF risks has not been conducted or documented, or the assessment does not address any of the prescribed requirements, there is complete or widespread non-compliance with the regulations. Failing to assess and identify ML/TF risks prevents REs from putting in place mitigation measures, leaving them vulnerable to being used for ML/TF, especially in those areas that pose the highest risk. This is assessed as posing the highest level of harm, as it has the highest impact on achieving objectives of the Act and FINTRAC's mandate, and incurs a penalty of $100,000.

5.2.2 Level 2 harm: The risk assessment does not include priority elements including those for high-risk situations The regulations, ministerial directives, FINTRAC and other AML/ATF authorities have identified situations that inherently present a high risk of ML/TF, which are key for the prescribed risk assessment. It is critical for REs to consider and assess them where applicable. Failing to consider high-risk situations may result in important weaknesses in the compliance program such as poor mitigation measures and high-risk situations potentially not being detected and reported to FINTRAC on suspicion of ML/TF offences. Non-compliance with this requirement poses Level 2 harm and incurs a penalty of $75,000.

5.2.3 Level 3 harm: The risk assessment does not include the basic elements ML/TF risk assessments allow REs to understand the vulnerabilities they are exposed to. Comprehensive risk assessments must include the prescribed elements as their basis in order to support risk mitigation. A risk assessment that does not include one or more of the prescribed elements may lead to weaknesses in the identification and mitigation of common risks, leaving the RE vulnerable to ML/TF offences and unable to effectively identify transactions that must be reported. Non-compliance with this requirement poses Level 3 harm and incurs a penalty of $50,000.

5.2.4 Level 4 harm: The risk assessment does not include any other relevant factors that could impact ML/TF risks Assessing other relevant factors allows REs to understand the ML/TF risks applicable to their operations and contributes to the efficiency of the risk assessment and mitigation strategies. Non-compliance with this requirement poses Level 4 harm and incurs a penalty of $25,000.

6. Violation related to the ongoing training program

This section outlines FINTRAC's approach to failing to develop and maintain a written ongoing training program, including the harm assessment and penalty calculation.

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
9.6(1)	71(1)(d)	Failure of a person or entity that has employees, agents or mandataries or other persons authorized to act on their behalf to develop and maintain a written ongoing compliance training program for those employees, agents or mandataries or persons	Serious$1-$100,000

Table 9— Violation related to the ongoing training program

6.1 Harm done in the case of a violation related to the ongoing training program

The purpose of a written ongoing compliance training program is to ensure that all employees, agents, mandataries and other persons authorized to act on an RE's behalf understand the requirements of the Act and its regulations and follow the policies and procedures that have been established for compliance. It also ensures that employees, agents, mandataries and other persons authorized to act on an RE's behalf understand ML/TF matters enough to be able to identify facts that may indicate financial transactions or activities related to ML/TF offences.

Failing to develop and maintain a written ongoing training program may result in the above listed purposes not being met over time, and consequently, an RE failing to comply with the requirements under the Act and its regulations. In turn, this non-compliance could ultimately affect the objectives of the Act and FINTRAC's ability to deliver on its mandate.

6.2 Penalty determination for a violation related to the ongoing training program

FINTRAC will assess the level of harm and penalty for failing to develop and maintain a written ongoing training program using the criteria listed below.

Level of harm	Type of non-compliance	Description of the non-compliance for the training program requirement	Penalty (not considering mitigating factors)
Level 1	The requirement is not met to any degree, or what is in place is not functional, causing widespread non-compliance. This is complete or widespread non-compliance.	A documented training program is not developed or maintained to cover all, or most, of the elements to comply with the Act and its regulations.	$100,000

Level of harm	Type of non-compliance	Description of the non-compliance for the training program requirement	Penalty (not considering mitigating factors)
Level 2	An element that is priority for achieving the objectives of the Act or FINTRAC's mandate is not met. This is partial non-compliance with important weaknesses.	The training program is missing priority elements, such as maintaining training on the:1. Compliance policies and procedures established; 2. Responsibilities of employees, agents and those acting on behalf of the RE when dealing with suspicious transactions; and3. Key ML/TF concepts including background information on how ML/TF related to the business.	$75,000

Level of harm	Type of non-compliance	Description of the non-compliance for the training program requirement	Penalty (not considering mitigating factors)
Level 3	An element that forms the basis for achieving the objectives of the Act or FINTRAC's mandate is not met.This is partial non-compliance with moderate weaknesses.	The training program is missing basic elements, such as:1. Frequency or timing of the training to be delivered; and2. Content that is relevant and specific for all employees, agents, and those acting on the RE's behalf.	$50,000
Level 4	An element that enables the efficient achievement of the objectives of the Act or FINTRAC's mandate is not met. This is to partial non-compliance with lesser weaknesses.	The training program is not maintained on an ongoing basis.	$25,000

Table 10—Levels of harm and penalties for a violation related to the ongoing training program

6.2.1 Level 1 harm: A documented training program is not developed or maintained When a training program has not been developed or maintained, or has been but only to a minimal degree, the foundational framework and controls that are required to comply with the requirements of the Act and its regulations are absent. This can potentially lead to widespread non-compliance and systemic weaknesses in the detection, prevention and de-

terrence of ML/TF, posing the highest possible harm to the Act's objectives and FINTRAC's mandate. Therefore, the penalty is $100,000, the prescribed maximum amount.

6.2.2 Level 2 harm: The training program is missing elements that are priority Priority elements for the training program include covering the established policies and procedures to comply with all the requirements of the Act and its regulations, the responsibilities of employees, agents and those acting on the RE's behalf when dealing with suspicious transactions, and key ML/TF concepts including background information on how they relate to the business. Non-compliance with these elements is assessed as Level 2 harm because a lack of training in these elements could cause failures in meeting other requirements such as reporting, record keeping and verifying client identity. As a result, the penalty is $75,000.

6.2.3 Level 3 harm: The training program is missing elements that are basic A plan that addresses the timing and frequency of delivery of the training program, that identifies who will receive the training and that includes content that is relevant and specific to different roles in the organization is forms the basis for the delivery of the training program. Not only does it help to comply with the requirement to maintain an ongoing training program, but it clearly lays out which employees, agents and those acting on an RE's behalf are to be provided with relevant training to effectively comply with all the requirements. The likelihood of exposure to ML/TF offences and associated risks varies for employees, depending on their roles. For example, tailored training for employees that detect transactions that need to be reported, that verify client identity, that keep records, and perform other customer due diligence measures will have a greater impact on compliance. Non-compliance with these requirements poses Level 3 harm, which incurs a penalty of $50,000.

6.2.4 Level 4 harm: The training program is not maintained on an ongoing basis Efficiency in the fight against ML/TF is found in those elements that assist in achieving the objectives of the Act and FINTRAC's mandate, and support Canada's AML/ATF regime by maximizing its performance. Guidelines dictating the frequency of training ensure that personnel receive information and training on new compliance requirements and are provided with reminders on existing requirements. Failing to establish clear guidelines for ongoing compliance training may result in program weaknesses over time, for example, due to changes to regulatory requirements, or changes in staff or organizational structure. This may lead to the RE not meeting its requirements to report, identify clients and keep records. Non-compliance with this requirement is assessed as posing Level 4 harm and incurs a penalty of $25,000.

7. Violations related to the prescribed review

This section outlines FINTRAC's approach to failing to institute and document the prescribed review, including the harm assessment and penalty calculation.

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
9.6(1)	71(1)(e)	Failure of a person or entity to institute and document the prescribed review	Serious$1-$100,000
9.6(1)	71(2)	Failure of a person or entity to report prescribed information within 30 days after assessment	Serious$1-$100,000

Table 11—Violations related to the prescribed review

7.1 Harm done in the case of violations related to the prescribed review

Changes to an organization's structure, personnel, policies and processes, and environment may over time, if not immediately, require revisions to the compliance program that is in place. The purpose of the prescribed review is to ensure that the RE's compliance program is continuously adapted to continue to comply with the requirements of the Act and its regulations. The prescribed review of the compliance policies and procedures, and that of the ongoing training program tests the reporting, client identity verification, record keeping and appropriate mitigation measures application. The prescribed review of the risk assessment ensures that the RE is adequately assessing, identifying and mitigating the risks of ML/TF over time.

Failing to conduct the prescribed review signals that the RE may not be fulfilling one or more of its other requirements under the Act and its regulations, by not having kept up to date with changes in the organization or external changes such as new technologies in the financial sector and regulatory updates. Additionally, any gaps or ineffective processes in the existing compliance program may go undetected, leading to uncorrected non-compliance. For example, the RE's existing risk assessment may not identify its most vulnerable areas, making it difficult to apply appropriate mitigating measures, to reduce the risks of ML/TF and contribute to safety of Canada's financial system and that of Canadians.

Ultimately, undetected non-compliance and inefficiencies could result in harming the achievement of the objectives of the Act and FINTRAC's mandate.

7.2 Penalty determination for violations related to the prescribed review

FINTRAC will assess the level of harm and penalty for failing to institute and document the prescribed review using the criteria listed below.

Level of harm	Type of non-compliance	Description of the non-compliance with the prescribed review requirement	Penalty (not considering mitigating factors)
Level 1	The requirement is not met to any degree, or what is in place is not functional, causing widespread non-compliance. This is complete or widespread non-compliance.	The RE has not conducted any part or most of the prescribed review.	$100,000
Level 2	An element that is priority for achieving the objectives of the Act or FINTRAC's mandate is not met. This is partial non-compliance with important weaknesses.	The review does not include testing for effectiveness; andThe scope of the review does not cover the compliance policies and procedures, risk assessment, and training program.	$75,000

Level of harm	Type of non-compliance	Description of the non-compliance with the prescribed review requirement	Penalty (not considering mitigating factors)
Level 3	An element that forms the basis for achieving the objectives of the Act or FINTRAC's mandate is not met.This is partial non-compliance with moderate weaknesses.	The review does not evaluate the compliance program documentation, such as policies and procedures, to ensure that they are complete and up to date.	$50,000
Level 4	An element that enables the efficient achievement of the objectives of the Act or FINTRAC's mandate is not met. This is to partial non-compliance with lesser weaknesses.	The review is conducted beyond the prescribed two-year period.The review methods are not clearly documented and do not demonstrate how the compliance program is tested for effective-ness.When required, an internal or external auditor did not conduct the review.	$25,000

Table 12—Levels of harm and penalties for violations related to the prescribed review

7.2.1 Level 1 harm: The RE has not conducted any part or most of the prescribed review When an RE does not conduct the prescribed

review, or when the review is absolutely minimal, this poses the highest harm to the objectives of the Act and FINTRAC's mandate. It is highly possible that policies, procedures, training, and risk assessments are outdated, inaccurate or ineffective, and therefore non-compliance with reporting, record keeping and client identification requirements is also more likely. This represents Level 1 harm, which incurs a penalty of $100,000 as the requirement has not been met to any degree, or in a manner that is too minimal for the requirement to be considered as being met.

7.2.2 Level 2 harm: The review does not include testing for effectiveness; and the scope of the review does not cover the compliance policies and procedures, risk assessment, and training program Effectiveness testing and a comprehensive review are key to meeting the requirement. Next to not instituting the prescribed review, the second-highest level of harm comes from reviews that do not include testing the effectiveness of the compliance program, and reviews that do not cover key elements of the compliance policies and procedures, risk assessment, and training program. This type of non-compliance poses Level 2 harm and incurs a penalty of $75,000.

A review that does not include effectiveness testing does not look at how the compliance program is applied in practice. It is essentially only a theoretical review of the documentation that has been developed. Even if the documentation were in order, there is still the potential that the policies and procedures are not being put into practice and this poses a high risk of errors and inadequacies in the compliance program that are not detected.

Additionally, when the review is incomplete, meaning that key elements are overlooked from the assessment, large gaps and weaknesses in the compliance program can go undetected. For example, if the review omitted to assess the training program, the staff may not be trained properly to carry out their duties. In turn, this could result in non-compliance with requirements of the Act and its regulations, despite having policies and procedures, and risk assessments.

7.2.3 Level 3 harm: The review does not evaluate the compliance program documentation to ensure that they are complete and up to date The documentation of the compliance program is the basis from which compliance is achieved. To this end, the prescribed review should at a minimum assess the documented policies and procedures, training program and risk assessment to ensure that the standards established by the RE is clear, complete and up to date, in accordance with the requirements of the Act and its regulations. A review that does not evaluate the compliance program documentation for completeness and accuracy could lead to processes that are not clearly understood, or are applied inconsistently. This type of non-compliance poses Level 3 harm and incurs a penalty of $50,000.

7.2.4 Level 4 harm: The review is conducted beyond the prescribed two-year frequency; the review methods are not clearly documented and do not demonstrate how the compliance program is tested for effectiveness; and when required, an internal or external auditor did not conduct the review Efficiency in the fight against ML/TF is found in those elements that assist in achieving the objectives of the Act and FINTRAC's mandate, and support Canada's AML/ATF regime by maximizing its performance. Non-compliance with these elements poses Level 4 harm and incurs a penalty of $25,000.

In order to identify and correct gaps in the compliance program in a timely manner, the prescribed frequency of the review is every two years. Failing to institute a review that respects this frequency could result in unidentified deficiencies that remain uncorrected for an undetermined period of time. If the period between reviews is extensive, undetected deficiencies could be exploited for ML/TF purposes.

Clearly documenting the methods used to conduct the review and demonstrating how program effectiveness will be tested contributes to the efficiency of the review and the RE's AML/ATF efforts. For example, the method for sampling and testing should reflect the size and complexity of the RE's operations to ensure that the review's findings are representative.

Where applicable, an internal or external auditor is to perform the review. This is to ensure an independent assessment of the compliance program's effectiveness and that the findings are neutral and objective. The expertise of an auditor also ensures that the scope and the effectiveness testing are adequate and comprehensive.

7.3 Harm done in the case of a violation related to prescribed review reporting

Reporting prescribed information following the compliance program's review provides an RE's senior officer with a timely understanding and oversight of the RE's overall compliance with the Act and its regulations, and of changes that would be required to improve or ensure compliance and risk mitigation. Failing to report the results of the prescribed review to an RE's senior officer within 30 days of the assessment impedes the senior officer's ability to oversee the effective application of policies and procedures and to manage ML/TF risks. This can undermine risk mitigation, leaving the RE vulnerable to ML/TF offences.

7.4 Penalty determination for a violation related to prescribed review reporting

FINTRAC will assess the level of harm and penalty for a failing to report prescribed information on the review using the criteria listed below.

Level of harm	Type of non-compliance	Description of the non-compliance with the reporting on the prescribed review requirement	Penalty (not considering mitigating factors)
Level 1	The requirement is not met to any degree, or what is in place is not functional, causing widespread non-compliance. This is complete or widespread non-compliance.	There is no reporting, or minimal reporting, of the results of the review to a senior officer.	$100,000
Level 2	An element that is key to achieving the objectives of the Act or FINTRAC's mandate is not met. This is partial non-compliance with important weaknesses.	Priority elements of the prescribed review are not reported to a senior officer, including:1. Results;2. Updates to policies and procedures, if applicable; and3. The implementation status of the updates to policies and procedures.	$75,000

Level of harm	Type of non-compliance	Description of the non-compliance with the reporting on the prescribed review requirement	Penalty (not considering mitigating factors)
Level 3	An element that forms the basis for achieving the objectives of the Act or FINTRAC's mandate is not met.This is partial non-compliance with moderate weaknesses.	The prescribed information was reported to an individual who is not a senior officer and does not have the authority to ensure that the changes to the compliance program are implemented.	$50,000
Level 4	An element that enables the efficient achievement of the objectives of the Act or FINTRAC's mandate is not met. This is to partial non-compliance with lesser weaknesses.	The prescribed information was reported beyond the 30-day period following the assessment, delaying the implementation of the required compliance program changes.	$25,000

Table 13—Levels of harm and penalties for a violation related to prescribed review reporting

7.4.1 Level 1 harm: There is no reporting, or minimal reporting, of the results to a senior officer Reporting to senior staff helps to ensure that those responsible for the RE's compliance are aware of the program's performance, including the weaknesses that must be addressed and oversight of the compliance officer's implementation of the compliance program. The harm is the greatest when the results of the review are not reported, or when minimal results are reported to a senior officer because there is a high likelihood that those

responsible for the business would not be aware the compliance challenges, making it impossible to adequately assess their seriousness, manage risks, and take corrective measures where needed. Non-compliance of this type poses Level 1 harm and incurs a penalty of $100,000.

7.4.2 Level 2 harm: Priority elements of the prescribed review are not reported to a senior officer The priority elements of the prescribed review that must be reported to senior management include: the findings of the review, updates to policies and procedures, and the implementation status of the updates. These elements give senior management a comprehensive picture of the RE's state of compliance; with this information, management can take the appropriate actions to mitigate risks and correct non-compliance. When the reporting does not cover one or more of these priority elements, it is incomplete and poses Level 2 harm, incurring a penalty of $75,000.

7.4.3 Level 3 harm: The prescribed information was reported to an individual who is not a senior officer and does not have the authority to ensure that the changes to the compliance program are implemented If the results are reported to someone who is not a senior officer, or if they are reported to a senior officer who is not in the position to bring about changes to improve the compliance program, there is a risk that nothing will come of the review. Without a senior officer's involvement, the proper attention and resources will not be given to the compliance program. As result, non-compliance issues and ML/TF risks could remain and increase in gravity over time. This type of non-compliance poses Level 3 harm and incurs a penalty of $50,000.

7.4.4 Level 4 harm: The prescribed information was reported beyond the 30-day period following the assessment, delaying the implementation of the required compliance program changes Timely communication allows senior management to make informed strategic decisions. When the prescribed information was reported to a senior officer beyond the 30-day period following the assessment, the delay affects the changes to the compliance program, which diminishes the efficient achievement of the objectives of the Act and FINTRAC's mandate. Those in charge of an RE's governance are unable to oversee the timely and efficient improvement of the compliance program and manage the ML/TF risks. This type of non-compliance poses Level 4 harm and incurs a penalty of $25,000.# Risk assessment guidance

Overview

FINTRAC developed this guidance to help you understand, as a reporting entity (RE):

- the types of money laundering (ML) and terrorist financing (TF) risks that you may encounter as a result of your business activities and clients; and

- what is a risk-based approach (RBA) and how you can use one to conduct a risk assessment of your business activities and clients.

This guidance also provides tools that you can use to develop and implement mitigation measures to address high-risk areas identified through your risk assessment. You can use these tools or you can develop your own risk assessment tools.This guidance is applicable to all REs subject to the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and associated Regulations. However, **some risk assessment obligations and/or examples may only apply to certain sectors**.

As part of your compliance program requirements under the PCMLTFA and associated Regulations, you must conduct a risk assessment of your ML/TF risks.Footnote 1 You are responsible for completing and documenting your own risk assessment. However, FINTRAC does not prescribe how a risk assessment should be conducted. Rather, this guidance explains an internationally recognized way of conducting a risk assessment using an RBA and provides you with other tools that may help you meet your risk assessment obligations. For more information about your risk assessment obligations see FINTRAC's Compliance program requirements guidance.

Who is this guidance for

- All reporting entities (REs)

1. What is risk?

Risk is the likelihood of a negative occurrence or event happening and its consequences. In simple terms, risk is a combination of the chance that something may happen and the degree of damage or loss that may result. In the context of ML/TF, risk means:

- **At the national level:** Threats and vulnerabilities presented by ML/TF that put the integrity of Canada's financial system at risk, as well as the safety and security of Canadians. For example, organized crime groups operating in Canada that launder the proceeds of crime.
- **At the RE level:** Internal and external threats and vulnerabilities that could open an RE up to the possibility of being used to facilitate ML/TF activities. For example, a possible ML/TF risk at the RE level could be conducting business with clients located in high-risk jurisdictions or locations of concern.

Threats: A person, group or object that could cause harm. In the ML/TF context, threats could be criminals, third parties facilitating ML/TF, terrorists or terrorist groups or their funds.

Vulnerabilities: Elements of a business or its processes that are susceptible to harm and could be exploited by a threat. In the ML/TF context, vulnerabilities

could include weak business controls or high-risk products or services.

2. What are inherent and residual risks?

Inherent risk is the risk of an event or circumstance that exists before you implement controls or mitigation measures.Footnote 2 Whereas residual risk is the level of risk that remains after you have implemented controls or mitigation measures.

When assessing risk, it is important to distinguish between inherent risk and residual risk. The RBA described in this guidance focuses on the inherent risks to your business, its activities and clients.

3. What is an RBA?

An RBA is a way for you to conduct your risk assessment by considering elements of your business, clients and/or business relationships to identify the impact of possible ML/TF risks, and to apply controls and measures to mitigate these risks.

The Financial Action Task Force (FATF), has developed a series of Recommendations that are recognized as the international standard for combating money laundering, terrorism financing and other related threats to the integrity of the international financial system. Recommendation 1 on the RBA, recognizes that an RBA is an effective way to combat money laundering and terrorist financing.

Using an RBA will enable you to:

- conduct a **risk assessment** of your business activities and clients taking into consideration certain elements, including:
  - your products, services and delivery channelsFootnote 3;
  - the geographic location of your activitiesFootnote 4;
  - new developments and technologiesFootnote 5;
  - your clients and business relationshipsFootnote 6;
  - the activities of your foreign and domestic affiliatesFootnote 7 — This only applies to you if you are a financial entity, life insurance company or securities dealer, and the affiliate carries out activities similar to those of a financial entity, life insurance company or securities dealer; and
  - any other relevant factorFootnote 8.
- **mitigate the risks you identify** through the implementation of controls and measures tailored to these risks, which includes the ongoing monitoring of business relationships for the purpose of:
  - keeping **client identification** information and, if required, beneficial ownership and business relationship information up to date in accordance with the assessed level of risk;Footnote 9 reassessing the level

of risk associated with transactions and activities;Footnote 10and
  - applying **enhanced or special measures** to those transactions and business relationships identified as high-risk.Footnote 11

- identify and assess potential gaps or weaknesses of your compliance program. For example, using an RBA can help you to identify and assess risks that could impact other parts of your compliance program, such as gaps in your written policies, procedures or training program.

The PCMLTFA and associated Regulations do not prohibit you from having high-risk activities or high-risk business relationships. However, it is important that if you identify high-risk activities or high-risk business relationships that you document and implement appropriate controls to mitigate these risks and apply prescribed special measures.

It is important to remember that assessing and mitigating the risk of ML/TF is not a static exercise. The risks you identify may change or evolve over time as new products, services, affiliations, or developments and technologies enter your business or its environment. You should be regularly reassessing the ML/TF-related risks to your business, and documenting that assessment to keep it up to date. For example, if you add a new product, service or technology to your business, or open a new location, you should evaluate and document the associated risks of this change to your business.

4. What is the RBA cycle?

The RBA cycle consists of six steps to follow to complete a risk assessment. The diagram below summarizes the RBA cycle. Additional information on how to conduct each step can be found further below.

There is no prescribed methodology for the assessment of risks. FINTRAC's suggested model presents business-based and relationship-based risk assessments separately. Although presented separately in this guidance, you can complete business-based and relationship-based assessments simultaneously. You will need to adapt this model to your business should you choose to use it.

RBA cycle — Step 1: Identify your inherent risks of ML/TF

To identify your inherent risks of ML/TF, you would start by assessing the following areas of your business:

- products, services and delivery channels;
- geography;
- new developments and technologies;
- clients and business relationships;
- activities of foreign and domestic affiliates, if applicable; and
- any other relevant factors.

Business-based risk assessment Begin your risk assessment by looking at your business as a whole. This will allow you to identify where risks occur across business lines, clients or particular products or services. You will need to document mitigation controls for the areas you identify as high-risk.Footnote 12 The number of risks you identify will vary based on the type of business activities you conduct and products and/or services you offer.

To conduct a business-based risk assessment, you need to identify the inherent risks of your business by assessing your vulnerabilities to ML/TF. Your overall business-based risk assessment includes the risk posed by the following:

1. The combination of your products, services and delivery channels;
2. The geographical locations in which your business operates;
3. The impact of new developments and technologies that affect your operations;
4. The risks that result from affiliates (the activities that they carry out); and
5. Other relevant factors.

1. Products, services and delivery channels You need to identify the products, services and delivery channels or ways in which they combine that may pose higher risks of ML/TF. Delivery channels are mediums through which you offer products and/or services to clients, or through which you can conduct transactions. See Annex 2 — Table 1: Business-based examples of higher risk indicators and considerations for products, services and delivery channels.

2. Geography You need to identify the extent to which the geographic locations where you operate or undertake activities could pose a high-risk for ML/TF. Depending on your business and operations, this can range from your immediate surroundings, whether rural or urban, to a province or territory, multiple jurisdictions within Canada (domestic) or other countries. See Annex 2 — Table 2: Business-based examples of higher risk indicators and considerations for geography.

3. New developments and technologies You need to identify the risks associated with new developments and the adoption of new technologies within your business. That is, if your business intends to put in place a new service/activity/location or introduce a new technology, then you must assess it in order to analyze the potential ML/TF risks it may bring to your business, before you implement it. See Annex 2 — Table 3: Business-based examples of higher risk indicators and considerations for new developments and technologies.

4. Foreign and domestic affiliates If you are a financial entity, life insurance company or securities dealer, you need to identify the risks associated with having foreign and domestic affiliates, if the affiliate carries out activities similar to those of a financial entity, life insurance company or securities dealer. An

entity is your affiliate if one of you is wholly owned by the other, you are both wholly owned by the same entity, or your financial statements are consolidated. See Annex 2 — Table 4: Business-based examples of higher risk indicators and considerations for foreign and domestic affiliates.

5. Other relevant factors (if applicable): You need to identify other factors relevant to your business and that could have an impact on the risk of ML/TF such as:

- **legal**: related to domestic laws, regulations and potential threats
- **structural**: related to specific business models and processes

Scoring your business-based risk assessment Once you have identified and documented all the inherent risks to your business, you can assign a level or score to each risk using a scale or scoring methodology tailored to the size and type of your business. For example, very small businesses engaged in occasional, straightforward transactions may only require distinguishing between low and high-risk categories. FINTRAC expects larger businesses to establish more sophisticated risk scales or scoring methodologies, which could include additional risk categories.

By law, you must apply and document special measures for the high-risk elements of your business.Footnote 13 You must also be able to demonstrate to FINTRAC that you have put controls and measures in place to address these high-risk elements (for example, in your policies and procedures or training program), and that they are effective (this could be done through your internal or independent review). See Annex 3 — Table 6: Examples of risk segregation for a business-based risk assessment.

Additionally, you can use a likelihood and impact matrix tool similar to the one provided in Annex 4, to help you evaluate your business-based risk assessment.

Business-based risk assessment worksheet Using a business-based risk assessment worksheet could be an easy way to document the inherent risks related to your business. The worksheet below is given as an example. You can also develop your own worksheet or method to document the inherent risks related to your business.

Column A: List of factorsIdentify all the risk factors that apply to your business (including, products, services and delivery channels, geography, new developments and technologies, foreign and domestic affiliates and other relevant factors)	Column B: Risk ratingAssess each risk factor (for example, low, medium or high).	Column C:RationaleExplain why you assigned a particular risk rating to each risk factor.
- High turnover within your business of employees who deal directly with clients.	High-risk	New employees may have less knowledge of certain clients and less experience with ML/TF indicators.
- Proximity to border crossings	High-risk	Your business may be the first point of entry into the local financial system.

Relationship-based risk assessment Once you complete your business-based risk assessment, you can focus on the last element of your risk assessment, which consists of your clients and the business relationships you have with them.

When you enter into a business relationship with a client, you have to keep a record of the purpose and intended nature of the business relationship.Footnote 14 You also have to review this information on a periodic basis, which will help you determine the risk of ML/TF and understand the patterns and transactional activity of your clients.Footnote 15 It is possible that your business deals with clients outside of business relationships. The interactions with these clients may be sporadic (for example, few transactions over time that are under the identification threshold requirement). As such, there will not be a lot of information available to assess these clients. The risk assessment of such clients may focus on the transactional or contextual information at your disposal, rather than on a detailed client file.

If you do not have business relationships, it is not necessary for you to complete a relationship-based risk assessment worksheet for low and medium risk clients. However, if you have high-risk clients outside of business relationships, you should include them in a relationship-based risk assessment. For example, clients that were included in a suspicious transaction report (STR) you submitted to FINTRAC.

To conduct a relationship-based risk assessment, you need to identify the in-

herent risks of ML/TF for your clients. You can assess the ML/TF risks for individual clients or for groups of clients with similar characteristics. Your overall relationship-based risk assessment includes the risk posed by the following:

1. The combination of products, services and delivery channels your client uses;
2. The geographical location of the client and their transactions;
3. The new developments and technologies you make available to your clients; and
4. Client characteristics and patterns of activity or transactions.

1. Products, services and delivery channels In the relationship-based risk assessment, you are looking at the products, services and delivery channels that your clients are using and the impact they have on your clients' overall risk.

Product risks:

Products will have a higher inherent risk when there is client anonymity or when the source of funds is unknown.

Where possible, it is advisable that you complete a review of such products with the employees who handle them to ensure the completeness of the risk assessment.

Service risks:

You should include in your risk assessment services that have been identified as potentially posing a high-risk by government authorities or other credible sources.

For example, potentially higher risk services could include: international electronic funds transfers (EFTs), international correspondent banking services, international private banking services, services involving banknote and precious metal trading and delivery, or front money accounts for casinos.

Delivery channel risks:

You should consider delivery channels as part of your risk assessment, given the potential impact of new developments and technologies.

Delivery channels that allow for non-face-to-face transactions pose a higher inherent risk. Many delivery channels do not bring the client into direct face-to-face contact with you (for example, internet, telephone or new products such as virtual currency, chat applications, online document signing, etc.) and are accessible 24 hours a day, 7 days a week, from almost anywhere. This can be used to obscure the true identity of a client or beneficial owner, and therefore poses a higher risk. Although some delivery channels may have become the norm (for example, the use of internet for banking), you should nonetheless consider them

in combination with other factors that could make a specific element, client or group of clients high-risk.

Some products, services and delivery channels inherently pose a higher risk. See Annex 5 — Table 9: Relationship-based examples of higher risk indicators and considerations for products, services and delivery channels.

2. Geography In the business-based risk assessment, you have identified high-risk elements related to the geographical location of your business. In the relationship-based risk assessment, you will look at the geography of your clients or business relationships and its impact on their overall risk.

Your business faces increased ML/TF risks when you receive funds from or destined to high-risk jurisdictions, and when a client has a material connection to a high-risk country. You should assess the risks associated with your clients and business relationships such as residency in a high-risk jurisdiction or transactions with those jurisdictions.

See Annex 5 — Table 10: Relationship-based examples of higher risk indicators and considerations for geography.

3. Impacts of new developments and technologies In the business-based risk assessment, you assessed potential high-risk elements related to the introduction of new developments and technologies in your business model, prior to implementing them. In the relationship-based risk assessment, you will examine the potential impacts that new developments (putting in place a new service/activity/location) and technologies (introducing a new technology) could have on your clients, affiliates, and anyone with whom you have a business relationship.

New developments and technologies can increase risk, as they may provide another layer of anonymity. For example, your business faces an increased risk of ML/TF when funds come from or are destined to high-risk jurisdictions, and when the origin of the funds can not be determined or is unknown, etc.

See Annex 5 — Table 11: Relationship-based examples of higher risk indicators and considerations for new developments and technologies.

4. Client characteristics and patterns of activity or transactions At the beginning of a business relationship, and periodically throughout the relationship, you should consider the purpose and intended nature of the relationship. Doing so will help you understand your clients' activities and transaction patterns, in order to determine their level of ML/TF risk. Your policies and procedures must reflect this process.

To help you with the overall risk assessment of a client or group of clients, you should also consider known risk factors that can **increase** a client's overall ML/TF risk rating, such as:

- criminal history of the client in regards to a designated offence.
- unknown source of funds;
- beneficiary of the transaction is unknown;
- individual conducting the transaction in unknown;
- absence of detail in the transaction records;
- unusual speed, volume and frequency of transactions; or
- unexplained complexity of accounts or transactions.

Similarly, you should also look at factors that can **decrease** a client's ML/TF risk, such as:

- a low volume of activity;
- a low aggregate balance;
- low dollar value transactions; or
- household expense accounts or accounts for the investments of funds that are subject to a regulatory scheme (for example, Registered Retirement Savings Plan).

Some client characteristics or patterns of activity will pose an inherently higher risk of ML/TF. For examples of:

- higher risk client characteristics and patterns of activity, see Annex 5 — Table 12: Relationship-based examples of higher risk indicators and rationale for client characteristics and patterns of activity;
- client characteristics that can be considered higher risk, see FINTRAC's ML/TF indicators; and
- additional higher risk indicators and rationale, see Annex 5 — Table 13: Relationship-based examples of additional higher risk indicators and related considerations.

Scoring your relationship-based risk assessment You can assess the ML/TF risk for individual clients or for groups of clients. This assessment could take the form clusters (or groups) of clients with similar characteristics. For example, you can group together clients with similar incomes, occupations and portfolios, or those who conduct similar types of transactions. This approach can be especially practical for financial institutions.

It is important to remember that identifying one high-risk indicator for a client does not necessarily mean that the client poses a high-risk (with the exception of the three indicators highlighted in Table 12). Your relationship-based risk assessment model ultimately **draws together** the products, services and delivery channels used by your client, your client's geographical risk and your client's characteristics and patterns of activity. It is up to you to determine how to best assess the risk each client or group of clients poses.

Every high-risk client (or group of clients) will need to be subjected to prescribed special measures (see step 3). You will have to document these measures in your policies and procedures, and document how you apply them to

your high-risk clients.Footnote 16

You can use a Likelihood and impact matrix like the one in Annex 4 to help you evaluate your relationship-based risk.

Relationship-based risk assessment worksheet Using a relationship-based risk assessment worksheet could be an easy way to document the inherent risks related to your clients and your business relationships with them. The worksheet below is given an example. You can also develop your own worksheet or method to document the inherent risks related to your clients.

Column A Business relationships and/or high-risk clientsIdentify all your business relationships and/or high-risk clients (individually or as groups).	Column B: Risk ratingRate each business relationship and/or client (or group of clients) (for example, low, medium or high risk).	Column C: RationaleExplain why you assigned that particular rating to each business relationship and/or client (or group of clients).
- Group A / Client A	Low-risk	Known group or client conducting standard transactions in line with their profile.
- Group B / Client B	High-risk	Conducts several large cash transactions that seem to be beyond their means.

RBA cycle — Step 2: Setting your risk tolerance

Risk tolerance is an important component of effective risk management. Consider your risk tolerance before deciding how you will address risks. When considering threats, the concept of risk tolerance will allow you to determine the level of risk exposure that you consider tolerable.

To do so, you may want to consider the following types of risk which can affect your organization:

- regulatory risk;
- reputational risk;
- legal risk; or
- financial risk.

The PCMLTFA and associated Regulations state that reporting entities have obligations when they identify high-risk business activities and high-risk clients. Setting a high risk tolerance does not allow reporting entities to avoid these obligations.

To set your risk tolerance, some questions that you may want to answer are:

- Are you willing to accept regulatory, reputational, legal or financial risks?
- Which risks are you willing to accept after implementing mitigation measures?
- Which risks are you not willing to accept?

This should help you determine your overall risk tolerance (notwithstanding your mandatory obligations).

RBA cycle — Step 3: Creating risk-reduction measures and key controls

Risk mitigation is the implementation of controls to manage the ML/TF risks you have identified while conducting your risk assessment. It includes:

1. **In all situations,** your business should consider implementing internal controls that will help mitigate your overall risk.
2. **For your business-based risk assessment,** you will have to document and mitigate all the high-risk elements identified by your assessment with controls or measures.Footnote 17
3. **For all your clients and business relationships**, you will be required to:Footnote 18
    1. Conduct ongoing monitoring of all your business relationships; and
    2. Keep a record of the measures and information obtained through this monitoring.
4. **For your high-risk clients and business relationships**, you will be required to adopt the prescribed special measures, including:Footnote 19
    1. Conducting **enhanced** monitoring of these clients and business relationships.
    2. Taking enhanced measures to verify their identity and/or keep client information up to date.

Implementing risk mitigation measures will allow your business to stay within your risk tolerance. It is important to note that having a higher risk tolerance may lead to your business accepting higher risk situations and/or clients. If you accept to do business in higher risk situations and/or with higher risk clients, you should have stronger mitigation measures and controls in place to adequately address the risks.

For **detailed** information on risk mitigation measures, please consult FINTRAC's Compliance program requirements guidance.

RBA cycle — Step 4: Evaluating your residual risks

Your residual risks should be in line with your risk tolerance. It is important to note that no matter how robust your risk mitigation measures and risk management program is, your business will always have exposure to some residual ML/TF risk that you must manage. If your residual risk is greater than your

risk tolerance, or your measures and controls do not sufficiently mitigate high-risk situations or high-risk posed by clients, you should go back to step 3 and review the mitigation measures that were put in place.

If your business is willing to deal with high-risk situations and/or clients, FINTRAC expects that the mitigation measures or controls put in place (see step 3) will be commensurate with the level of risk, and that the residual risks will be reasonable and acceptable.

Types of residual risk:

- **Tolerated risks:** These are risks that you accept because there is no benefit in trying to reduce them. Tolerated risks may increase over time. For example, when you introduce a new product or a new threat appears.
- **Mitigated risks:** These are risks that you have reduced but not eliminated. In practice, the controls put in place may fail from time to time (for example, you do not report a transaction within the prescribed timeframe because your transaction review process has failed).

This is an example of a business further mitigating risk because over time their risks and clients have evolved:

Business A offers international EFTs as a service to its clients. Reporting systems are in place to capture transactions of $10,000 or more, and Business A has developed policies and procedures to properly verify identity for transactions of $1,000 or more. A reporting system is also in place to identify transactions that could be related to an ML/TF offence (for suspicious transaction reporting purposes).

Since Business A considers international EFTs to be a high-risk service, it added a mitigation measure to control the risk associated with the service. The staff (through the training program) is reminded regularly of the risks associated with international EFTs and are made aware of updates and changes to high-risk jurisdictions as indicated in government advisories. These measures were put in place by Business A years ago and are well understood and followed by the staff.

In this example, the mitigation measures put in place at the time were in line with the risk tolerance of Business A in regards to international EFTs. As such, the residual risk was tolerable for Business A.

However, as risks and/or clients changed over time, Business A now feels that the mitigation measures are no longer sufficient to meet its risk tolerance. In fact, Business A's risk tolerance is now lower than it used to be (that is, it is less inclined to take on high-risks). The residual risks from the previously established mitigation measures now exceed the new risk tolerance.

Business A will add new mitigation measures to realign the residual risk with its new tolerance level. Some examples of additional mitigation measures are:

- put a limit on specific transactions (for example, international EFTs to specific jurisdictions);
- require additional internal approvals for certain transactions; and/or
- monitor some transactions more frequently to help reduce the risk of structuring (for example, a $12,000 transaction that is split into two $6,000 transactions to avoid reporting).

RBA cycle — Step 5: Implementing your RBA

You will implement your RBA as part of your day-to-day activities.

You must document your risk assessment as part of your compliance program.Footnote 20 A detailed and well-documented compliance program shows your commitment to preventing, detecting and addressing your organization's ML/TF risks.

Risk and risk mitigation requires the leadership and engagement of your senior management (should this apply to your business). Senior management or your business owner is ultimately accountable, and may be responsible for making decisions related to policies, procedures and processes that mitigate and control ML/TF risks.

For more information, please consult FINTRAC's Compliance program requirements guidance.

RBA cycle — Step 6: Reviewing your RBA

You must institute and document a periodic review (minimum of every two years) of your compliance program, to test its effectiveness, which includes reviewing:Footnote 21

- your policies and procedures;
- your risk assessment related to ML/TF; and
- your training program (for employees and senior management).

If your business model changes and you offer new products or services, you should update your risk assessment along with your policies and procedures, mitigating measures and controls, as appropriate.

When reviewing your risk assessment to test its effectiveness, you must cover all components, including your policies and procedures on risk assessment, risk mitigation strategies and special measures which include your enhanced ongoing monitoring procedures. This will help you evaluate the need to modify existing policies and procedures or to implement new ones. Consequently, the completion of this step is crucial to the implementation of an effective RBA.

For more information, please consult FINTRAC's Compliance program requirements guidance.

Annex 1 — FINTRAC's RBA expectations

Overall expectations

There is no standard risk assessment methodology. In building a new or validating an existing risk assessment, you may find this guidance useful to inform your risk assessment. However, you should not limit yourself to the information provided in this guidance when developing your own RBA.

The expectations below are at a high level. FINTRAC's risk assessment expectations for each step of the RBA cycle are described further in this annex.

- Your risk assessment must be documented and should:
  - reflect the reality of your business;
  - include all prescribed elements (products, services and delivery channels, geography, new developments and technologies, affiliates if applicable, and any other factors relevant to your business); and
  - be shared with FINTRAC during an examination upon request.
- You need to tailor your risk assessment to your business size and type. For example, FINTRAC would expect a more detailed assessment from REs that conduct large volumes of transactions across various business lines and/or products. Additionally, FINTRAC would expect the overall business-based risk rating for larger REs to have separate risk ratings for different lines of business.
- You need to document all steps of your risk assessment, the process you followed, and the rationale that supports your risk assessment.
- During an examination, FINTRAC may review:
  - your risk assessment, your controls and mitigating measures (including your policies and procedures) to assess the overall effectiveness of your risk assessment;
  - your business relationships and evaluate whether they have been assessed based on the products, services, delivery channels, geographical risk, impact of new developments and technologies and other characteristics or patterns of activities;
  - your high-risk client files to ensure that the prescribed special measures have been applied;
  - your records to assess whether monitoring and reporting are done in accordance with the PCMLTFA and associated Regulations and with your policies and procedures; and
  - whether your prescribed review (to be conducted at least once every two years) appropriately assessed the effectiveness of your business and relationship-based risk assessment.

Expectations for Step 1 — Identification of your inherent risks

FINTRAC expects that:

- You have considered and assessed your business risks (including, prod-

ucts, services and delivery channels, geography, new developments and technologies, affiliates if applicable, and any other factors relevant to your business) and you are able to provide a rationale for your assessment. For every element that you assess as posing a high-risk, you will need to document the controls and mitigation measures you are taking. You need to be able to show that these controls and measures have been implemented.

- You have considered and assessed your clients and business relationships based on the products, services and delivery channels they use, on their geography, and on their characteristics and patterns of activity. You can do this by:
  - Demonstrating that you have assessed the risks posed by each client you have a business relationship with; or
  - Assessing groups of clients or of business relationships that share similar characteristics, as long as you can demonstrate that the groupings are logical and specific enough to reflect the reality of your business.
- You can provide documented information that demonstrates that you have considered high-risk indicators in your assessment (such as those included in this guidance where applicable).
- In situations where high-risk indicators are not considered (for example, FINTRAC considers a specific element to pose a high-risk but you decide that the element poses a lower level of risk), you must be able to provide a reasonable rationale.
- For every high-risk relationship, you have put in place the prescribed special measures and document these measures in your policies and procedures.
- If you use a checklist for your risk assessment, you must be able to provide a documented analysis of the risk that draws conclusions on your business's vulnerabilities to ML/TF and the threats it faces, including the required elements (referred to above).
- If your business is using a service provider to perform the risk assessment, you are nonetheless ultimately responsible to ensure that the for the risk assessment obligation is met correctly.

Expectations for Step 2 — Set your risk tolerance

FINTRAC expects that:

- You take time to establish your risk tolerance, as it is an important component of effectively assessing and managing your risks.
- Your risk tolerance will have a direct impact on creating risk-reduction measures and controls, on your policies and procedures, and on training (step 3).

Setting your risk tolerance includes obtaining approval from senior management (should that be a part of your business structure).

Expectations for Step 3 — Create risk-reduction measures and key controls

FINTRAC expects that:

- You keep the client identification and beneficial ownership information of your business relationships up to date.Footnote 22
- You establish and conduct the appropriate level of ongoing monitoring for your business relationships (taking enhanced measures for high-risk clients).Footnote 23
- You implement mitigation measures for situations where the risk of ML/TF is high (for your business-based risks and relationship-based risks). These written mitigation strategies must be included in your policies and procedures.

Apply your controls and procedures consistently. FINTRAC may assess them through transaction testing.

Expectations for Step 4 — Evaluate your residual risks

FINTRAC expects that:

- You take the time to evaluate your level of residual risk.
- You confirm that the level of residual risk is aligned with your risk tolerance (as described in step 2).

Expectations for Step 5 — Implement your RBA

FINTRAC expects that:

- Your RBA process is documented, and includes your ongoing monitoring procedures (including their frequency) and the measures and controls put in place to mitigate the high-risks identified in step 1.
- You apply your RBA as described in your documentation.
- You keep the client and beneficial ownership information of your business relationships up to date.Footnote 24
- You conduct ongoing monitoring of all your business relationships.Footnote 25
- You apply the appropriate prescribed special measures to your high-risk clients and business relationships.Footnote 26
- You involve the persons responsible for compliance when dealing with high-risk situations (for example, when dealing with foreign politically exposed persons (PEPs), obtain senior management approval to keep accounts open after a determination has been made).

Expectations for Step 6 — Review your RBA

FINTRAC expects that:

- You conduct a review at least every two years, or when there are changes to your business model, when you acquire a new portfolio, etc.Footnote 27
- This prescribed review will test the effectiveness of your entire compliance program, including your compliance policies and procedures, your risk assessment of ML/TF risks and your ongoing training program.Footnote 28
- You document the review and report it to senior management within 30 days.Footnote 29
- You document the results of the review, along with corrective measures and follow-up actions.Footnote 30

Annex 2 — Examples of higher risk indicators and considerations for your business-based risk assessment

Examples of higher risk indicators	Considerations
Higher risk products and services, such as:- EFTs, - electronic cash (for example, stored value cards and payroll cards) - letters of credit- bank drafts- front money accounts- products offered through the use of intermediaries or agents- private banking - mobile applications	Legitimate products and services can be used to mask the illegitimate origins of funds, to move funds to finance terrorist acts or to hide the true identity of the owner or beneficiary of the product or service. You should assess the market for your products and services (for example, corporations, individuals, working professionals, wholesale or retail etc.), as this may have an impact on the risk.Do the products or services you provide allow your clients to conduct business or transactions with higher risk business segments? Could your clients use the products or services on behalf of third parties? Products and services offered that are based on new developments and technologies such as electronic wallets, mobile payments, or virtual currencies, may be considered higher risk as they can transmit funds quickly and anonymously.

Examples of higher risk indicators	Considerations
Delivery channels, such as transactions for which an individual is **not physically present**, including- agent network - online trading	Your delivery channels may have a higher inherent risk if you offer non face-to-face transactions, use agents, or if clients can initiate a business relationship online. This is especially true if you rely on an agent (that may or may not be covered by the PCMLTFA) to verify the identity of your clients.For the purpose of the PCMLTFA, REs are accountable for the activities conducted by their agents.In addition, new delivery channels (for example, products or services such as virtual currency) may pose inherently higher ML/TF risks due to the anonymous nature of transactions when conducted remotely.

Table 1: Business-based examples of higher risk indicators and considerations for products, services and delivery channels

Examples of higher risk indicators	Considerations
Border-crossings:- air (for example, airports)- water (for example, ports, marinas)- land (for example, land border-crossings)- rail (for example, passenger and cargo)	If your business is near a border-crossing, you may have a higher inherent risk because your business may be the first point of entry into the Canadian financial system.This does not mean that you should assess all activities and clients as posing a high-risk if your business is located near a border-crossing or major airport. FINTRAC is simply highlighting that such businesses may want to pay closer attention to the fact that their geographical location may impact their business. For example, this could be done through training so that staff better understand the placement stage of ML and its potential impacts.

Examples of higher risk indicators	Considerations
Geographical location and demographics:- large city- rural area	Your geographical location may also affect your overall business risks. For example, a rural area where you know your clients could present a lesser risk compared to a large city where new clients and anonymity are more likely. However, the known presence of organized crime would obviously have the reverse effect. Some provincial governments have interactive maps on crime by regions, which may inform your risk assessment. Other websites provide good information on crime in Canada, including statistics and trends by province. For example, crimes, by type of violation, and by province and territory:http://www.statcan.gc.ca/tables-tableaux/sum-som/l01/cst01/legal50b-eng.htm.

Examples of higher risk indicators	Considerations
Your business is located in an area known for having a high crime rate	High crime rate areas should be indicated in the overall assessment of your business as they may present higher ML/TF risks.You do not need to consider every client from a higher crime area as posing a high-risk. However, you should be aware of how these areas can affect client activities. Searching online for crime related statistics in your city or area should result insources you can consult (such as municipal police departments or other databases). For example, the following websites provide information on crime in cities or neighborhoods: - Vancouver: http://vancouver.ca/police/organization/planning-research-audit/neighbourhood-statistics.html- Edmonton: http://crimemapping.edmontonpolice.ca/- Calgary: http://www.calgary.ca/cps/Pages/Statistics/Calgary-Police-statistical-reports.aspx#- Winnipeg: https://winnipeg.ca/police/crimestat/viewMap.aspx- Toronto: http://www.torontopolice.on.ca/statistics/stats.php- Ottawa: https://www.ottawapolice.ca/en/crime/crime-stats.aspx- Montreal: https://ville.montreal.qc.ca/vuesurlasecuritepublique/ (in French only) - Halifax: https://www.halifax.ca/fire-police/police/crime-mappingPlease note that statistics such as those found under the links above are not necessarily linked to ML/TF offences. They provide a general idea of where crime occurs in a given city.

Examples of higher risk indicators	Considerations
Events and patterns	Depending on your clientele, are there events or patterns (either domestic or international) that could affect your business? For example, you may be dealing with clients that have a connection to high-risk jurisdictions or with jurisdictions that are dealing with a specific event (such as terrorism, war, etc.). You do not need to classify all activities and clients as posing a high-risk in relation to an event, conflict or high-risk jurisdiction. However, you should be aware of these circumstances in order to determine whether a transaction becomes unusual or suspicious.

Examples of higher risk indicators	Considerations
Connection to high-risk countries:- Special Economic Measures Act (SEMA)- FATF list of High-Risk Countries and Non-Cooperative Jurisdictions- UN Security Council Resolutions- Freezing Assets of Corrupt Foreign Officials Act (FACFOA) sanctions	International conventions and standards may affect mitigation measures aimed at the detection and deterrence of ML/TF. You should identify certain countries as posing a high-risk for ML/TF based on (among other things) their level of corruption, the prevalence of crime in their region, the weaknesses of their ML/TF control regime, or the fact that they are listed in the advisories of competent authorities such as the FATF or FINTRAC. If you and/or your clients have no connection to these countries, the risk will likely be low or non-existent.If you transfer funds to or receive funds from a country subject to economic sanctions, embargoes or other measures, you should consider that country as high-risk. For example, you should be aware of: - Canadian Economic Sanctions: https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/index.aspx?lang=eng- High-Risk and Non-Cooperative Jurisdictions: http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/- FINTRAC Advisories: https://fintrac-canafe.canada.ca/new-neuf/1-eng- Security Council Resolutions: https://www.un.org/securitycouncil/content/resolutions- Freezing Assets of Corrupt Foreign Officials Act sanctions: https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/current-actuelles.aspx?lang=eng

Table 2: Business-based examples of higher risk indicators and considerations

for geography

Examples of higher risk indicators	Considerations
Use of technology, such as:- Payment methods: - E-wallets in fiat currencies (CAD, USD, etc.) - E-wallets in virtual currencies - pre-paid cards - internet payment services - mobile payments - money transfers between individuals over mobile devices and the Internet- Methods of communication or identification: - phone - email - chat applications - electronic information exchange - document signing on a cloud server such as DocuSign	Your overall inherent risks may be higher if your business adopts new technologies or operates in an environment subject to frequent technological change. New technologies may include systems or software used in your organizations ML/TF mitigation strategy such as a transaction monitoring system or a client onboarding or identification tool.The implementation of new technologies such as mobile payment services could subject your business to a wide range of vulnerabilities that can be exploited for ML. For example, the use of new technologies can result in less face-to-face interaction with customers, allowing more anonymity and possibly increasing ML/TF risks. Therefore, when you implement new technology in your business, it is important that you assess the associated ML/TF risks and document and implement appropriate controls to mitigate those risks. **Payment methods**The payment method examples listed in the Indicators column can be used to transfer funds faster and anonymously, which can increase ML/TF risks.If your business offers such products, services and delivery channels, you must assess them for ML/TF risks to your business.**Methods of communication or identification**Your business may communicate with clients through means other than the telephone and email or your clients may use new ways to communicate with you or identify themselves to you. Communications means are evolving continually and can affect your overall inherent risks.

Examples of higher risk indicators	Considerations
New developments	Consider acquisitions, changes to your business model, or business restructuring.

Table 3: Business-based examples of higher risk indicators and considerations for new developments and technologies

Examples of higher risk indicators	Considerations
Business model of foreign affiliate: - operational structure- reputational risk	Review the business model, size, number of employees and the products and services of your affiliates to determine whether they represent a risk that can affect your business. For example: - If a business has hundreds of branches and thousands of employees, it poses different risks than a business with a single location and two employees.- If the media negatively mentions one of your affiliates, your reputation could also be affected given the connection between you and that affiliate.

Table 4: Business-based examples of higher risk indicators and considerations for foreign and domestic affiliates

Examples of higher risk indicators	Considerations
- Special Economic Measures Act (SEMA)- ministerial directives- regulators- national risk assessment	Restrictions such as economic sanctions can impact your business by:- prohibiting trade and other economic activity with a foreign market;- restricting financial transactions such as foreign investments or acquisitions; or- leading to the seizure of property situated in Canada. These restrictions may apply to dealings with entire countries, regions, non-state actors (such as terrorist organizations), or designated persons from a target country.As part of your risk assessment, you must also take into consideration ministerial directives.Your sector's regulator may also impose additional measures (for example, provincial, prudential, etc.).The national risk assessment assesses the ML/TF risks in Canada, which may help you identify potential links to your own business activities.
Trends, typologies and potential threats of ML/TF:- ML/TF methods used in specific sectors- ML/TF actors including organized crime groups, terrorist organizations, facilitators, etc.- corruption and other crimes	Trends and typologies for your respective activity sector may include specific elements of risks that your business should consider. For example:- FATF Methods and Trends (not available for all activity sectors): http://www.fatf-gafi.org/topics/methodsandtrends/. - Public Safety Canada — Organized Crime: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cmbtng-rgnzd-crm/index-en.aspx- Transparency International (rank by country): https://www.transparency.org/en/countries/canadaNot all elements listed in these trends and typologies will affect you, but you should be aware of the high-risk indicators that may have an impact on your business.

Examples of higher risk indicators	Considerations
Business model: - operational structure- third party and/or service providers	To determine if risks exist in relation to this element, you need to consider your business model, the size of your business, and the number of branches and employees. For example: - A business with hundreds of branches and thousands of employees will present different risks than a business that has one location and two employees.- A business with a high employee turnover. These examples highlight the fact that your risk assessment should be related to other compliance program elements, such as training. Training should give employees an understanding of the reporting, client identification, and record keeping requirements, and an understanding of the penalties for not meeting those requirements. If you have numerous branches or a high employee turnover, your training program should address these risks.It is also important to remember that although the use of a third party or service provider can be a good business practice, your business is ultimately responsible for complying with your obligations under the PCMLTFA and associated Regulations. You will want to ensure that you fully understand how your third party or service provider is functioning.

Table 5: Business-based examples of higher risk indicators and considerations for other relevant factors

Annex 3 — Examples of risk segregation for your business-based risk assessment

The table below lists examples of risk factors you could encounter **as part of your business-based risk assessment**. It also provides a rationale on how you could differentiate between risk ratings.

Please note that:

1. The PCMLTFA and associated Regulations do not require you to use a low, medium and high scale. You could use low and high-risk categories only. You must establish a risk scale and you must tailor the risk scale to your business's size and type.
2. Utilizing a table similar to this one **is not** in itself a risk assessment, as it does not meet the requirement as stated in the Regulations. However, the table below is an example of a business-based risk assessment. It does not consider your clients or business relationships.

This list includes **inherent risks** that have not been mitigated yet. By law, controls or mitigation measures are required for all high-risk factors.

Factors	Low	Medium	High
Products & services — Electronic transactions	No electronic transaction services	You have some electronic transaction services and offer limited products and services	You offer a wide array of electronic transactions services
Products & services — Currency transactions	Few or no large transactions	Medium volume of large transactions	Significant volume of large or structured transactions
Products & services — EFTs	Limited number of funds and transfers of low value for clients and non-clientsLimited third party transactions and no foreign funds transfers	Regular funds transfers and transfers of medium valueFew international funds transfers from personal or business accounts with typically low-risk countries	Frequent funds transfers and transfers of high value from personal or business accounts, to or from high-risk jurisdictions and financial secrecy jurisdictions

Factors	Low	Medium	High
Products & services (business model) — International exposure	Few international accounts or very low volume of transactions in international accounts	Some international accounts with unexplained transactions	High number of international accounts with unexplained transactions
Geography (location) — Prevalence of crime	All locations are in an area known to have a low crime rate	One or a few locations are in an area known to have an average crime rate	One or a few locations are in an area known to have a high crime rate and/or criminal organization(s)
Technology	No new technologies are used to conduct the business in terms of products and services to clientsNo new technologies are used to contact clients	Certain areas of the business use new technologies to contact clients but products, services and payment methods do not use new technologies	The majority of products, services, delivery channels, payment methods and client contact methods use new technologies.

Table 6: Examples of risk segregation for a business-based risk assessment

Note: Some of the descriptors in the above table are vague (such as "some", "significant", etc.). A table such as this one needs to be customized to the reality of your business. For example, if FINTRAC states that it considers a "significant volume of transactions with high-risk countries" as posing a high-risk, this could mean that a business could compare the transactions to high-risk countries to the overall quantity of transactions conducted by their business. If a business conducting 600 transactions with high-risk-countries out of 1,000 monthly transactions it has a "significant" inherent risk. Qualifiers depend on the specifics of your own business.

Annex 4 — Likelihood and impact matrix

You can use the likelihood and impact matrix described below for your business and client risks. It can help you determine the level of effort or monitoring required for inherent risks. You use the matrix or develop your own to better reflect the realities of your business.

Likelihood is the chance of an ML/TF risk is present. What is the likelihood that the identified risks are actually present? The "likelihood" is the level of risk you have identified as part of your business-based risk assessment and/or your relationship-based risk assessment (for example, a client assessed as posing a medium risk). You can use a scale similar to this one:

Rating	Likelihood of ML/TF risk
High	High probability that the risk is present
Medium	Reasonable probability that the risk is present
Low	Unlikely that the risk is present

Table 7: Rating and likelihood of the ML/TF risk

Impact isthe damage incurred if ML/TF occurs. Depending on business circumstances, the impact could be a financial loss, or a regulatory, legal, reputational or other impact. To help you determine the impact of your ML/TF risks, you can use a scale similar to this one:

Rating	Likelihood of ML/TF risk
High	The risk has severe consequences
Medium	The risk has moderate consequences
Low	The risk has minor or no consequences

Table 8: Rating and impact of the ML/TF risk

You can use the matrix to help you decide which actions to take considering the overall risk. Each box in the matrix shows the level of resources required for:

- action (the need to respond to the risk)
- effort (level of effort required to mitigate the risk)
- monitoring (level of monitoring required)

Diagram 4: Likelihood and impact matrix

!Likelihood and impact matrix.jpg)

View Text Equivelant

The following graphic is called the likelihood and impact matrix. It is made up of 2 axes. The vertical axis is the likelihood of ML/TF risk while the horizontal axis is the impact of ML/TF. Each axis contains 3 levels of risk – low, medium and high - for a total of 9 boxes within the matrix.

On the impact axis, the left side represents the low risk category, the middle being medium risk and the right side representing high risk. On the vertical

axis, the bottom represents the low risk category, the middle being medium risk and the top representing high risk.

The 9 boxes within the matrix represent various combinations of risk. In addition, each box contains a level of resource required for: action (i.e. the need to respond to risk), effort (i.e. level of effort required to mitigate the risk) and monitoring (i.e. level of monitoring required). The level of resource is being represented by level 0, being the lowest, up to level 3 being the highest.

1. The box on the lower left corner (low impact and low likelihood) represents the lowest overall risk. Action is at level 0 while effort and monitoring are at level 1.
2. The box immediately to its right (medium impact and low likelihood) is also considered to be in the lower overall risk. Action is at level 0 while effort and monitoring are at level 1.
3. The box on the bottom right corner (high impact and low likelihood) represents a medium / low overall risk. Action and effort are at level 1 while monitoring is at level 2.
4. The box located at low impact and medium likelihood is considered to be in the lower overall risk. Action is at level 0 while effort and monitoring are at level 1.
5. The box immediately to its right, at the centre of the matrix (medium impact and medium likelihood), is considered to be medium overall risk. Action, effort and monitoring are at level 2.
6. The box located at high impact and medium likelihood is considered to be in the higher overall risk. Action, effort and monitoring are at level 3.
7. The box on the top left corner (low impact and high likelihood) represents a medium / low overall risk. Action and effort are at level 1 while monitoring is at level 2.
8. The box immediately to its right (medium impact and high likelihood), is considered to be in the higher overall risk. Action, effort and monitoring are at level 3.
9. The box on the top right corner (high impact and high likelihood) represents the highest overall risk. Action, effort and monitoring are at level 3.

How to read the matrix

Box 6 may not require any response, effort or monitoring because you consider both the likelihood and impact to be low.

Box 3 will require you to allocate resources for action, effort and monitoring. You will want to monitor all business risks and business relationships that are in box 3 to ensure that the risks identified do not move into the red categories (boxes 1 and 2).

In Box 1, you have identified the risks to be highly likely to occur and to have a severe impact on your business. Anything in this box (for example, business

risks, business relationship, etc.) would require the most resources for action, effort, and monitoring.

Examples

For the example below, you should consider all risk factors or clients as:

- low-risk if situated in boxes 5–6;
- medium-risk if situated in boxes 3–4; and
- high-risk if situated in boxes 1–2.

Example 1 You complete the risk assessment of clients A and B and determine that they both have the same likelihood of ML/TF risk: medium.

Taking a closer look at their accounts, you realize that both have EFTs on file (product/service with a high inherent risk). However, client A has not conducted an EFT in months and you know that the EFTs were to family members abroad. However, client B regularly conducts EFTs but you do not know a lot about the recipients or the reasons for the EFTs.

As such, you could assess the impact of the ML/TF risk to be greater with client B than with client A. You could decide to leave client A in the medium impact category (placing the client in box 3) and to move client B to the high-impact category (placing the client in box 2). You should document your decision and rationale.

In this example, you would need to implement mitigation measures for client B, who is now a high-risk client.

Example 2 After completing the risk assessment of clients A and B, you determine that they have the same likelihood of ML/TF risk: high.

Taking a closer look at the volume of transactions both clients conduct, you see that client A conducts 1 transaction per week on average; whereas client B conducts several transactions every day. In this example, the impact not submitting suspicious transaction reports would be greater with client B because of the volume of transactions.

You could decide to place client A in a lower category (placing the client in box 4) while client B could remain in a higher category (placing the client in box 1 or 2). You should document your decision and rationale

In this example, you would implement mitigation measures for client B, who is now a high-risk client.

Example 3 In this scenario, an RE applies the risk matrix to risk elements identified in their risk assessment:

Risk factor	Likelihood	Impact	Overall	Mitigation measures
Clients always use cash as method of payment	High	Medium	**High (box 2)**	- Perform enhanced ongoing monitoring of transactions or business relationships.- Obtain additional information beyond the minimum requirements about the intended nature and purpose of the business relationship, including the type of business activity.

Risk factor	Likelihood	Impact	Overall	Mitigation measures
Clients frequently use EFTs for no apparent reason	Medium	High	**High (box 2)**	- Set transaction limits for high-risk products such as EFTs to high-risk jurisdictions.- Obtain additional information beyond the minimum requirements for the intended nature and purpose of the business relationship, including type of business activity.- Implement a process to end existing high-risk relationships that exceed your risk tolerance level.

Diagram 5 — Example of a risk matrix

Annex 5 — Examples of higher risk indicators and considerations for your relationship-based risk assessment

Examples of higher risk indicators	Considerations
Your clients use electronic funds payment services such as: - EFTs - electronic cash	EFTs can be done in a non-face-to-face environment. Additionally, transmitting large amounts of funds outside of Canada or into Canada can disguise the origin of the funds.**Electronic cash** is a higher risk service because it can allow unidentified parties to conduct transactions.
Your clients use products such as bank drafts and letters of credit.	**Bank drafts** can move large amounts of funds in bearer form without the bulkiness of cash. They are much like cash in the sense that the holder of the draft is the owner of the money. For example, a 100,000 dollar bank draft (showing a financial institution as the payee) and can be passed from one person to another, effectively blurring the money trail.You can mitigate the inherent risk of this product when it is issued as payable only to specific payees and when the information about the draft's originator are included (name, account number, etc.). **Letters of credit** are essentially a guarantee from a bank that a seller will receive payment for goods. While guaranteed by a bank, letters of credit have a higher inherent ML/TF risk as they can be used in trade-based transactions to increase the appearance of legitimacy and reduce the risk of detection. Money launderers using trade-based transactions (for example, seller or importer) may also use under or over valuation schemes, which will allow them to move money under the veil of legitimacy.There is also higher risk when letters of credit are not used in a way consistent with the usual pattern of activity of the client.

Examples of higher risk indicators	Considerations
Your clients use some products and services that you offer through non-face-to-face channels or use intermediaries, agents or introducers (refer clients or businesses to you for specific products or services).	Non-face-to-face transactions can make it more difficult to verify the identity of your clients.Using intermediaries or agents may increase your inherent risks, because intermediaries or agents may lack adequate supervision if they are not subject to anti-money laundering and anti-terrorist financing (AML/ATF) laws or measures. It is important to note that under the PCMLTFA, you are accountable for the activities conducted by all your agents. As a result, you need to ensure that they meet all compliance obligations on an ongoing basis. Furthermore, you should have due diligence processes in place (such as background checks and ongoing monitoring) to lessen the risk of your agent network being used for ML/TF purposes.

Table 9: Relationship-based examples of higher risk indicators and considerations for products, service and delivery channels

Examples of higher risk indicators	Considerations
Your client's proximity to a branch or location	A client that conducts business or transactions away from their home branch or address without reasonable explanation. For example, one of your clients conducts transactions at different branches across a broad geographical area over one day and this does not appear to be practical.
Your client is a non-resident	Identifying non-resident clients may prove to be more difficult if they are not present and as such, could raise the inherent level of risk.

Examples of higher risk indicators	Considerations
Your client has offshore business activities or interests	Is there a legitimate reason for your client to have offshore interests? Offshore activities may be used by a person to add a layer of complexity to transactions, thus raising the overall risk of ML/TF.
Your client's connection to high-risk countries	Take your client's connection to high-risk countries into account as some countries have weaker or inadequate AML/ATF standards, insufficient regulatory supervision or present a greater risk for crime, corruption or TF.

Table 10: Relationship-based examples of higher risk indicators and considerations for geography

Examples of higher risk indicators	Considerations
Changing payment methods	The variety of payment methods made possible by advancements in technology is a potential risk for ML/TF. Many countries and companies have moved to a "cashless world" approach. As a result, clients are using alternative payment methods such as e-wallets. It is important to analyze the risk associated with these payment methods (for example, anonymity, borderless transactions, speed of the transactions, vulnerabilities in terms of know your client requirements) to determine how the technology used by your clients may increase their risk level.
A new service or activity that offers transaction anonymity	It is important to assess the impact that a new service or activity can have on the behaviour of your clients who may use it to distance themselves from a transaction.

Table 11: Relationship-based examples of higher risk indicators and considera-

tions for new developments and technologies

Examples of higher risk indicators	Rationale
Your client is in possession or control of property that you **know/believe** is owned or controlled by or on behalf of a terrorist or a terrorist group	You are required to send a terrorist property report to FINTRAC if you have property in your possession or control that you **know/believe** is owned or controlled by or on behalf of a terrorist or a terrorist group. This includes information about transactions or proposed transactions relating to that property. Once you file a terrorist property report, the client automatically becomes high-risk.
Your client is a foreign PEP	A foreign PEP is an individual who is or has been entrusted with a prominent function. Because of their position and the influence they may hold, a foreign PEP, their family members and their close associates are vulnerable to ML/TF and other offences such as corruption. As a business, you **must** consider a foreign PEP, their family members and their close associates as a high-risk client.

Examples of higher risk indicators	Rationale
The entity has a complex structure that conceals the identity of beneficial owners	When you cannot obtain or confirm the ownership and control information of a corporation or an entity, you are required to verify the identity of the most senior managing officer of the entity and treat the entity as high-risk, and apply the prescribed special measures as stated in the Proceeds of Crime Money Laundering and Terrorist Financing Regulations.For more information, please consult FINTRAC's Beneficial ownership requirements guidance.It is important to note that when you do have the information on beneficial ownership, there may be other information or indicators that would make this relationship pose a higher risk.

Table 12: Relationship-based examples of higher risk indicators and rationale for client characteristics and patterns of activity

Examples of higher risk indicators	Considerations
STR was previously filed or considered	Suspicious transactions (or attempted transactions) are financial transactions for which you have reasonable grounds to suspect they are related to the commission or attempted commission of an **ML/TF offence**. For more information about STRs and ML/TF indicators, see FINTRAC's STR guidance.Clients that are the conductors of suspicious transactions that have been reported should be assessed as posing a higher risk.
Transactions involving third parties	Transactions involving third parties may indicate high-risk when the link between the third party and the client is not obvious.

Examples of higher risk indicators	Considerations
The account activity does not match the client profile	Account activity that does not match the client profile may indicate a higher risk of ML/TF.You may face situations where you have submitted several large cash transaction reports to FINTRAC about a client with an occupation that does not match this type of activity (for example, student, unemployed, etc.).
Your client's business generates cash for transactions not normally cash intensive	The fact that there is no legitimate reason for the business to generate cash represents a higher risk of ML/TF.
Your client's business is a cash-intensive business (such as a bar, a club, etc.)	Certain types of business, especially those that are cash-intensive may have a higher inherent risk for ML/TF because legitimate money can be co-mingled with illegitimate money. For example, clients that own white label ATMs.
Your client offers online gambling	Industry intelligence, including reports from the Royal Canadian Mounted Police, indicates that due to the nature of the business, the gambling sector is susceptible to ML activity. Additionally, the FATF has indicated that internet payment systems are an emerging risk in the gambling industry. Internet payment systems are used to conduct transactions related to online gambling, these two factors make the online gambling industry inherently higher risk.As well, higher inherent risk may exist if the online gambling activities are not managed by provincial lottery and gaming corporations.

Examples of higher risk indicators	Considerations
Your client's business structure (or transactions) seems unusually or unnecessarily complex	An unnecessarily complex business structure or complex client transactions (compared to what you normally see in a similar circumstance) may indicate that the client is trying to hide transactions or suspicious activities.
Your client is a financial institution with which you have a correspondent banking relationship; **or**Your client is a correspondent bank that has been subject to sanctions.	Some countries have weaker or inadequate AML/ATF standards, insufficient regulatory supervision or simply present a greater risk for crime, corruption or TF. Additionally, the nature of the businesses that your correspondent bank client engages in and the type of markets it serves may present greater risks. The fact that your client has been subject to sanctions should raise the risk level and you should put appropriate measures in place to monitor the account.
Your client is an RE under the PCMLTFA that is not otherwise regulated	Some reporting entities that are not federally or provincially regulated (other than under the PCMLTFA) may present higher risks of ML/TF. In addition, some may have cash intensive businesses that can also increase the overall risks of ML/TF.
Your client is an intermediary or a gatekeeper (such as a lawyer or accountant) holding accounts for others unknown to you	Accountants, lawyers and other professionals sometimes hold co-mingled funds accounts for which beneficial ownership may be difficult to verify. This does not mean that all clients with these occupations are high-risk. You need to be aware of the risks that exist for these occupations and determine if the activities of the clients are in line with what you would expect and with the intended purpose of the account (for example a personal, business or trust account).

Examples of higher risk indicators	Considerations
Your client is an unregistered charity	Individuals and organizations can misuse charities in ML schemes or to finance or support terrorist activity. It is important to be aware of the risks in relation to charities and to apply due diligence by confirming if a charity is registered with the Canada Revenue Agency
Domestic PEPs and heads of international organizations (HIOs)	Corruption is the misuse of public power for private benefit. Internationally, as well as in Canada, it is important to understand that the possibility for corruption exists and that domestic PEPs or HIOs can be vulnerable to carrying out or being used for ML/TF offences.Once you have determined that a person is a domestic PEP, a HIO or a family member or close associate of them, you must determine if the person poses a higher risk for committing an ML/TF offence. If you assess the risk to be high, then you must treat the person as a high-risk client.For more information, please consult the PEP and HIO guidance for your sector (if applicable).

Table 13: Relationship-based examples of additional higher risk indicators and related considerations# Compliance program requirements : FINTRAC's compliance guidance

From: Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)

This guidance explains the compliance program requirements under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (the Act) and associated Regulations that **apply to all reporting entities**.

1. What is a compliance program and what are its requirements

A compliance program is established and implemented by a reporting entity that is intended to ensure its compliance with the Proceeds of Crime (Money

Laundering) and Terrorist Financing Act (the Act) and associated Regulations. A compliance program forms the basis for meeting all of your reporting, record keeping, client identification and other know-your-client requirements under the Act and associated Regulations. All reporting entities must establish and implement a compliance program.

Specifically, all reporting entities must implement the following elements of a compliance program:

- appoint a compliance officer who is responsible for implementing the program
- develop and apply written compliance policies and procedures that are kept up to date and, in the case of an entity, are approved by a senior officer
- conduct a risk assessment of your business to assess and document the risk of a money laundering or terrorist activity financing offence occurring in the course of your activities
- develop and maintain a written, ongoing compliance training program for your employees, agents or mandataries, or other authorized persons
- institute and document a plan for the ongoing compliance training program and deliver the training (training plan)
- institute and document a plan for a review of the compliance program for the purpose of testing its effectiveness, and carry out this review every two years at a minimum (two-year effectiveness review)

2. Who can be a compliance officer and what are their responsibilities

Depending on the size of your business, you could be the appointed compliance officer, or it could be another individual, such as:

- a senior manager, the owner or the operator of your small business, or
- someone from a senior level who has direct access to senior management and the board of directors of your large business

If you are a person rather than an entity, such as a sole proprietor, you can appoint yourself as the compliance officer, or you may choose to appoint someone else to help you implement the compliance program.

As a best practice, the appointed compliance officer of a larger business should not be directly involved in the receipt, transfer or payment of funds. The appointed compliance officer should also have independent oversight and be able to communicate directly with those parties who make decisions about the business such as senior management or the board of directors.

Appointing someone to be your compliance officer alone does not fulfil your compliance program requirements. The appointed compliance officer is responsible for implementing all elements of a compliance program. Therefore, a compliance officer needs to:

- have the necessary authority and access to resources in order to implement an effective compliance program and make any desired changes
- have knowledge of your business's functions and structure
- have knowledge of your business sector's money laundering, terrorist activity financing and sanctions evasion risks and vulnerabilities as well as money laundering, terrorist activity financing and sanctions evasion trends and typologies
- understand your business sector's requirements under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (the Act) and associated Regulations

A compliance officer may delegate certain duties to other employees. For example, the compliance officer of a large business may delegate responsibility to an individual in another office or branch. However, the compliance officer remains responsible for the implementation of the compliance program.

While the compliance officer is appointed, it is the reporting entity's responsibility to meet its compliance program requirements under the Act and associated Regulations.

3. Compliance policies and procedures requirements

Your compliance policies and procedures must be:

- written and should be in a form or format that is accessible to its intended audience
- kept up to date (including changes to legislation or your internal processes, as well as any other changes that would require an update)
- approved by a senior officer, if you are an entity

Your policies and procedures should be made available to all those authorized to act on your behalf, including employees, agents and any others that deal with clients, transactions, or other activities.

Your compliance policies and procedures should cover at minimum the following requirements as applicable to you as a reporting entity:

- **compliance program**: this includes your requirements to have an appointed compliance officer, a risk assessment, an ongoing compliance training program and plan, and a two-year effectiveness review and plan, which consists of a review of your policies and procedures, risk assessment, and ongoing training program and plan
- **know your client**: this includes your requirements for verifying client identity, politically exposed persons, heads of international organizations, their family members and close associates, beneficial ownership, and third party determination
- **business relationship and ongoing monitoring**
- **record keeping**
- **Transaction reporting**

- **travel rule** requirements: this includes your requirement to develop and apply written risk-based policies and procedures to help determine whether you should suspend or reject an electronic funds transfer or virtual currency transfer that you receive, and any other follow-up measures, if the transfer does not include the required travel rule information and you are unable to obtain this information through your reasonable measures
- **Ministerial directive** requirements

Your compliance policies and procedures should also include the processes and controls you have put in place to meet your requirements, including:

- when the obligation is triggered
- the information that must be reported, recorded, or considered
- the procedures you created to ensure that you fulfill a requirement
- the timelines associated with your requirements and methods of reporting (if applicable)

Your policies and procedures must also describe the steps you will take for all the obligations that require you to take reasonable measures. For example, when you are required to take reasonable measures to obtain information to include in a report, your policies and procedures must describe the steps you will take, which could include asking the client.

If your reporting entity sector has an industry association or governing body that has provided you with a generic set of policies and procedures, you must tailor them to your business.

The level of detail in your compliance policies and procedures will depend on your business's size, structure, and complexity, and degree of exposure to money laundering, terrorist activity financing and sanctions evasion risks.

4. Risk assessment requirements

Your compliance program must include policies and procedures that you develop and apply to assess your money laundering, terrorist activity financing and sanctions evasion risks in the course of your activities. When assessing and documenting your money laundering, terrorist activity financing and sanctions evasion risks, you must consider the following:

- your clients, business relationships, and correspondent banking relationships including their activity patterns and geographic locations
- the products, services and delivery channels you offer
- the geographic location(s) where you conduct your activities
- if you are a **financial entity**, **life insurance company**, or **securities dealer**, the risks resulting from the activities of an **affiliate,** if it is also subject to the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and associated Regulations under these reporting entity sectors, or if it is a foreign affiliate that carries out activities outside Canada that are similar to these sectors

- the risks resulting from new developments or new technologies you intend to carry out or introduce, before doing so, that may have an impact on your clients, business relationships, products, services or delivery channels, or the geographic location of your activities
- the applicable risks for your reporting entity sector, detailed in the latest National Risk Assessment of Money Laundering and Terrorist Financing in Canada
- any other relevant factors affecting your business (for example, employee turnover, industry rules and regulations)

If, at any time, you consider the risk of a money laundering or terrorist activity financing offence to be high, you must take enhanced measures.

5. Enhanced measures

Enhanced measures are the additional controls and processes that you have put in place to manage and reduce the risks associated with your high-risk clients and business areas. As part of your compliance program, you must develop and apply written policies and procedures for the enhanced measures that you will take for any money laundering, terrorist activity financing or sanctions evasion risks you identify as high.

Your policies and procedures for enhanced measures must include:

- the additional steps, based on assessment of the risk, that you will take to verify the identity of a person or entity
- any other additional steps that you will take to mitigate the risks, including, but not limited to, the additional steps to:
  - ensure client identification information and beneficial ownership information is updated at a frequency that is appropriate to the level of risk
  - conduct ongoing monitoring of business relationships at a frequency that is appropriate to the level of risk

Enhanced measures to mitigate risk can include:

- obtaining additional information on a client (for example, information from public databases and the internet)
- obtaining information on the client's source of funds or source of wealth
- obtaining information on the reasons for attempted or conducted transactions, or
- any other measures you deem appropriate

6. Training program and plan requirements

If you have employees, agents or mandataries, or other persons authorized to act on your behalf, you must develop and maintain a written, ongoing compliance training program. Your training program should explain what your employees,

agents or mandataries, or other persons authorized to act on your behalf, need to know and understand, including:

- your requirements under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (the Act) and associated Regulations
- background information on money laundering and terrorist activity financing, such as the definition of money laundering and terrorist activity financing, and methods of money laundering and terrorist activity financing
- how your business or profession could be vulnerable to money laundering and terrorist activity financing activities (provide indicators and examples)
- the compliance policies and procedures you have developed to help meet your requirements under the Act and associated Regulations for preventing and detecting money laundering and terrorist activity financing, including your reporting, record keeping and know your client requirements
- their roles and responsibilities in detecting and deterring money laundering and terrorist activity financing activities, and when dealing with potentially suspicious activities or transactions

You must institute and document a plan for your ongoing compliance training program and for delivering the training. Your training plan should cover how you will implement your ongoing compliance training program and its delivery.

This includes documenting the steps you will take to ensure your employees, agents or mandataries, or other persons authorized to act on your behalf receive an appropriate level of training relevant to their duties and position, on an ongoing basis.

Your training plan should include information on:

- training recipients
- training topics and materials
- training methods for delivery
- training frequency

Training recipients

Your training plan should explain who will receive training. Training recipients should include those who:

- have contact with clients, such as front-line staff or agents
- are involved in client transaction activities
- handle cash, funds, or virtual currency for you, in any way, and
- are responsible for implementing or overseeing the compliance program, such as the compliance officer, senior management, information technology staff or internal auditors

Training topics and material

Your training plan should outline the topics that will be covered in your training program. It should also include the sources of the training materials that will cover these topics.

Training methods for delivery

Your training plan should describe the training method(s) that you will use to deliver your ongoing compliance training program.

Training methods could include:

- self-directed learning (where recipients read materials on their own, register for on-line courses or use e-learning materials)
- information sessions
- face-to-face meetings
- classroom
- conferences, and
- on-the-job training where instruction is provided

Instructors can be in-house personnel or an external service provider, but they should have knowledge of the Act and associated Regulations. If you decide to use in-house personnel, you may need to hire or allocate staff to provide training.

If you decide to use an external service provider, you may need to determine whether their services and training content are suitable for your business. You can use 1 or more training methods. The method(s) that you choose may depend on the size of your business and the number of people that need to be trained.

Training frequency

Your training plan should describe the frequency of your training program. Training can be delivered at regular intervals (for example, monthly, semi-annually, annually), when certain events occur (for example, before a new employee deals with clients, after a procedure is changed), or by using a combination of both.

Your training program and plan should be tailored to your business's size, structure and complexity, and its degree of exposure to money laundering, terrorist activity financing and sanctions evasion risk. For example, if you are a large business, you may decide to provide different types of training to your employees, agents or mandataries, or other persons authorized to act on your behalf based on their specific roles and duties (for example, general or specialized training). This should be explained in your training plan.

Your training program should also include a record of the training that has been delivered (for example, the date the training took place, a list of the attendees who received the training, the topics that were covered). Training

records will help you keep track of the training and assist you in scheduling the next training dates. They will also demonstrate that you are carrying out your training program on an ongoing basis.

Note: If you are a sole proprietor with no employees, agents or other individuals authorized to act on your behalf, you are not required to have a training program nor are you required to have a training plan in place for yourself.

7. Two-year effectiveness review and plan requirements

A two-year effectiveness review is an evaluation that must be conducted every 2 years (at a minimum) to test the effectiveness of the elements of your compliance program (policies and procedures, risk assessment, and ongoing training program and plan). You must start your effectiveness review no later than 2 years (24 months) from the start of your previous review. You must also ensure that you have completed your previous review before you start the next review.

The purpose of an effectiveness review is to determine whether your compliance program has gaps or weaknesses that may prevent your business from effectively detecting and preventing money laundering, terrorist activity financing and sanctions evasion.

Your effectiveness review will help you determine if:

- your business practices reflect what is written in your compliance program documentation and if you are meeting your requirements under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (the Act) and associated Regulations
- your risk assessment is effective at identifying and mitigating the money laundering, terrorist activity financing and sanctions evasion risks related to your clients, affiliates (if any), products, services, delivery channels, new developments or technology, and geographic locations where you do business

The review must be carried out and the results documented by an internal or external auditor, or by yourself if you do not have an auditor. Your review should be conducted by someone who is knowledgeable of your requirements under the Act and associated Regulations. Also, as a best practice, to ensure that your review is impartial, it should not be conducted by someone who is directly involved in your compliance program activities. Regardless of who carries out the review, as a reporting entity it is your responsibility to ensure that the review is conducted (at a minimum) every 2 years and that the review tests the effectiveness of your compliance program.

You must also institute and document a plan for the two-year effectiveness review of your compliance program. This plan should describe the scope of the review and must include all the elements of your compliance program. The breadth and depth of review for each element may vary depending on factors such as:

- the complexity of your business
- transaction volumes
- findings from previous reviews
- current money laundering, terrorist activity financing and sanctions evasion risks.

Your plan should not only describe the scope of the review, but it should include the rationale that supports the areas of focus, the time period that will be reviewed, the anticipated evaluation methods and sample sizes.

The evaluation methods can include, but are not limited to, interviewing staff, sampling records and reviewing documentation. The following are examples of what can be included in your review:

- interviews with those handling transactions to evaluate their knowledge of your policies and procedures and related record keeping, client identification and reporting requirements
- a review of a sample of your records to assess whether your client identification policies and procedures are being followed
- a review of your agreements with agents or mandataries, as applicable, as well as a review of a sample of the information that your agents or mandataries referred to in order to verify the identity of persons, to assess whether client identification policies and procedures are being followed
- a review of transactions to assess whether suspicious transactions were reported to FINTRAC
- a review of large cash transactions to assess whether they were reported to FINTRAC with accurate information and within the prescribed timelines
- a review of electronic funds transfers to assess whether reportable transfers were reported to FINTRAC with accurate information and within the prescribed timelines (applicable to reporting entity sectors that have electronic funds transfer obligations)
- a review of a sample of your client records to see whether the risk assessment was applied in accordance with your risk assessment process
- a review of a sample of your client records to see whether the frequency of your ongoing monitoring is adequate and carried out in accordance with the client's risk level assessment
- a review of a sample of high-risk client records to confirm that enhanced mitigation measures were taken
- a review of a sample of your records to confirm that proper record keeping procedures are being followed
- a review of your risk assessment to confirm that it reflects your current operations
- a review of your policies and procedures to ensure that they are up to date and reflect the current legislative requirements and that they reflect your current business practices

You should also document the following in your two-year effectiveness review:

- the date the review was conducted, the period that was covered by the review and the person or entity who performed the review
- the results of the tests that were performed
- the conclusions, including deficiencies, recommendations and action plans, if any

If you are an entity, you must report, in writing, the following to a senior officer no later than 30 days after the completion of the effectiveness review:

- the findings of the review (for example, deficiencies, recommendations, action plans)
- any updates made to the policies and procedures during the reporting period (the period covered by the two-year review) that were not made as a result of the review itself
- the status of the implementation of the updates made to your policies and procedures# FINTRAC assessment manual: The approach and methods used during examinations

From: Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)

Introduction

Why is the manual important and what does it cover?

The Financial Transactions and Reports Analysis Centre of Canada, known as FINTRAC, is committed to helping you meet the legal requirements set out in the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and associated Regulations.

Our objective is to support businesses as we work together to protect Canadians and the integrity of Canada's financial system from money laundering and terrorist activity financing vulnerabilities.

To this end, in the spirit of openness and transparency, we have published this assessment manual detailing how we conduct examinations.

Examinations are one of the main activities we use to assess whether businesses are adequately implementing and maintaining a compliance program, which is important to detecting and mitigating the money laundering and terrorist activity financing risks your business may face. In turn, it can also reduce financial, reputational and legal risks should criminals try to exploit your business's vulnerabilities.

The manual does not replace the PCMLTFA and associated Regulations, establish new legal requirements or expectations, serve as regulatory guidance, or tell you how to carry out your day-to-day business operations.

The manual, which is for all Canadian businesses covered by the PCMLTFA, describes how FINTRAC conducts its compliance examinations. It is meant to

help you understand how we assess whether you have implemented and maintained a compliance program that adequately meets all of the legal requirements, and to help you prepare for a FINTRAC examination.

The manual is divided into three parts:

1. Part 1—the framework we apply to ensure that we conduct our examinations in a consistent manner;
2. Part 2—the phases of an examination; and
3. Part 3—the methods we use in examinations to assess whether you are adequately meeting the legal requirements.

Canadian businesses covered under the Act:

- Accountants
- British Columbia notaries
- Casinos
- Dealers in precious metals and stones
- Financial entities
- Life insurance
- Money services businesses
- Real estate
- Securities dealers

While our examinations take into account the differences across business sectors, our overall examination approach and methods remain the same for all.

The assessment methods we may use in an examination are not limited to those described in the manual. The manual is an evergreen document that we will update through consultations with businesses as our assessment methods evolve, or as legislative and regulatory changes are introduced.

The manual represents FINTRAC's examination approach and methods. It does not address how other federal or provincial regulators or supervisors carry out their oversight activities relating to compliance with anti-money laundering and anti-terrorist activity financing requirements.

Note: FINTRAC typically refers to the businesses covered by the PCMLTFA as reporting entities, while the PCMLTFA refers to "persons" and "entities". In this manual, the term "businesses" will be used.

Part 1—Examination framework

The examination framework we use ensures that we conduct our examinations in a consistent manner, while taking into account the type, nature, size, and complexity of different businesses.

The framework is comprised of three main components outlined below.

Risk-based examinations

We focus our examinations on areas where your business may be vulnerable to money laundering or terrorist activity financing risks and where there is a greater risk of not meeting the legal requirements (risk of non-compliance). Using this approach reduces the burden on businesses by minimizing disruptions and ensuring the effective and efficient use of resources.

When determining the risks your business may be exposed to, we rely on our experience, knowledge, training, and professional judgment. We take into account relevant information from FINTRAC publications and guidance. We may also take into consideration relevant information taken from publicly available reports and publications issued by well-known credible sources on money laundering and terrorist activity financing.

We recognize that businesses will adopt different approaches to implementing and maintaining their compliance programs, based on their type, nature, size, complexity and risk profile. In light of this, we will include in our examination plans the areas you have identified as posing a higher risk to your business as well as gaps you have identified in your compliance program, where appropriate.

Part 2 of the manual describes in more detail how risk informs our examinations.

Assessment methods

Once we have evaluated your business's risks, we select assessment methods described in Part 3 that we will use as part of our examination.

We use the methods to assess how you comply with the legal requirements set out in the PCMLTFA and associated Regulations. We also consider FINTRAC guidance, which sets out how we interpret the legal requirements.

For example, the PCMLTFA requires that Suspicious Transaction Reports be submitted to FINTRAC under certain circumstances. FINTRAC guidance presents money laundering and terrorist activity financing indicators to help businesses better understand typical risks they may be exposed to, and should watch for, in their day-to-day activities. When we assess the requirement to report suspicious transactions using the methods described in the manual, we may refer to the indicators we provide in the guidance, in addition to the obligation in the PCMLTFA, to support the rationale for suspicion.

When applying our assessment methods, we may review your documents, client records, records of transactions, and financial transaction reports, as well as conduct interviews.

Assessment approach to evaluating findings

We take an assessment approach when evaluating examination findings. This means that we take a holistic approach when evaluating findings rather than evaluating them in isolation. We focus less on technical non-compliance and

more on the overall soundness of the areas of your compliance program we are assessing.

We look at all the information gathered to ensure that your compliance program is complete and put into practice. When we identify technical non-compliance within an otherwise adequate system of policies, procedures, processes, and controls, we will notify you of the non-compliance, but the overall result of our assessment may not be negatively affected by it.

With our findings, we aim to make decisions that are reasonable, fair, and balanced. We base our decisions on what we believe a reasonable, experienced and knowledgeable person in your business sector would have done if they were assessing the same set of facts and circumstances.

We expect you to provide us with, or make available, all relevant facts and information so that we can make decisions based on complete information.

Finally, in the spirit of transparency, openness, and fairness in our examinations, we will share our findings with you during the examination, explain them, and offer you the opportunity to provide us with additional information for our consideration.

Part 2—Examination phases

Examinations are conducted on weekdays, during FINTRAC's regular business hours (8 a.m. to 5 p.m.). If these hours do not suit your business, please notify us, as we may be able to offer some flexibility.

The number of days we will spend on your premises will depend on the type, nature, size, and complexity of your business. For example, the examination of a small or medium-sized business may take less than a week, while the examination of a bank may take several weeks.

In order to ensure the examination runs efficiently, and to reduce unnecessary business disruptions, it is important that you provide us with the requested information, documents, client records, records of transactions, and access to your staff, for interview purposes, in a timely manner.

Our examinations are broken down into three phases: planning and scoping; examination and assessment; and developing the findings and finalizing the examination. Below, we present each phase and describe the roles and responsibilities of each party to an examination.

Roles and responsibilities

You can expect us to be professional, provide clear information, respect your privacy and the confidentiality of your clients' personal and financial information, and offer services in either official language. You can also expect us to observe the highest standard of ethical conduct.

The PCMLTFA requires FINTRAC to protect the personal information under its control. We take this mandate very seriously and safeguard all personal information when we carry out an examination.

The PCMLTFA also requires that you provide FINTRAC with assistance during an examination. This assistance includes providing us with the information we ask for within the agreed upon timelines, giving us access to your place of business, providing us with the documents and records we request, answering our questions about your business and making employees available for interviews. We may also ask you to assist us in accessing information stored on your computers and systems, to help us better understand your operations.

Phase 1—Planning and scoping

Once we select a business for examination, we begin planning the examination, which includes selecting the areas and requirements we will examine (examination scope), as well as the assessment methods we will use.

Planning the examination We develop the overall plan to determine the staffing needs and level of expertise required to conduct the examination based on the type, nature, size, and complexity of the business to be examined.

Setting the scope of the examination When we set the scope of the examination, we choose the business areas and the specific requirements that we will examine.

To do this, we first gain a general understanding of your business model, environment, activities and operations. We then look at the risks your business may be exposed to, as well as the risks associated with your business sector. This includes determining:

1. your business areas at risk of being used for money laundering and terrorist activity financing; and
2. your business areas at risk of not meeting the legal requirements of the PCMLTFA and associated Regulations (the risk of non-compliance).

In order to gather this information and assess your risk, we may consult the files we have on your business and search the internet. For example, we may look at, as applicable:

- Your history of compliance with the PCMLTFA and associated Regulations;
- Findings from previous FINTRAC examinations or examinations conducted by a regulator or supervisor with whom FINTRAC has established a Memorandum of Understanding (MOU) to share information related to compliance with the PCMLTFA;
- Letters and emails you may have sent us describing how you will address previously found non-compliance;

- Voluntary self-declarations of non-compliance (VSDONC) in which you informed us that you have not met certain requirements;
- Previous questions you asked about the requirements or requests for policy interpretations to ensure that potential non-compliance has been addressed in a reasonable period following the enquiries (if applicable);
- Financial transaction reports you sent to FINTRAC;
- Actions taken when you received feedback from us about the quality, timing or volume of your financial transaction reports;
- Policies and procedures, risk assessments and two-year reviews and other documents and information that we may have on file from a previous examination;
- Information about your business or your clients available on the internet; and
- History of enforcement actions (administrative or criminal), in respect of your business, taken by FINTRAC, other regulatory/supervisory bodies, and law enforcement.

We use this information to assess risk and determine the scope of the examination, including the requirements we will assess and the appropriate assessment methods we will use. We also use a risk-based approach to establish the number of sample documents, client records, records of transactions, and financial transaction reports we plan to examine, the period covered by the examination, and who will be interviewed from your business.

When we have limited information on file regarding a business, we rely on the characteristics of similar businesses, and on the information obtained in our examination notification call to define the scope of the examination.

Desk versus on-site examinations We conduct examinations either remotely (a desk examination), or at your place of business (an on-site examination). You will be informed of the examination's location during our notification call and in the notification letter.

In either case, you must send all the requested information, documents and records to FINTRAC for a preliminary review.

When we conduct an examination remotely, we hold interviews with your compliance officer, employees, and agents (if applicable). When we conduct our examination at your place of business, we typically hold in-person interviews at your main location and may visit or call your other locations, if applicable, to conduct our interviews.

If you have multiple business locations, we typically ask that the information, documents, and records from all your locations be made available for our review at the location that has been selected for the examination.

Examination notification We will call the person responsible for the implementation of your compliance program (commonly referred to as the compliance

officer) to discuss an upcoming examination's scope and date.

After our notification call, we will confirm the examination details in writing with a notification letter addressed to your compliance officer. The letter will indicate where and when we will conduct the examination. We will usually send you the letter 30 to 45 days before the examination date. Given the amount of information and data involved, we may provide larger businesses with more than 45 days' notice to grant them sufficient time to gather the required information.

The letter is our formal request for information, documents and records, and for your assistance during the examination. We will ask you to send the requested material to FINTRAC, including, for example, your compliance program documents and when applicable, lists of transactions and records of transactions.

While we always encourage businesses to address non-compliance whenever they detect it, we will not generally accept certain documents, records, or financial transaction reports once an examination has started.

If you identify non-compliance after a FINTRAC examination has started, you should inform the FINTRAC officer immediately and send us a voluntary self-declaration of non-compliance. We consider the date on which we notify you of the examination to be the start of the examination (that is, the date of the notification call).

When we receive a voluntary self-declaration of non-compliance on an issue that was not previously voluntarily disclosed before a FINTRAC examination has started, we will not consider enforcement actions, such as an administrative monetary penalty. However, if we receive a self-declaration during an examination, we will assess the non-compliance as part of the examination, work with the business to correct it, and determine if the non-compliance warrants an enforcement action.

For example, if you did not submit a financial transaction report to FINTRAC when required and then submit it after the notification date, we will consider that you did not meet your requirement to submit the report. In addition, there may be situations where compliance program documents (for example, compliance policies and procedures) are created or adjusted after the notification date. In such cases, we may determine that you did not meet the compliance program requirements.

When we ask you to send us documents, client records and transaction records in advance of the examination, we do so to conduct the examination more efficiently and to minimize any disruption to your business during the on-site examination.

While we request most of the documents that we will need during the planning phase, we may request additional information or documents at a later stage of the examination process.

Given the sensitive nature of the documentation, and in the interest of limiting

the risk of loss during transit, we encourage you to provide the material electronically through a secure digital mailbox service. This type of service uses advanced encryption that allows for the transmission of sensitive information securely. If you agree to use this option, please contact FINTRAC for further information on the process.

Reviewing the material you send us We will review the material we requested in our notification letter, including your compliance program documents. This material is used to help us prepare interview questions. It may also further inform the scope of our examination. If the scope of the examination changes, we will notify you.

Phase 2—Examination and assessment

In this phase, we apply the assessment methods described in Part 3.

We start by conducting a preliminary assessment of the requirements that were part of the initial examination scope. We review your documents, conduct preliminarily interviews with your compliance officer, employees, or agents and review a sample of your transaction records and financial transaction reports. The objective of this preliminary assessment is to determine areas where we need to focus our attention.

If we identify areas or issues that require further attention, we will sample more client records, transaction records and reports, and if required, conduct follow-up interviews with your compliance officer, employees or agents. This may lead us to broaden the scope of the examination. If we need to adjust the scope of the examination, you will be notified.

This phase of the examination may extend beyond our last day on your premises or beyond the date of our videoconference or telephone interviews for desk examinations. This may be necessary if we need to further review and analyze certain documents, client records, transaction records, and reports before we consolidate our findings.

Conducting interviews We may interview different members of your staff and your agents. These one-on-one interviews may be in person, by telephone, or by videoconference.

We do our best to minimize undue business disruptions, particularly as they relate to front-line business functions. We also make every effort to make employees feel at ease.

We do not expect interviewees to memorize your business's policies and procedures or other documents. Rather, our goal is to confirm that your employees and agents are aware of the requirements applicable to their duties and know how to seek clarification when needed.

Exit meeting Even if we need to continue our review, once we are ready to leave your premises or have concluded the desk examination, we will hold an exit meeting in person, by telephone, or videoconference to discuss our preliminary findings with you. The findings are presented as "deficiencies". Each deficiency is a violation of a provision in the PCMLTFA or associated Regulations.

At this time, you may offer additional information to help clarify a deficiency. We will agree on a timeline for you to provide this material. After our review of this material, we may maintain our original deficiency, modify it, or withdraw it.

Phase 3—Developing conclusions and finalizing the examination

Deciding on our findings When we consolidate our findings, we use the assessment approach described in Part 1. Using this approach, we focus less on technical non-compliance and more on the overall soundness of the areas of your compliance program we are assessing. We evaluate findings holistically, rather than in isolation, to determine if you are adequately meeting the requirements.

As part of our evaluation, we consider the harm done by not meeting a requirement. In doing so, we assess the nature, relative importance, extent, the root cause of the non-compliance, and any mitigating or aggravating factors.

The nature of the non-compliance means which requirement (such as a compliance program or financial transaction reporting requirement) was not met.

We consider the relative importance of the requirement with which you were not compliant. While all requirements are important, and we expect businesses to fulfill them, certain requirements have a greater impact on FINTRAC's ability to carry out its mandate and on Canada's anti-money laundering and anti-terrorist financing regime. For example, the requirement to submit financial transaction reports could have a greater impact on FINTRAC's intelligence mandate and the regime as a whole than the requirement to submit reports that are free of minor data-quality issues.

We also assess the extent (degree) of the non-compliance; that is, how much information is missing from a required document, record or financial transaction report; how many times the non-compliance is repeated; and if the non-compliance points to gaps in the compliance program. We also try to identify the root cause of the non-compliance.

We look at all of the information we have gathered to ensure that your compliance program is complete and put into practice. When we identify technical non-compliance within an otherwise adequate system of policies, procedures, processes, and controls, we will make note of the non-compliance, but the overall results of our assessment may not be negatively affected by it.

Finally, we take into account other mitigating or aggravating factors that may influence how we view the non-compliance. Mitigating factors may decrease

the seriousness of the non-compliance, while aggravating factors may increase it. For example, a business may have submitted a Suspicious Transaction Report (STR), but omitted to send a Large Cash Transaction Report (LCTR) that was also required. If most of the LCTR's information is included in the STR, we may consider this a mitigating factor.

Examination findings letter We will send our examination findings letter to your compliance officer. This letter describes the findings that we discussed during the exit interview.

The letter will indicate the documents, client records, transaction records and financial transaction reports we have examined, as well as the consolidated results of our interviews with your employees and agent. When applicable, we will provide additional information, such as the number of documents we sampled and the number of instances of non-compliance that were found in the sample. The individual records and reports that we have found to be deficient will be listed in an annex to the letter.

In some cases, the letter may also include "observations". They are included to help you improve your business processes and practices in order to strengthen your compliance program.

The letter will also state which of the following three actions we may take following an examination based on the results of our assessment:

- no further compliance or enforcement action;
- possible follow-up compliance action; or
- a recommendation for an enforcement action, such as an administrative monetary penalty (AMP).

When you receive a findings letter, we expect you to address the causes of the identified deficiencies within a reasonable amount of time. In certain cases, we may ask you to send us an action plan that describes how and when the cause of the deficiencies will be addressed. When requested, an action plan must be sent within 30 calendar days of the receipt of the findings letter, unless otherwise specified. When an action plan is not requested, we still expect that you will take the time to address the cause of the deficiencies. Whether an action plan has been requested or not, you do not need to send us documents that demonstrate that the deficiencies have been addressed. We will evaluate these documents should we conduct a follow-up compliance activity.

If, on the basis of the examination findings, FINTRAC is considering issuing an administrative monetary penalty, this will be stated in the findings letter. The findings letter will also inform you how many days you have to send us any additional information, which is generally 30 calendar days, that you believe could influence our findings or our decision to issue an administrative monetary penalty. We will take into consideration additional relevant information you provide us within the established timeline and send you a written response of

our decision. In cases where any adjustment to the findings is required, our response will include a revised findings letter.

Follow-up activities After an examination, we may follow up to make sure that you have addressed the deficiencies we identified in our findings letter. We may:

- Conduct a follow-up on-site or desk examination;
- Monitor the reports you send to FINTRAC, if the examination revealed that the quality of your reports was inadequate or that the reports were late; and
- Monitor the progress of your action plan, if we asked you to provide one.

Penalties for non-compliance Our focus is on supporting businesses—administrative monetary penalties are not meant as an automatic response to non-compliance. If we decide to impose a penalty, our aim is to encourage a change in compliance behaviour. When deciding whether a penalty should be considered, FINTRAC compliance officers assess the harm done by looking at various factors. They will assess the nature, relative importance, extent, and root cause of the non-compliance, mitigating or aggravating factors, and a business's history of compliance. Generally speaking, penalties may be issued in cases of serious or repeated non-compliance. We will consider the unique factors in each case to determine if the examination should result in a penalty.

Should you receive a penalty, you have the right to make representations to FINTRAC's Director and Chief Executive Officer (CEO) for the review of your file. You also have the right to appeal the Director and CEO's decision to the Federal Court. Please visit our administrative monetary penalties page for more information.

We may disclose cases of non-compliance to law enforcement when there is extensive non-compliance or little expectation of immediate or future compliance, and where there are reasonable grounds to suspect that the information would be relevant to investigating or prosecuting an offence arising out of a contravention of Part 1 or Part 1.1 of the PCMLTFA (related to non-compliance). It is then up to law enforcement to conduct an investigation and decide whether further action is warranted. Please visit our penalties for non-compliance page for more information.

Part 3—Assessment methods

In Part 3, we describe the assessment methods that we use to ensure that you are adequately meeting the requirements.

We use the methods to assess how you comply with the legal requirements set out in the PCMLTFA and associated Regulations. We also consider FINTRAC guidance, which sets out how we interpret the legal requirements.

We assess the following requirements, unless exemptions apply:

- compliance program requirements;
- client identification and other know your client requirements;
- financial transactions reporting requirements;
- record keeping requirements;
- correspondent banking relationship requirements;
- foreign branches, foreign subsidiaries and affiliates requirements;
- registration of money services business and foreign money services business requirements; and
- ministerial directives' requirements.

We may not assess all of the requirements listed above during an examination, nor will we use every assessment method described in this section. Instead we will choose the requirements and the assessment methods that best fit our risk assessment of your business and the scope of the examination.

In the interest of efficiency, we may apply some of our assessment methods simultaneously, or use variations of the methods described in this section.

3.1. Compliance program requirements

This section describes the methods we use to assess whether you have adequately implemented and maintained a compliance program.

The five required elements of a compliance program are to:

- appoint a compliance officer;
- develop policies and procedures;
- conduct a risk assessment;
- develop and provide an ongoing compliance training program; and a plan for the delivery of the program; and
- develop a plan to conduct an effectiveness review of the compliance program, and carry it out every two years.

We will verify that you have a well-documented and complete compliance program in place, and assess whether your compliance program is put into practice.

To do so, we assess your compliance with other requirements, such as client identification and other know your client requirements, reporting requirements, and record keeping requirements. We may consider deficiencies identified through the assessment of these other requirements to be an indication that one or more of the five elements of your compliance program is not being applied.

3.1.1. Compliance officer—the person responsible for the implementation of the compliance program (Applicable to all business sectors)

We use the methods described in this section to assess your compliance with the requirement to appoint a compliance officer who is responsible for implementing your compliance program.

We verify that the following criteria have been adequately met:appointment (selection), authority, knowledge, and duties.

To conduct this assessment, we may:

- Review documents that show you have formally appointed a compliance officer. We may also review your compliance officer's job description, documents that describe their authority, and an organizational chart. We may also review your policies and procedures to confirm that they give your compliance officer enough guidance to meet the legal requirements.
  - Confirm that the compliance officer has direct access to senior management or the board of directors, to those who make important decisions about compliance issues or who control the company (where applicable).
  - Confirm that the compliance officer has timely access to information from all business lines to ensure they have knowledge of and are aware of potential compliance related risks or concerns (where applicable).
- Look at the compliance officer's background and experience, as well as the training you have given them to verify that you have made sure that the officer has enough knowledge of:
  - your business's functions and structure;
  - your sector's money laundering and terrorist activity financing risks and vulnerabilities, as well as related trends and typologies; and
  - your sector's requirements under the PCMLTFA and associated Regulations.

Our focus While we assess the appointment, authority, knowledge and duties of the compliance officer, our focus is on verifying that the compliance officer is fulfilling their duties to implement a sound compliance program. To make this determination, we assess whether the areas of your compliance program that we examined are adequately put into practice.

3.1.2. Policies and procedures (Applicable to all business sectors)

We use the methods described in this section to assess your compliance with the requirement to develop, document and apply policies and procedures.

We verify that your policies and procedures cover requirements such as (if applicable, and not meant to be exhaustive):

- compliance program, including special measures you take for high risk;
- client identification and other know your client requirements;
- financial transactions reporting;
- record keeping;
- correspondent banking relationships;
- foreign branches, foreign subsidiaries and affiliates;

- registration of money services businesses and foreign money services businesses;
- travel rule;
- reasonable measures; and
- ministerial directives.

We also verify that your policies and procedures include the processes and controls you have in place to implement your policies and meet your requirements. For example:

- The process you have in place and the source you use to convert foreign currency and virtual currency into Canadian dollars to meet your reporting, verifying identity and record keeping obligations when an exchange rate is not published by the Bank of Canada.
- The processes you have in place to take reasonable measures to obtain and report information.
- The process you have in place to establish reasonable grounds to suspect that transactions or attempted transactions may be related to money laundering or terrorist activity financing, and your process for submitting Suspicious Transaction Reports " as soon as practicable" and as a priority over other tasks.
- The process you have in place for electronic funds transfer and virtual currency transfers to meet your travel rule obligations. We will also review the process you follow when, after taking reasonable measures, you are unable to obtain the required information and the steps that you take to decide whether you allow, suspend or reject a transaction, and any follow-up measures you take.

We also verify that your policies and procedures are adequate, tailored to your business (that is, they take into account the type, nature, size, and complexity of your business) and are designed to control the risks you may face.

To conduct this assessment, we may:

- Review your policies and procedures to confirm that they are written, up to date and, if your business is an entity, approved by a senior officer.
- Review your policies and procedures to confirm that they provide enough guidance for your employees or agents.
- Interview your employees and agents to assess their knowledge of your policies and procedures.

Our focus While we assess your policies and procedures, we will focus on ensuring that you are adequately putting them into practice with respect to your obligations, including reporting, client identification, beneficial ownership, third party determination, politically exposed persons and heads of international organizations, ministerial directives, and special measures for high-risk client requirements, when required.

3.1.3. Risk assessment (Applicable to all business sectors)

We use the methods described in this section to assess your compliance with the requirement to assess and document your business risks and vulnerabilities related to money laundering and terrorist activity financing.

We verify that you have a documented risk assessment and that it includes the following elements, as applicable: products, services and delivery channels; clients and business relationships; geographic locations; new developments and new technologies; foreign and domestic affiliated entities (if applicable), and other prescribed high-risk elements such as persons or entities listed in ministerial directives.

We also verify that your risk assessment takes into account the type, nature, size, and complexity of your business, and we consider the rationale for each element of your business risk assessment.

To conduct this assessment, we may:

- Verify that you have assessed and documented the risks to your business related to money laundering and terrorist activity financing and that you have identified measures to mitigate these risks, and applied special measures for any high risks.
- Verify that you have assessed and documented risk using a risk-based approach before you implement a new development or introduce a new technology that may affect your clients, business relationships, products, services or delivery channels, or the geographic location of your activities. We may also review the process you follow before introducing new developments or new technologies.
- Verify that you have assessed risks adequately by looking at the areas you have identified as posing a high-risk and the assessment's written rationale. We may review a sample of client records and transaction records in order to determine whether your risk assessment is reasonable and consistent with your business's risk profile, and policies and procedures.
- Verify that you document and apply special measures to elements you have determined pose a high risk. Special measures include taking enhanced measures to identify clients and to mitigate risks such as keeping client identification information up to date and conducting ongoing monitoring for the purpose of detecting suspicious transactions, as well as any other enhanced measures you identify.
- Verify that the controls you have in place are consistent with your identified risk levels (ratings or rankings) and adequately mitigate your business risks.
- Verify that your compliance program is in line with and informed by the results of your risk assessment. For example, we will confirm that your policies and procedures, ongoing training documentation and two-year review documentation adequately address the areas you have assessed as posing a higher risk and that they provide adequate guidance to your

employees or agents.
- Verify how you use publicly available information to inform your compliance program.
- Interview the employees and agents responsible for your risk assessment to assess their knowledge of the requirements associated with conducting a risk assessment.

Our focus While we review the elements of your risk assessment, we will focus on verifying that you have considered and rated the risk of all aspects of your business, that you have provided rationales for your decisions, and that you have applied special measures to areas identified as posing a high risk.

3.1.4. Ongoing compliance training program and plan (Applicable to all business sectors)

We use the methods described in this section to assess your compliance with the requirement to develop and maintain a written, ongoing compliance training program for employees, agents, and those acting on your behalf. We will also assess your compliance with the requirement to have a documented plan to deliver your training program on an ongoing basis.

We look at who receives training, what topics are covered, when and how often training takes place, how you have implemented your training program, and how training is delivered.

We also verify that your training program is adequate, takes into account the size, type, nature and complexity of your business, and is put into practice.

To conduct this assessment, we may:

- Review your policies and procedures to confirm that they provide enough guidance to your employees, agents, and those acting on your behalf to develop, implement and maintain an ongoing training program.
- Review your training plan to confirm that it considers and documents the steps you take to develop, maintain, and deliver your training program.
- Review your training material to confirm that the training content is suitable. For example, we verify that it is tailored to your business and adequate for your employees, agents and their respective responsibilities.
- Interview your employees and agents to confirm that they understand the requirements as they relate to their positions, understand and follow the policies and procedures, understand how your business could be vulnerable to ML/TF activities, and have received adequate ongoing training.

Our focus While we assess your ongoing training program, we will focus on whether it helps your employees and agents understand the requirements, your policies and procedures, and indicators and trends of money laundering and terrorist activity financing. We will also pay close attention to the training you provide regarding the detection of suspicious transactions.

3.1.5. Two-year effectiveness review (Applicable to all business sectors)

We use the methods described in this section to assess your compliance with the requirement to institute and document a review of the compliance program to test its effectiveness.

We will verify that you have a documented plan to conduct a review of your policies and procedures, risk assessment, and training program for the purpose of testing their effectiveness, and that you carry out this plan to conduct a review every two years.

We will verify that your two-year effectiveness review is adequate, tailored to your business by taking into account the type, nature, size, and complexity of your business, and consistent with your risk assessment.

To conduct this assessment, we may:

- Review your documented plan to verify that it considers all the elements of your compliance program for the purpose of testing its effectiveness.
- Review your policies and procedures to determine whether they give enough guidance to your employees or agents to conduct a two-year effectiveness review.
- Look at the scope of the review (what the review covered) and methodology (how the review was conducted):
  - Interview the person who conducted the review to learn about its scope and methodology, and to ensure that they understand all the requirements that apply to your business;
  - When looking at the scope, for example, we assess whether your policies and procedures, risk assessment and ongoing compliance training program have been reviewed and cover the current legal requirements and your current operations. We also confirm that the review covers and tests all the requirements applicable to your sector; and
  - When looking at the methodology, for example, we verify whether the review was carried out by an internal or external auditor, or by you if you do not have an auditor; whether it was conducted within the required timelines; and whether the testing methods and methodology used were adequate and reasonable.
- Verify that a written report has been provided to a senior officer within 30 days after the completion of the review, and that the report includes the findings of the review, updates made to the policies and procedures within the reporting period of the review, and the status of the implementation of these updates.
- Verify that the findings of the review are being actioned.

Our focus We verify that your review assesses whether you have a well-documented compliance program and that your program is adequately put into practice. We will also focus on whether your review adequately identifies areas where you did not meet your requirements, whether you updated your policies and procedures, and the status of these updates.

3.2. Client identification and other know your client requirements

We use the methods described in this section to assess your compliance with client identification and other know your client requirements.

3.2.1. Client identification requirements (Applicable to all business sectors)

To conduct our assessment of your compliance with the verifying client identity requirements we may:

- Review your policies and procedures to confirm that they give enough guidance to your employees or agents to verify the identity of your clients.
- Review client records and transaction records to confirm that you apply these policies and procedures.
- Confirm, through a review of client records and transaction records, that you verify the identity of persons and entities in all situations where you are required to do so. These situations include, but are not limited to, when you:
  - open an account for a client, if applicable;
  - receive cash or virtual currency in the amount of $10,000 or more from, or on behalf of, the same person or entity within a 24-hour period;
  - must submit a Suspicious Transaction Report;
  - must create an information record; and
  - are unable to obtain or confirm beneficial ownership information and must therefore take reasonable measures to identify the most senior managing officer of the entity.
- Verify that you use the methods prescribed by law to verify the identity of a person or an entity and that you rely on valid and current information, or authentic, valid and current documents to do so.
- Confirm that you verify the identity of your clients within the prescribed timeframe.
- Interview your employees and agents to assess their knowledge of verifying client identity requirements.

If you use an agent, another reporting entity, or a foreign affiliated entity to help you verify the identity of clients, we may:

- Verify that you have a written agreement with the agent, reporting entity, or the foreign affiliate.

- Verify that you obtain all the required information from the agent, reporting entity, or the foreign affiliate as soon as feasible.
- Verify how you ensure that your agent, reporting entity, or foreign affiliate is using the identity verification methods required by law.

In addition, we verify that you document the required information when you verify the identity of a person or an entity. Refer to our record keeping guidance for more information on the requirement to keep records and to the section of this manual that describes the methods we use to assess record keeping.

When you have verified the identity of a client as required by the PCMLTFA and associated Regulations, you may have additional responsibilities related to know your client requirements. Refer to our know your client guidance and to the section of this manual that describes the methods we use to assess these requirements for more information.

Our focus We will focus on the steps you take to ensure that you verify the identity of a person or an entity.

3.2.2. Know your client requirements We use the methods described in this section to assess your compliance with the know your client requirements, including:

- Business relationships and ongoing monitoring requirements;
- Beneficial ownership requirements;
- Third party determination requirements; and **(based on specific activity)**
- Politically exposed persons and heads of international organizations requirements. **(Based on specific activity)**

To assess the requirements listed above, we may:

- Review your policies and procedures to confirm that they provide enough guidance for your employees or agents.
- Review your client records and transaction records to confirm that you put the policies and procedures into practice.
- Review records of transactions to confirm that you take the necessary steps for all the know your client requirements (as applicable) including:
  - taking all the measures as described in the know your client guidance;
  - obtaining the required approvals;
  - identifying your clients;
  - obtaining and keeping records of required information;
  - performing a risk assessment and ongoing monitoring;
  - taking special measures when required; and
  - meeting the requirements within the prescribed timeframes.
- Interview your employees and agents to assess their knowledge of the know your client requirements.

We use the methods listed below to evaluate your risk assessment practices relating to knowing your client.

Business relationships and ongoing monitoring To conduct this assessment, we may:

- Verify that you used the results of your risk assessment to determine how often you monitor your clients, or which transactions you will monitor more often or more closely. We focus on situations where you may not be adequately monitoring a client or transactions that you consider to pose a high-risk or to be suspicious.
- Verify that you monitor your high-risk business relationships more frequently to identify suspicious transactions, and apply special measures to mitigate risks.
- Review business relationships that you have ranked as posing a low or medium risk to determine whether this ranking is appropriate. We will compare your low-risk and medium-risk clients to your high-risk clients in light of the criteria you have established to identify high-risk situations.
- Review your ongoing monitoring of low and medium risk business relationships to ensure they are adequately monitored.
- Verify that you identify and address inconsistencies between a client's actual and expected transactional activity. Transactional activity inconsistency is a common indicator of money laundering and terrorist activity financing.

Beneficial ownership To conduct this assessment, we may:

- Verify that you have a process in place to obtain beneficial ownership information.
- Verify your records and the process you have in place to confirm the accuracy of the information obtained.
- Verify whether you take reasonable measures to identify the chief executive officer of an entity, or the person who performs that function, for which you are unable to obtain or confirm the beneficial ownership information, and treat the entity as posing a high risk and apply special measures.
- Verify whether you monitor the entities you consider to pose a high risk more frequently than other entities, and apply special measures to mitigate the risks.

Third party transactions To conduct this assessment, we may:

- Review your procedures, processes and controls for situations where you are not able to determine whether an account is to be used by, or on behalf of, a third party when there are reasonable grounds to suspect that it would be.

Politically exposed persons and heads of international organizations To conduct this assessment, we may:

- Verify your records to confirm that you rate all your foreign politically exposed person clients as posing a high risk, as well as their family members and close associates.
- Review your records of domestic politically exposed persons and heads of international organizations, as well as those of their family members and close associates, to ensure that you have adequately assessed the level of risk posed by these clients. To do so, we look at a sample of these clients to see if they meet the criteria you have established to rate a client as posing a high-risk.
- Verify whether you monitor your high-risk clients more frequently than your lower risk clients and apply special measures.
- Review transaction records involving politically exposed persons and heads of international organizations, as well as their family members and close associates, to confirm that you are reporting suspicious transactions when required.

Our focus We will focus on the following:

- **Business relationships and ongoing monitoring:** we will focus on ensuring you have an adequate ongoing monitoring process in place.
- **Beneficial ownership:** we will focus on ensuring that you have a process in place to obtain, and take reasonable steps to confirm the accuracy of beneficial ownership information.
- **Third party determination:** we will focus on ensuring that you are taking reasonable steps to determine whether there is a third party to a transaction or giving instructions on an account.
- **Politically exposed persons and heads of international organizations:** we will focus on ensuring that you are taking reasonable steps to find out if your clients are politically exposed persons or heads of international organizations (including family members and close associates), and for those who pose a high risk, we will focus on the special measures you have in place.

3.3. Financial transactions reporting requirements

We use the methods described in this section to assess your compliance with financial transaction reporting requirements.

To conduct this assessment, we may:

- Review your policies and procedures to confirm that they provide enough guidance for your employees or agents to meet the reporting requirements.
- Review your client records, transaction records and submitted reports to confirm that you adequately apply your policies and procedures.

- Interview your employees and agents to assess their knowledge of the reporting requirements.

Our focus We will focus on confirming that you have sound policies, procedures, processes and controls in place to adequately meet the following requirements: to submit financial transaction reports to FINTRAC (when required); to submit the reports on time; and to submit complete and accurate reports.

3.3.1. Requirements related to all reports types (all report types) (Applicable to all business sectors)

We use the methods described in this section to assess your compliance with reporting requirements. The methods apply to all report types (Large Cash Transaction Reports, Large Virtual Currency Transaction Reports, Electronic Funds Transfer Reports, Casino Disbursement Reports, and Suspicious Transaction Reports), with the exception of Terrorist Property Reports, for which only the assessment method titled "All report types 5" applies.

We use comparison testing, follow-up testing, quality testing, and timing testing.

Comparison testing (All report types 1) Reviewing changes in your reporting behaviour

We review your reporting history to identify important variations, such as a noticeable increase or decrease in reporting, and confirm that you send reportable transactions when required. If we observe changes, we check to see if we have an explanation for them on file. If not, we follow up with you. We may review your transaction records to see if there are reports that should have been sent to us.

Follow-up testing (All report types 2): Ensuring that you resubmit the reports FINTRAC rejected for technical errors

FINTRAC can reject a report if it contains technical errors, such as the way the report is formatted, or when quality issues are identified by our validation process. At the assessment, we provide you with a list of rejected reports which you did not correct and resubmit.

If you think this list is incorrect, we may ask you to provide us with the FINTRAC generated External Report Reference Number or the Reporting Entity's Report Reference Number to allow us to further enquire. Refer to our guidance on Batch Reporting Instructions and Specifications and FINTRAC Web Reporting system (FWR, formerly F2R).

For the reports that were not resubmitted, we may ask you why that was the case. We may also look at the records of transactions to confirm whether they were reportable.

(All report types 3) Ensuring past reporting issues have been fixed

We review your records and transaction records to confirm that you have fixed previous compliance issues related to reporting, such as those identified by way of a voluntary self-declaration of non-compliance, and those identified through previous compliance assessment activities that FINTRAC has conducted.

Quality testing (All report types 4) Ensuring you report on transactions handled by your agents

We verify that you are reporting the transactions conducted by your agents on your behalf. You, not your agents, are ultimately responsible for submitting these reports. We may ask you to give us a list of your agents, including agency agreements, and a list of the transactions conducted by each agent to ensure that reportable transactions were submitted to FINTRAC.

(All report types 5) Ensuring your reports are complete and accurate

We review the information in your reports to verify that they are complete and accurate.

When we assess the quality of your reports, we verify whether any information is missing, inadequate or incomplete. For example, if the address field in a report was blank, we would consider this to be missing information. If the field included a post office box rather than a civic address, we would consider this to be inadequate information. If the field showed a civic address without the city, we would consider this to be incomplete. All of the fields in your reports must be complete and accurate.

We review the quality of your reports by considering all of the fields, including those that are mandatory, mandatory if applicable, and reasonable measures fields.

When reasonable measure fields are left blank, we will examine your records to see if you had the information at the time of the transaction. If you did have the information but did not include it in the report, as required, we will ask you to explain why.

We assess the information reported in Part G, "Description of Suspicious Activity" of Suspicious Transaction Reports to verify that there is an adequate description of the reasonable grounds to suspect that the reported transaction(s), or attempted transaction(s), were related to the commission, or attempted commission, of a money laundering offence or a terrorist activity financing offence.

In Terrorist Property Reports, we verify that information about the property and the persons or groups that own or control it, and information about transactions or attempted transactions related to the property, has been provided.

(All report types 6) Ensuring that your third party service provider reports correctly

When you use a third-party service provider to submit reports on your behalf, we verify that the reports list the correct identification information, such as your business name, phone number and location, not the identification information of the service provider.

We examine your records of transactions to identify the ones that should have been reported, and then verify that the service provider sent us the reports with the correct identification information. If we cannot find the reports in our database under the name of your business, we will seek to determine if your service provider used the wrong identification information when it sent the reports to FINTRAC or if the reports were not submitted.

Timing testing (All report types 7) Ensuring that you are sending reports on time

We assess whether you are submitting reports within the timelines set out in the PCMLTFA and associated Regulations, and as described in FINTRAC guidance. We may review the reports you submitted and compare them to your transaction records to confirm that the reports were sent on time.

3.3.2. Large Cash Transaction Reports (LCTRs) We use methods described in this section to assess your compliance with requirements relating to Large Cash Transaction Reports.

(LCTR 1) Confirming you are submitting LCTRs (Applicable to all business sectors)

We ask you to provide us with a list of your cash transactions or records of transactions of $10,000 or more, or both, including transaction and client identification information, so that we can compare the transactions with your reporting. If we cannot find a report for a given transaction, we will enquire into the reasons behind this discrepancy.

To be clear, we do not require a list of the Large Cash Transaction Reports you or your third-party service provider have submitted; we already have these reports in our database. What we require is a list that includes the information about your large cash transactions, one that comes directly from your business records or the systems that you or your third-party service provider may have used to gather the information to submit Large Cash Transaction Reports. We may ask you to send us a sample of this list before requesting the complete list in order to verify that it is in the format that we need.

If you do not have an automated system that can extract the information and produce a list, you will need to provide the records of the transactions. These could be deposit slips, invoices, sales receipts, receipt books, foreign currency exchange transaction tickets, pit logs (casino sector), records of player buy-ins (casino sector), etc.

(LCTR 2) Confirming you are correctly applying the 24-hour rule to LCTRs (Applicable to all business sectors)

We review your policies and procedures, records of transactions, internal records and reports and other documents to identify how you treat cash transactions of less than $10,000 conducted by, or on behalf of, the same person or entity, that, when combined, total $10,000 or more within a 24-hour period. We confirm that you combine these transactions and send us the required Large Cash Transaction Reports when the transactions were made within 24 consecutive hours.

We also verify that you send us separate Large Cash Transaction Reports for lump-sum cash transactions of $10,000 or more, and that you do not combine these with cash transactions of less than $10,000 conducted within a 24-hour period.

(LCTR 3) Confirming that you are submitting all the required reports for a given transaction (Applicable to financial entities, casinos and money services businesses)

We review your records to verify that you have submitted a Large Cash Transaction Report **and** an Electronic Funds Transfer Report when you have received $10,000 or more in cash from, or on behalf of, the same person or entity, in a lump sum or over a 24-hour period, for the purpose of initiating an outgoing international electronic funds transfer of $10,000 or more. We look at your transaction records or the Large Cash Transaction Reports in which you indicated that the disposition of funds was through an "outgoing electronic funds transfer". We may ask you to provide the report numbers for the Electronic Funds Transfer Reports and the Large Cash Transaction Reports to confirm that both types of reports were submitted to FINTRAC.

(LCTR 4) Reviewing exceptions to submitting LCTRs Exception—Alternative to large cash transactions

(Applicable to financial entities)

If a financial entity has used the alternative to submitting Large Cash Transaction Reports, as permitted under the PCMLTFA and associated Regulations and as described in our guidance, we verify that all of the conditions associated with this exception were respected. We confirm that you submitted, within the prescribed timeframe, a complete and accurate Financial Entity Business Client Report that includes a list of all the clients to which the exception has been applied. If you continue to apply the alternative to a client who no longer meets the prescribed conditions, we will review the client's cash transactions to determine whether Large Cash Transaction Reports should have been submitted to FINTRAC.

Exception—Cash received from financial entities or public bodies or from a person who is acting on behalf of a client that is a financial

entity or public body

(Applicable to all business sectors)

If you did not send us Large Cash Transaction Reports for clients who are financial entities, public bodies, or a person who is acting on behalf of a client that is financial entity or public body as the law permits, we will verify that the clients are financial entities or public bodies as defined in the PCMLTFA and associated Regulations. If they do not meet the definition, we may review the client's cash transaction history to determine if there are Large Cash Transaction Reports that should have been submitted to FINTRAC.

3.3.3. Large Virtual Currency Transaction Reports (LVCTRs) We use the methods described in this section to assess your compliance with the requirements relating to Large Virtual Currency Transaction Reports.

(LVCTR 1) Confirming you are submitting LVCTRs (Applicable to all business sectors)

We ask you to provide us with a list of your virtual currency transactions or records of virtual currency transactions of $10,000 or more, or both, including transaction and client identification information, so that we can compare the transactions with your reporting. If we cannot find a report for a given transaction, we will enquire into the reasons behind this discrepancy.

To be clear, we do not require a list of the Large Virtual Currency Transaction Reports you or your third-party service provider have submitted; we already have these reports in our database. What we require is a list that includes the information about your large virtual currency transactions, one that comes directly from your business records or the systems that you or your third-party service provider may have used to gather the information to submit Large Virtual Currency Transaction Reports. We may ask you to send us a sample of this list before requesting the complete list in order to verify that it is in the format that we need.

If you do not have an automated system that can extract the information and produce a list, you will need to provide the records of the transactions. These could be virtual currency exchange transaction tickets, deposit slips, invoices, sales receipts, receipt books, foreign currency exchange transaction tickets, pit logs (casino sector), records of player buy-ins (casino sector), etc.

(LVCTR 2) Confirming you are correctly applying the 24-hour rule to LVCTRs (Applicable to all business sectors)

We review your policies and procedures, records of transactions, internal records and reports, and other documents to identify how you treat virtual currency transactions that total $10,000 or more within 24 consecutive hours, and that are conducted by, or on behalf of, the same person or entity, or when the

amounts are for the same beneficiary. We confirm that you combine these virtual currency transactions and send us the required Large Virtual Currency Transaction Reports when the transactions were made within 24 consecutive hours.

(LVCTR 3) Confirming that you are submitting all the required reports for a given transaction (Applicable to financial entities, casinos, money services businesses and foreign money services businesses)

We review your records to verify that you have submitted a Large Virtual Currency Transaction Report **and** an Electronic Funds Transfer Report when you have received $10,000 or more in virtual currency, in a deemed single transaction, for the purpose of initiating an outgoing international electronic funds transfer of $10,000 or more. We look at your transaction records or the Large Virtual Currency Transaction Reports in which you indicated that the disposition of funds was an "outgoing international electronic funds transfer". We may ask you to provide the relevant report numbers to confirm that both types of reports were submitted to FINTRAC.

3.3.4. International Electronic Funds Transfer Reports (EFTRs) (Applicable to financial entities, casinos, money services businesses and foreign money services businesses)

We use methods described in this section to assess your compliance with the requirements relating to Electronic Funds Transfer Reports.

(EFTR 1) Confirming that you are submitting EFTRs We ask you to provide us with a list of your international electronic funds transfers of $10,000 or more, including transaction and client information, when you are the initiator or final receiver of the international electronic funds transfer, so that we can compare the transactions with your reporting. If we cannot find a report for a given transaction, we will enquire into the reasons behind this discrepancy.

To be clear, we do not require a list of the Electronic Funds Transfer Reports that you or your third-party service provider have submitted; we already have these reports in our database. What we require is a list that includes the information about your international electronic funds transfer transactions, one that comes directly from your business records or the systems you or your third-party service provider may have used to submit Electronic Fund Transfer Reports. We may ask you to send us a sample of this list before requesting the complete list in order to verify that it is in the format that we need.

If you do not have an automated system that can extract the information and produce a list, you will need to provide the records of the transactions. These could be transfer slips, wire logs, foreign currency exchange transaction tickets, invoices, etc.

(EFTR 2) Confirming that you are applying the 24-hour rule to EFTRs We review your policies and procedures, records of transactions, internal records and reports and other documents to identify how you treat international electronic funds transfers of less than $10,000 conducted by, or on behalf of, the same person or entity, that, when combined, total $10,000 or more within a 24-hour period. We then confirm that you combine these transactions and send us the required Electronic Funds Transfer Reports.

We verify that you send us separate Electronic Funds Transfer Reports for lump-sum international transfers of $10,000 or more, and that you do not combine these with international electronic funds transfers of less than $10,000 conducted within a 24-hour period.

We also verify that you do not combine incoming international electronic funds transfers with outgoing international electronic funds transfers. In addition, for outgoing international electronic funds transfers, we verify that you combine transactions correctly when applying the 24-hour rule for transactions conducted by, or on behalf of, the same client. We also ensure you correctly combine incoming international electronic funds transfers.

(EFTR 3) Confirming that you are submitting all the required reports for a given transaction (Applicable to financial entities, casinos, money services businesses and foreign money services businesses)

We review your records to verify that you have submitted a Large Cash Transaction Report **and** an Electronic Funds Transfer Report when you have received $10,000 or more in cash, in a deemed single transaction, for the purpose of initiating an outgoing international electronic funds transfers of $10,000 or more. We look at your transaction records or the Large Cash Transaction Reports in which you have indicated that the disposition of funds was an "outgoing electronic funds transfer". We may ask you to provide the relevant report numbers to confirm that both types of reports were submitted to FINTRAC.

Assessment methods LCTR 3, LVCTR 3 and EFTR 3 are identical and are repeated for ease of reference.

3.3.5. Casino Disbursement Reports (CDRs) (Applicable to casinos)

We use the methods described in this section to assess your compliance with the requirements related to Casino Disbursement Reports.

(CDR 1) Confirming that you are submitting CDRs For this test, we ask you to provide us with a list of your casino disbursement records of $10,000 or more, including transaction and client information, so we can compare the transactions with your reporting. If we cannot find a report for a given transaction, we will enquire into the reason behind this discrepancy.

To be clear, we do not require a list of the Casino Disbursement Reports that you or your third-party service provider have submitted; we already have these reports in our database. What we require is a list that includes the information about your cash disbursements, one that comes directly from your business records or systems. We may ask you to send us a sample of this list before requesting the complete list, in order to verify that it is in the format we need.

If you do not have an automated system that can extract the information and produce a list, you will need to provide records of the disbursements. These could be cheque registers, player tracking sheets, transaction logs, etc.

(CDR 2) Confirming that you are applying the 24-hour rule to CDRs
We review your policies and procedures, records of transactions, internal records and reports and other documents to identify how you treat disbursements of less than $10,000 received by, or on behalf of, the same client, that, when combined total $10,000 or more, within a 24-hour period. We confirm that you combine these transactions and send us the required Casino Disbursement Reports.

We also confirm that you send us separate Casino Disbursement Reports for lump-sum disbursements of $10,000 or more and that you do not combine these with disbursements of less than $10,000 conducted within a 24-hour period.

3.3.6. Suspicious Transaction Reports (STR) (Applicable to all business sectors, with the exception of STR 13, STR 14 and STR 15)

We use the methods described in this section to assess your compliance with Suspicious Transaction Report requirements.

Suspicious Transaction Reports are of significant intelligence value to FINTRAC as they are the cornerstone of the Centre's mandate to detect, deter and prevent money laundering and terrorist activity financing. Suspicious Transaction Reports, and other reports, enable the Centre to conduct analysis and produce actionable financial intelligence, which it discloses to police, law enforcement and national security agencies when prescribed thresholds are met.

Most of the assessment methods described in this section are based on money laundering and terrorist activity financing indicators published in FINTRAC guidance and other well-known reliable sources, such as the Financial Action Task Force (FATF).

The assessment methods for Suspicious Transaction Reports serve to evaluate how you address suspicious transactions, as well as other requirements. We use them to:

- Assess your compliance with other requirements, such as the risk assessment, special measures, and ongoing monitoring requirements;
- Verify that you identify money laundering and terrorist activity financing indicators, as well as transactions that may give rise to reasonable grounds to suspect that the transactions, or attempted transactions, are related to

the commission or attempted commission of a money laundering offence or terrorist activity financing offence;
- Verify that you have a sound escalation and decision-making process for suspicious transactions;
- Verify that all relevant business areas receive key information regarding suspicious transaction activity; and
- Verify that you are sending us Suspicious Transaction Reports when required.

When assessing the information we gather through the application of these methods, we will use the approach described in Part 1 to arrive at our conclusions. We will evaluate the body of information and the totality of the circumstances and take a holistic and reasonable approach when arriving at our conclusions.

We use monitoring and unusual transactions testing, testing of high-risk areas, money laundering and terrorist activity financing indicator testing, external information testing, comparison testing, transaction reversal and relationship termination testing, and business sector specific testing.

The methods described in this section apply to both completed and attempted suspicious transactions. Assessment methods relating to the quality and timing of reports can be found in section 3.3.1 (all reports types).

Monitoring and unusual transaction testing (STRs) In this section, the words "alerts" and "unusual transactions" refer to completed or attempted transactions that have been identified or flagged as part of your internal monitoring process because they may be related to money laundering or terrorist activity financing. Alerts and unusual transactions should be further assessed in keeping with your policies and procedures and could eventually lead to a Suspicious Transaction Report.

(STR 1) Reviewing your policies and procedures on how you monitor activities and transactions

We review your policies and procedures to confirm that you have a monitoring process that enables you to detect, assess and, when required, report suspicious transactions related to money laundering and terrorist activity financing. If you use generic policies and procedures developed by an industry group or consultant, we verify that you have adapted these policies and procedures to your business, including monitoring procedures.

We may ask questions such as:

- Is your monitoring process automated, manual or both?
- How are you alerted to, or informed of, unusual transactions, and how do you prioritize and action these?
- When you receive an alert, what process do you follow to identify, assess, and make a decision about the unusual transaction and, when required, report the transaction to FINTRAC?

- How often do you review your transaction monitoring process to make sure it remains in line with your risk assessment, and policies and procedures?

(STR 2) Reviewing your monitoring rules

We review the automated and manual monitoring rules that you have put in place to confirm that they help you detect unusual transactions and provide alerts on potentially suspicious transactions. When we review your rules, we confirm that they are reasonable, put into practice, and that they monitor transactions in keeping with your risk assessment. We may also ask you how often you adjust the rules, what would cause you to adjust them, what steps you take to do so, and how you document these adjustments. We may verify whether you periodically review your rules, to confirm that you are not overlooking potentially suspicious transactions.

(STR 3) Reviewing unusual transactions

We review the unusual transactions identified by your monitoring system that you did not report to confirm that your decisions were sound.

We look into whether you use a risk-based approach to identify unusual transactions and generate alerts, so that you can direct more of your time and effort to areas of higher risks of money laundering and terrorist activity financing. For example, you may place more importance on transactions that present two or more money laundering or terrorist activity financing indicators.

If you do use a risk-based approach to manage unusual transactions, we will determine if your approach is reasonable. To do this, we will assess:

- If you have sufficient resources to monitor and review transactions based on the size of your business and its transaction volume.
- If you have a reasonable rationale to support the thresholds placed on the monitoring rules and unusual transactions.
- How often you monitor and action unusual transactions that pose a lower risk.

Testing high-risk areas (STR) (STR 4) Reviewing your high-risk areas

We review client records and transaction records related to the high-risk areas identified in your risk assessment, such as high-risk clients, high-risk delivery channels, or high-risk jurisdictions. We may also review a sample of client records and transaction records for areas you did not determine to pose a high risk to ensure no gaps exist in your risk assessment or reporting procedures.

Money laundering and terrorist activity financing indicator testing (STR) (STR 5) Identifying indicators consistently

We ensure that you are applying your money laundering or terrorist activity financing indicators in a consistent manner when submitting Suspicious Transaction Reports. We first review Part G of the reports you have submitted to

identify the most common indicators listed. We then verify your records to assess whether you continue to submit suspicious transaction reports when these common indicators are present in other transactions, and there are reasonable grounds to suspect that the transactions are potentially related to money laundering or terrorist activity financing. If we identify suspicious transactions that were not reported, we will prioritize transactions that would have given FINTRAC new information for analysis.

(STR 6) Reviewing transactions for money laundering and terrorist activity financing indicators

As part of our risk assessment of your business, we identify money laundering and terrorist activity financing indicators that you may come across in the course of your business. We verify that these indicators inform your compliance program and support your efforts to detect, assess, and report suspicious transactions. Should we detect transactions that reflect these indicators in our review of your client records and transaction records, we will look into the actions you took to determine whether they were reasonable.

In addition, while we recognize that you may prioritize certain indicators over others, we verify that your processes and systems do not overlook suspicious behaviour.

External information testing (STR) (STR 7) Reviewing how you use publicly available information

We look at how you use publicly available information as part of your risk assessment, monitoring and Suspicious Transaction Report processes. Publicly available information includes news releases issued by industry regulators, police and other law enforcement agencies, mainstream news media, and other credible sources. We assess whether you take reasonable steps when you discover something of interest about a client. We will enquire about your reasons for not acting upon publicly available information.

(STR 8) Reviewing how you process information from credible sources

We verify how you use information received from police, law enforcement and national security agencies, and regulatory or supervisory bodies, related to money laundering and terrorist activity financing, to inform your compliance program. This information could include production orders, comfort letters, alerts and internal referrals. Specifically, we look at how you use this information to identify potential high-risk clients, take measures to reduce the risk related to these clients, and submit Suspicious Transaction Reports when required. We verify that the information is forwarded to your compliance officer or your compliance department when it is addressed to a different person or department.

FINTRAC will not ask to see sealed production orders nor those that include an order of non-disclosure.

Comparison testing (STR) (STR 9) Verifying variances in actual versus expected transactional behaviour

We verify whether you detect when a client's transactions differ noticeably from what is expected and that you take action. We may review the client records and transaction records of clients whose transactions noticeably differ from those of similar clients. For example, a client may conduct more transactions or transactions of higher value than what is expected when compared to a group of similar clients.

(STR 10) Detecting unusual patterns

We review your client records of transactions for unusual patterns or connections that we determine meet the reasonable grounds to suspect threshold and should be reported. For example, we may look for:

- Clients who appear unrelated but have the same address or phone numbers.
- Clients who are in school or unemployed and conducting high-value transactions.
- People without any apparent relation making deposits into the same account.

When we search for patterns or connections, we look through your electronic or paper records, as well as through the reports you sent us. We also ask if you look for such patterns or connections and how you do so.

Transaction reversal and relationship termination testing (STR) (STR 11) Reviewing your refunds, cancellations and overpayments

We review records of transactions where a refund cheque was issued because a customer returned an item, cancelled a life insurance policy, terminated a service, cancelled a real estate transaction, or overpaid for transactions. These situations may represent common money laundering and terrorist activity financing indicators, and as such, we review your procedures to ensure that you are adequately assessing these situations and taking the necessary measures, as applicable.

(STR 12) Reviewing how you end relationships with clients and agents

The PCMLTFA and associated Regulations do not require you to end business relationships. That decision remains yours to make. However, if you decide to end a relationship with a client or an agent because of concerns related to money laundering or terrorist activity financing, we verify that you continue to monitor their transactions for possible suspicious transactions, and take steps to mitigate risks, until the relationship is officially ended.

Business-sector-specific testing (STR) The Suspicious Transaction Report assessment methods described above are applicable to most business sec-

tors. However, some sectors have characteristics that require specific testing.

(STR 13) Real estate: Reviewing how you use market values and local market conditions

(Applicable to real estate)

We verify that you detect purchase or sale transactions that are noticeably below or above the expected market value, based on local market conditions, to determine whether the transaction is suspicious. Real estate values and market conditions vary across Canada based on location, the economic cycle and other factors. We assess whether you are aware of these market conditions and that you identify transactions that are well outside their expected or average market value.

(STR 14) Real estate: Reviewing deals with last-minute changes in ownership

(Applicable to real estate)

We review transaction records, including client records, receipt of funds records, bank drafts and third party determination records where there are unexplained or last-minute substitutions of the buyer. We assess whether you have identified these cases as needing further review and assessment for possible layering or hiding of the true ownership, or that the original purchaser may be instructed by a third party until the property is assigned.

(STR 15) Casino: Reviewing your issued cheques for unusual buy-ins or disbursements

(Applicable to casinos)

We review the cheques you issued to clients to identify unusual buy-ins or disbursements that may indicate an attempt to layer proceeds of crime. We first ask you to explain how you identify unusual buy-ins or disbursements, reduce potential risks, monitor the transactions, and decide whether to submit a Suspicious Transaction Report.

Then, we may ask you for a list of the clients you have issued cheques to, so that we can identify irregularities, such as clients who may have received more cheques than what would usually be seen. If we do identify irregularities, we ask for the client history information and look for suspicious buy-ins or disbursements that should have been reported.

3.3.7 Terrorist Property Report (TPRs) We use the methods described in this section to assess your compliance with Terrorist Property Report requirements.

(TPR 1) Reviewing your correspondence with authorities (Applicable as indicated below)

We review:

- For all business sectors, correspondence with the Royal Canadian Mounted Police (RCMP) or the Canadian Security Intelligence Service (CSIS) in which you indicated that you are in possession or in control of property owned or controlled by, or on behalf of, a terrorist, terrorist group, or listed person.
- The reports that financial entities, life insurance companies, and securities dealers are required to submit under the Criminal Code or the Regulations Implementing the United Nations Resolution on the Suppression of Terrorism. These reports are sent to provincial or federal regulators, in which the business indicated being in possession or control of property owned or controlled by, or on behalf of, a listed entity or listed person.

If you have disclosed that you are in possession of such property, we confirm that you sent us a Terrorist Property Report. We also verify that the information in the Terrorist Property Report is consistent with the information you sent the RCMP, CSIS, and your regulator (if applicable).

(TPR 2) Verifying lists for terrorist or terrorist groups and listed persons (Applicable to all business sectors)

We confirm the steps you take to determine whether your business possesses or controls the property of a terrorist, terrorist group or listed person, and submit a Terrorist Property Report. If you are, or were, in possession or control of such property, we verify that you sent us a Terrorist Property Report.

We may assess how you handle situations where you cannot determine, based on the information you have, if you are dealing with a terrorist, terrorist group or listed person.

Whether you cannot file a Terrorist Property Report because you cannot make the necessary determination, or whether you are able to file a Terrorist Property Report, we verify that you send us Suspicious Transaction Reports when required. The added information in the Suspicious Transaction Report may prove valuable to FINTRAC in its intelligence work.

We may compare your clients' names against the list published in the Regulations Establishing a List of Entities issued under the Criminal Code and the list published in the Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism. If one of your clients is on either list, we verify that you submitted a Terrorist Property Report.

3.4. Record keeping requirements

(Applicable to all business sectors)

We use the methods described in this section to assess your compliance with record keeping requirements.

To conduct this assessment, we may

- Review your policies and procedures to confirm that they give enough guidance to your employees or agents to meet the record keeping requirements.
- Review your client records and records of transactions to confirm that you put these policies and procedures into practice.
- Verify that you keep records as required by the PCMLTFA and associated Regulations when reviewing your client records and transaction records.
- Records may include the following, as applicable:
  - account opening records;
  - credit card account and transaction records;
  - prepaid payment product account and transaction records;
  - records of large cash transactions or large virtual currency transactions
  - records of electronic funds transfer or virtual currency transfer transactions;
  - records of casino disbursements;
  - foreign currency exchange or virtual currency exchange transaction tickets;
  - information records;
  - records that you are required to keep under client identification and know your client requirements; and
  - copies of reports submitted to FINTRAC
- Verify that you keep the information that is required (for example, name, address, date of transaction, etc.) for each type of record. The information that you are required to keep is determined by the type of record that needs to be kept.
- Verify that your records are kept in a format that can be produced within 30 calendar days of a request, and confirm that you keep the records for five years, or as long as required by the PCMLTFA and associated Regulations.
- Interview your employees and agents to assess their knowledge of record keeping requirements.

Our focus While we assess record keeping, we will focus on ensuring that you accurately record information that identifies persons and entities that open or control accounts, and conduct or direct transactions.

3.5. Correspondent banking relationship requirements

(Applicable to financial entities)

We use the methods described in this section to assess your compliance with correspondent banking relationships requirements.

To conduct this assessment, we may:

- Review your policies and procedures to confirm that they provide enough

guidance for your employees or agents.
- Review your records, including records of transactions to confirm that your policies and procedures are put into practice.
- Review your records of transactions to confirm that you, as applicable:
  - take all required measures as per the PCMLTFA and associated Regulations—described in FINTRAC guidance;
  - do not deal with a shell bank;
  - obtain the required approvals;
  - identify your clients, when required;
  - obtain and keep records of required information;
  - risk assess the relationship;
  - take special measures, when required; and
  - meet the requirements within the prescribed timeframes.
- Interview your employees and agents to assess their knowledge of correspondent banking requirements.

When we evaluate your risk assessment, we may:

- Verify whether you have considered correspondent banking relationship risks such as the correspondent bank's location, corporate structure, profile and reputation, clientele, products and services, type and volume of activity, openness to sharing information as needed, and regulatory history.
- Review your record of the correspondent bank's anticipated account activity, including products or services. We may ask if, and how, you use this information to review the transactions conducted through your correspondent banking accounts in order to determine whether there are transactions or attempted transactions that deviate from the terms of your agreement. We may also review the records of transactions to this end.

If your policies and procedures allow for:

- Payable-through accounts: we verify that you take reasonable measures to confirm that the correspondent bank identifies its clients who have direct access to your correspondent banking services in a manner that is consistent with Canadian client identification requirements and that it has agreed to provide you with relevant client identification data upon request;
- Nested accounts: as a best practice, we may review the information that you have about the downstream bank and the controls you have implemented to mitigate risk and monitor the transactions conducted by the downstream banks and their clients.

If your policies and procedures prohibit payable-through accounts and nested accounts, we will ensure you have the appropriate controls in place to detect transactions involving these types of accounts and, if detected, that you have taken remedial action in keeping with your policies and procedures.

As part of our assessment, we may also:

- Verify that you update information regarding your correspondent banking relationship, the type of information that you update, and how often you update it.
- Verify that you have disclosed all your correspondent relationships to us, which may include a review of your records of transactions to confirm.
- Review your process to end a correspondent banking relationship because of money laundering or terrorist activity financing concerns.

Our focus We will focus on the steps you take to ensure that senior management has approved your correspondent banking relationships and is aware of the risks involved.

We will also focus on the steps you take to ensure that you are not dealing with a shell bank. Shell banks operate outside the country where they are incorporated and licensed; they are not affiliated to a financial services group that is supervised in that country. Shell banks pose a serious risk to the Canadian anti-money laundering and anti-terrorism financing regime because of the difficulty that exists in ensuring regulatory oversight for requirements such as customer due diligence and risk mitigation measures.

3.6. Foreign branches, foreign subsidiaries and affiliates requirements

(Applicable to financial entities, securities dealers, and life insurance)

We use the methods described in this section to assess your compliance with requirements relating to foreign branches, foreign subsidiaries and affiliates.

Foreign branches and foreign subsidiaries Information on requirements relating to foreign branches and foreign subsidiaries is available in our guidance.

To conduct this assessment, we may:

- Review the policies and procedures that you developed for your foreign branches and foreign subsidiaries to ensure that they are adequate, and reflect Canadian obligations when it comes to:
  - the establishment and implementation of a compliance program, including policies and procedures to evaluate the risk of money laundering and terrorist activity financing and risk mitigation measures when risk is considered high;
  - record keeping and retention; and
  - client identification.
- Confirm that the Board of Directors (if you have one) has approved these policies and procedures before they are put into practice.
- Review your client records and transaction records to confirm that your foreign branches and foreign subsidiaries apply these policies and procedures to the extent permitted by the laws of the country where the branch or subsidiary is located. If the policies and procedures conflict with local laws, we may ask you for the reason of the conflict and whether you have

informed FINTRAC and your primary regulator of this issue, and have considered how you plan to mitigate any associated risks.
- Confirm how you ensure that your foreign branches and foreign subsidiaries are implementing the policies and procedures.

Domestic and foreign affiliates Information on requirements relating to affiliates is available in our guidance.

To conduct this assessment, we may confirm that you have adequate policies and procedures in place to share information with your affiliates for the purpose of assessing the risk of money laundering and terrorist activity financing, and detecting and deterring such offences.

As part of our evaluation of your risk assessment, we may:

- Verify that you have assessed the risk of money laundering and terrorist activity financing for all of your foreign and domestic affiliates. This includes verifying that you have implemented measures to reduce risks should foreign affiliates be located in higher-risk countries.
- Ask you how you use information from affiliates about suspicious activities or transactions in your compliance program.

Our focus We will focus on whether, as described, your foreign branches and foreign subsidiaries have policies and procedures in place and whether you have policies and procedures in place to share information with your affiliates.

3.7. Money services business (MSB), and Foreign money services business (FMSB) registration requirements

(Applicable to money services businesses and foreign money services businesses)

We use the methods described in this section to assess your compliance with money services business and foreign money services business registration requirements.

We verify that you keep registration information up to date, respond to clarification requests, renew your registration, and cancel your registration (if applicable).

To conduct this assessment, we may:

- Review your policies and procedures to confirm that they give enough guidance to your employees or agents to meet the requirements relating to money services business and foreign money services business registration.
- Review your client records and transaction records to confirm that the information provided to FINTRAC is accurate and that your policies and procedures are put into practice.

- Interview your employees and agents to assess their knowledge of the registration requirements.

Our focus We will focus on ensuring that your registration information is accurate and up to date.

3.8. Ministerial directives' requirements

(Applicable to all business sectors)

We use the methods described in this section to assess your compliance with requirements relating to ministerial directives.

The instructions provided in each ministerial directive will vary and, as such, our assessment will focus on the essence of the directive.

To conduct this assessment, we may:

- Review your policies and procedures to confirm that they give enough guidance to your employees or agents to meet the ministerial directive requirements.
- Verify that your policies and procedures clarify what ministerial directives are and where they can be found. We may also look to see whether your policies and procedures indicate how often you should check for new, updated or amended directives; who should be informed when a directive is applicable to your business; and what steps to take to make sure the directive is being followed.
- Review your client records and transaction records to confirm that you put the policies and procedures into practice.
- Verify that you have taken action when directives are applicable through our review of your client records and transaction records. These records may include:
  - the verification of the identity of a person or an entity;
  - the exercise of customer due diligence, including ascertaining the source of funds of a financial transaction, the purpose of a financial transaction or the beneficial ownership or control of an entity;
  - monitoring financial transaction for an account;
  - keeping records;
  - reporting financial transactions to FINTRAC; and
  - complying with other requirements of the PCMLTFA and associated Regulations.
- Interview your employees and agents to assess their knowledge of the requirements relating to ministerial directives.
- Verify that your business, including foreign branches and subsidiaries (if applicable), follows the directives.

When a foreign branch or foreign subsidiary cannot comply with a directive because it conflicts with local laws, we may:

- Review your records to verify that you obtained documents to confirm the conflict.
- Verify that you informed FINTRAC of the reasons for the conflict and, as applicable, the principal agency or body that supervises or regulates your business under federal or provincial law within a reasonable period.
- Ask about the measures you put in place to reduce the risks.

When you conduct business in a foreign jurisdiction or with a foreign entity named in a ministerial directive, we may:

- Verify that your risk assessment considers the parameters of the ministerial directive.
- Verify that you apply the processes that you have in place to manage high-risk transactions associated with ministerial directives, including monitoring the transactions more frequently, applying special measures, and submitting Suspicious Transaction Reports when required.

Our focus We will focus on determining whether you are adequately implementing ministerial directives.# Guide on harm done assessment for violations of other compliance measures

1. Introduction

This page presents how we assess the harm done and calculate the base penalty amount applied to violations of requirements related to correspondent banking, foreign branches and subsidiaries, complying with the Minister's Directive, prescribed information in prescribed electronic funds transfers (travel rule), and providing assistance or information reasonably required to FINTRAC.

1.1 Purpose of the guide

This guide presents how FINTRAC approaches the harm done criterion and the base penalty amount for violations under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (the Act) and its regulations. According to section 73.11 of the Act, FINTRAC must consider the harm done by a violation, that the purpose of an administrative monetary penalty (AMP) is to encourage compliance rather than to punish, and all other criteria prescribed in the regulations, including a reporting entity's (RE) history of compliance, when determining the amount of a penalty. Considerations for the non-punitive nature of an AMP and an REs' compliance history are assessed in another step in the penalty calculation and are outlined separately in FINTRAC's AMP policy.

1.2 Definition of harm

FINTRAC defines "harm" as the degree to which a violation interferes with achieving the objectives of the ActFootnote 1 or with FINTRAC's ability

to carry out its mandateFootnote 2. Therefore, the consequences of non-compliance, when an AMP is imposed, are linked to its effects on Canada's efforts to combat money laundering and terrorist activity financing (ML/TF).

Compliance enforcement activities are undertaken to prevent and correct the harm that comes from non-compliance with the Act and regulations. REs' adherence to requirements such as record keeping and verifying client identity assists in the deterrence of ML/TF and supports investigations and criminal prosecutions. The requirements related to reporting ensure that FINTRAC is supplied with the high-quality, timely financial transaction reports it needs to produce the financial intelligence that helps with the investigation and prosecution of ML/TF offences.

1.3 Considering harm in AMP calculations

When determining a penalty, FINTRAC considers the harm caused, that is, the degree to which the non-compliance interferes with the purpose of the Act and/or with FINTRAC's mandate. Non-compliance and harm are measured using the standards described in this guide, which outline the benchmark amounts for the corresponding levels of harm for a specific violation. FINTRAC considers the specific circumstances of each case, including the extent of the non-compliance and mitigating factors, which may further reduce the actual amounts applied.

2. Violations related to other compliance measures

Compliance measures related to correspondent banking, foreign branches and subsidiaries, minister's directives, prescribed information in electronic funds transfers (EFTs) and assistance to the Centre have been put in place to strengthen Canada's Anti-Money Laundering and Anti-Terrorism Financing (AML/ATF) regime. In particular, measures related to correspondent banking, foreign branches and subsidiaries, and minister's directives help to achieve the objectives set out in subsections 3(c) and 3(d) of the Act concerning Canada's international commitment to fight transnational crime, especially ML/TF. These measures also strengthen Canada's ability to take targeted steps to protect Canada's financial system. Measures concerning prescribed information in EFTs help eliminate anonymous transactions and ensure that transaction information is made available for compliance, risk assessment, analysis, investigations and prosecutions. Finally, measures concerning assistance to FINTRAC are in place so that we can ensure REs comply with the requirements of the Act and its regulations. If an RE fails to meet these requirements, it interferes with the regime's ability to achieve the objectives of the Act and FINTRAC's mandate, which is to detect, prevent and deter ML/TF.

3. Violations related to complying with a Minister's directive

In order to safeguard the integrity of Canada's financial system, the Minister of Finance has the authority to issue directives to REs and their foreign branches and subsidiaries, in respect of a designated foreign jurisdiction or entity. A directive allows the Minister to require that specific measures be carried out beyond those of the Act and its regulations when a foreign jurisdiction or entity is at a heightened risk of facilitating ML/TF. These additional, targeted measures are designed to enhance existing requirements to mitigate the specific ML/TF risks of financial transactions originating from or destined to foreign jurisdictions or entities with ineffective or insufficient AML/ATF measures. These additional, targeted measures may help avoid an adverse impact on the integrity of Canada's financial system or on its reputation.

Provision of the Act	Description	Classification of violation
11.43	Failure to comply with a ministerial directive	Very serious$1-$500,000
11.44(1)	Failure to ensure that a foreign branch or foreign subsidiary complies with a ministerial directive	Very serious$1-$500,000

Table 1—Violations related to complying with a Minister's directive

3.1 Harm done in the case violations related to complying with a Minister's directive

Failing to comply with a Minister's directive could interfere with the achievement of the objectives described under paragraphs 3(c) and (d) of the Act with respect to fulfilling Canada's international commitments to fight transnational crime, particularly ML/TF, and enhancing Canada's targeted measures to protect its financial system from ML/TF. Non-compliance with a minister's directive poses a very high risk to the integrity of Canada's financial system and the safety of Canadians. This is because detection and mitigation measures would not be applied to transactions originating from or destined to a foreign state or a foreign entity that has an ineffective or insufficient AML/ATF regime. In a worst case scenario, suspicious transactions related to ML or TF offences could remain undetected, posing a risk to the financial system and the safety of Canadians.

3.2 Penalty determination for violations related to complying with a Minister's directive

When an RE or its foreign branches or subsidiaries fail to comply with a minister's directive, Canada's financial system is at risk to be used for international ML/TF transactions. The prescribed maximum penalty of $500,000 is applied when a directive is not implemented because ministerial directive violations pose the greatest harm to the achievement of the objectives of the Act and FINTRAC's mandate.

The measures required by a Minister's directive vary, therefore, the penalty determination criteria for partial violations is dependent on the contraventions and the extent of the non-compliance. FINTRAC will consider the circumstances of each case to determine if there are mitigating factors that may reduce the penalty amount.

4. Violations related to correspondent banking

This section outlines FINTRAC's approach to the violations related to correspondent banking requirements, including harm assessments and penalty calculations.

4.1 Violation for having a correspondent banking relationship with a shell bank

Removing anonymity in transactions is one of the most important safeguards against the exploitation of Canada's financial system for ML/TF. Financial entities in Canada are specifically prohibited from having correspondent banking relationships with shell banks because this could facilitate anonymity in transactions and give little or no AML/ATF oversight.

Provision of the Act	Description	Classification of violation
9.4(2)	Having a correspondent banking relationship with a shell bank	Serious$1-$100,000

Table 2—Violation for having a correspondent banking relationship with a shell bank

4.1.1 Harm done in the case of a violation related to having a correspondent banking relationship with a shell bank Shell banks operate outside the country where they are incorporated and licensed, and are not affiliated with a financial services group that is subject to supervision in that country. The control and management of a shell bank happens from a different jurisdiction, sometimes from a private residence, and poses a serious risk to

Canada's AML/ATF regime as it is difficult to ensure regulatory oversight for requirements such as customer due diligence and risk mitigation. The banking supervisor in the country where the shell bank operates is generally unaware of its existence. Shell banks pose a higher risk of ML/TF and they are known for being used to launder the proceeds of crime. If a financial entity in Canada were to allow a shell bank to access to Canada's financial system, this could interfere with the detection, prevention and deterrence of ML/TF activities here, and could also interfere with the achievement of one of the objectives set out in paragraph 3(c), of the Act which is to assist in fulfilling Canada's international commitments to participate in the fight against transnational crime, particularly money laundering, and the fight against terrorist activity.

4.1.2 Penalty determination for a violation related to having a correspondent banking relationship with a shell bank When an RE provides financial services to a shell bank, the RE provides the shell bank with broad access to the Canadian financial system, putting it at risk for ML/TF because of the anonymity the shell bank entails. An RE that has a correspondent banking relationship with a shell bank, that has conducted a transaction with that shell bank, poses the highest risk to Canada's AML/ATF regime and directly contravenes the prohibition under subsection 9.4(2) of the Act. Therefore, the penalty is determined at the prescribed maximum, $100,000. FINTRAC will consider mitigating factors in its calculation of the penalty.

4.2 Violation related to obtaining approval of senior management for correspondent banking relationship

A correspondent banking relationship requires the financial entity's senior management oversight to ensure that it is not a conduit for anonymous, illicit financial transactions. Approval from senior management is required to enter into such a relationship, to ensure accountability at the highest level, and that the organization fully understands the associated ML/TF risks, and has the proper controls in place to mitigate risks.

Provision of the Act	Provision of the PCMLTFRFootnote 3	Description	Classification of violation
9.4(1)(c)	15.1(1)	Failure of a specified entity entering into a correspondent banking relationship with a prescribed foreign entity to obtain the approval of senior management	Minor$1-$1,000

Table 3—Violation related to obtaining approval of senior management for correspondent banking relationship

4.2.1 Harm done in the case of a violation related to obtaining approval of senior management for a correspondent banking relationship When approval to enter into a correspondent banking relationship is not obtained, there is high potential for harm related to the detection, prevention and deterrence of ML/TF in Canada, because there is no oversight and accountability from a financial entity's senior management which would ensure proper assessment and risk mitigation. Transactions posing high ML/TF risk could be conducted through a correspondent banking relationship that has not been scrutinized and risk-assessed by senior management. This makes the financial entity's operations more vulnerable to ML/TF offences and introduces vulnerabilities into Canada's financial system that may go undetected.

4.2.2 Penalty determination for a violation related to obtaining approval of senior management for a correspondent banking relationship When approval to enter into a correspondent banking relationship is not obtained, there is high potential for harm as the financial entity's operations are more vulnerable to ML/TF offences and introduces vulnerabilities into Canada's financial system that may go undetected. Therefore, the prescribed maximum penalty of $1,000 is determined for each correspondent banking relationship that senior management did not approve.

FINTRAC will consider relevant mitigating factors in its determination of the penalty. For example, if there have been no financial transactions or activities conducted with that foreign financial institution at the time that the non-compliance was discovered.

4.3 Violation related to ascertaining the name and address of a foreign financial institution

Financial entities that enter into a correspondent banking relationship are required to ascertain the name and address of the foreign financial institution by examining specific records from recognized authorities. This verification confirms the existence of the foreign financial institution and mitigates the possibility that the foreign financial institution is a shell bank. This information can be used for risk assessment, preparation of reports to FINTRAC, and as evidence when investigating and prosecuting ML/TF offences.

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
9.4(1)(a)	55.1(a)	Failure of a financial entity that enters into a correspondent banking relationship with a foreign financial institution to ascertain, in the prescribed manner, prescribed information in respect of the foreign financial institution	Minor$1-$1,000

Table 4—Violation related to ascertaining the name and address of a foreign financial institution

4.3.1 Harm done in the case of a violation related to ascertaining the name and address of a foreign financial institution Financial entities that enter into a correspondent banking relationship are required to ascertain the name and address of the foreign financial institution by examining specific records from recognized authorities. This verification confirms the existence of the foreign financial institution and mitigates the possibility that the foreign financial institution is a shell bank. This information can be used as evidence when police investigate ML/TF offences and for the preparation of reports to FINTRAC, as well as risk assessments.

Failing to ascertain the name and address of the foreign financial institution

makes the Canadian RE's operations more vulnerable to ML/TF offences and introduces vulnerabilities into Canada's financial system that may go undetected.

4.3.2 Penalty determination for a violation related to ascertaining the name and address of a foreign financial institution The PCMLTFR set out the manner in which the foreign financial institution's name and address must be verified. The requirements were developed to ensure that records from a recognized authority are used to ascertain the information.

Because of the risk that dealing with shell banks poses, when an RE has taken no measures to verify a foreign financial institution's name and address this constitutes a complete violation of the requirement, therefore the maximum penalty of $1,000 per instance will apply.

When the methods used to verify the information are not in line with the methods set out in the PCMLTFR, or when an RE fails to completely adhere to them, the requirement has not been met. As a result, the harm to achieving the objectives of the Act and FINTRAC's mandate is the same as that of a complete violation, therefore the same penalty ($1,000 per instance) will apply. FINTRAC will consider mitigating factors in its determination of the penalty. For example, there have been no financial transactions or activities conducted with that foreign financial institution at the time that the non-compliance was discovered, or corrective measures were taken before any financial transactions or activities were conducted.

4.4 Violations related to ascertaining prescribed information in respect of a foreign financial institution

Correspondent banking relationships with foreign financial institutions that have AML/ATF policies and procedures in place help safeguard Canada's financial system from ML and TF. When foreign financial institutions do not have AML/ATF policies and procedures in place, the risk of exposure to ML/TF offences is heightened for REs transacting with them under correspondent banking relationships. This risk can be further heightened when foreign financial institutions have received civil or criminal penalties related to violations of AML/ATF requirements.

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
9.4(1)(e)	15.1(1) and (3)	Failure of a specified entity to take reasonable measures to ascertain whether a prescribed foreign entity with whom it has entered into a correspondent banking relationship has in place prescribed policies and procedures and, if they are not in place, to take prescribed measures	Minor$1-$1,000

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
9.4(1)(a)	55.1(b)	Failure of a financial entity that enters into a correspondent banking relationship with a foreign financial institution to take reasonable measures to ascertain, in the prescribed manner, prescribed information in respect of the foreign financial institution and to conduct prescribed monitoring	Minor$1-$1,000

Table 5—Violations related to ascertaining prescribed information in respect of a foreign financial institution

4.4.1 Harm done in the case of violations related to ascertaining prescribed information in respect of a foreign financial institution Financial entities entering into a correspondent banking relationship with foreign financial institutions must take reasonable measures to ascertain whether the foreign financial institutions have AML/ATF policies and procedures, including those for approval of new account openings, and whether there are any civil or criminal penalties that have been imposed. If the foreign financial institution does not have the required policies and procedures, or if there has been a civil or criminal penalty imposed, then the Canadian financial entity must take reasonable measures to conduct ongoing monitoring of all transactions under the correspondent banking relationship, for the purpose of detecting transactions that must be submitted as a Suspicious Transaction Report (STR). Not meeting these requirements could signify that the ML/TF risks posed by the correspondent banking relationship are not managed effectively, which can result in unreported suspicious transactions, a loss of financial intelligence and other non-compliance issues. This impedes the achievement of the objectives

set out in subparagraph 3(a)(ii) and paragraph 40(b) of the Act.

4.4.2 Penalty determination for violations related to ascertaining prescribed information in respect of a foreign financial institution The potential harm is highest when an RE fails to take reasonable measures to determine whether the above circumstances apply to a correspondent banking relationship. If ongoing monitoring is not conducted on a foreign financial institution that has no AML/ATF procedures in place, or the foreign financial institution has received civil or criminal penalties for non-compliance with AML/ATF requirements, the prescribed maximum penalty of $1,000 per instance applies.

FINTRAC will consider mitigating factors in its determination of the penalty. For example, FINTRAC will consider whether very limited financial services (or none) have been provided to the foreign financial institution; or whether ongoing monitoring is in place for all transactions, including those conducted under the correspondent banking relationship. In these cases, FINTRAC may consider a penalty amount that is lower than the maximum prescribed.

4.5 Violations related to ascertaining that a foreign financial institution meets client identification requirements

Regulatory requirements are designed to identify individuals and entities that conduct, control, direct, or are involved in financial transactions in order to remove anonymity. The requirements extend to the clients of foreign financial institutions who can access Canada's financial system through a correspondent banking relationship. REs that allow clients of foreign financial institutions direct access to their accounts must take reasonable measures to find out if the foreign financial institutions apply the requirement to verify client identity and confirm the existence of entities in a manner that is consistent with the Act and its regulations. The REs must also take reasonable measures to find out if the foreign financial institutions agree to provide client identification data upon request.

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
9.4(1)(a)	55.2(a)	Failure of a financial entity that enters into a correspondent banking relationship with a foreign financial institution to take reasonable measures to ascertain whether the institution has met the prescribed requirements	Minor$1-$1,000
9.4(1)(a)	55.2(b)	Failure of a financial entity that enters into a correspondent banking relationship with a foreign financial institution to take reasonable measures to ascertain whether the institution has agreed to provide customer identification data	Minor$1-$1,000

Table 6—Violations related to ascertaining that a foreign financial institution meets client identification requirements

4.5.1 Harm done in the case of violations related to ascertaining that a foreign financial institution meets client identification requirements
Failing to comply with the requirements described above potentially allows the

clients of foreign financial institutions to conduct financial transactions directly through the RE, allowing them to move funds through Canada anonymously. This increases the Canadian financial system's exposure to ML/TF risk, because REs would not be able to identify the true beneficiaries of transactions. This violation contravenes the objectives set out in subparagraph 3(a)(i), paragraphs 3(c) and 40(e) of the Act and its regulations.

4.5.2 Penalty determination for violations related to ascertaining that a foreign financial institution meets client identification requirements

If an RE fails to take reasonable measures to find out if a foreign financial institution has met client identification requirements in keeping with sections 54 and 64 of the PCMLTFR, or if client identification data will be provided upon request, there is a high likelihood that individuals and entities that conduct, control, direct, or are involved in financial transactions in Canada through a correspondent banking relationship would not be identified. Therefore, the prescribed maximum penalty of $1,000 per instance applies.

FINTRAC will consider mitigating factors in its determination of the penalty. This could include when an RE has not transacted with the foreign financial institution or the clients did not have direct access to the accounts under the correspondent banking relationship. Another example of a mitigating factor would be if the foreign financial institution ultimately meets the client identification standards set out in the PCMLTFR through other means or processes.

4.6 Violations related to correspondent banking relationships records

See the guide on harm done assessment for record keeping violations for the harm rationale and penalty calculation for the violations below.

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
9.1(4)(a)	15.1(1) and (2)	Failure of a specified entity entering into a correspondent banking relationship with a prescribed foreign entity to keep a prescribed record.	Minor$1-$1,000

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
9.4(1)(d)	15.1(1)	Failure of a specified entity entering into a correspondent banking relationship with a prescribed foreign entity to set out in writing their obligations and those of the foreign entity in respect of the correspondent banking services	Minor$1-$1,000

Table 7—Violations related to correspondent banking relationships records

5. Violations related to requirements for foreign branches and subsidiaries

This section outlines FINTRAC's approach to the violations related to requirements for foreign branches and subsidiaries, including the harm assessments and penalty calculations.

5.1 Violations related to compliance policies for foreign branches and subsidiaries

The requirement for certain RE sectors to hold their foreign operations to the same compliance standards as those in Canada supports the objective under paragraph 3(a) of the Act to detect, prevent and deter ML/TF. It also fulfills Canada's international commitments to fight transnational crimes as per paragraph 3(c) of the Act.

Provision of the Act	Description	Classification of violation
9.7(1)	Failure to develop policies that establish requirements similar to those of sections 6, 6.1 and 9.6 of the Act and to ensure that foreign branches and foreign subsidiaries apply those policies	Serious$1-100,000
9.7(2)	Applying policies that establish requirements similar to those of sections 6, 6.1 and 9.6 of the Act before they are approved by a board of directors	Serious$1-100,000

Table 8—Violations related to compliance policies for foreign branches and subsidiaries

5.1.1 Harm done in the case of violations related to compliance policies for foreign branches and subsidiaries Failing to develop policies that meet the requirements similar to those of sections 6, 6.1 and 9.6 of the Act leaves foreign branches and foreign subsidiaries vulnerable to ML/TF, ultimately posing a risk to the RE in Canada as well, given the possibility of overlapping services and accounts. This results in the possibility of anonymous transactions being conducted across borders without the accountability and structure to ensure group-wide compliance. Also, the necessary information and records to support client identification, risk assessments, ongoing monitoring, and transaction reporting would be missing. This could ultimately result in suspicious transactions not being detected and reported to FINTRAC to support investigations and prosecutions of ML/TF offences.

5.1.2 Penalty determination for violations related to compliance policies for foreign branches and subsidiaries We use the penalty calculation for compliance program violations to address the failure to develop and apply compliance policies for foreign branches and subsidiaries. Refer to the guide on harm done assessment for compliance program violations for harm standards and penalty determinations.

5.2 Violation related to policies and procedures for the exchange of information between affiliated entities

The Act requires the development and application of policies and procedures on the exchange of information between REs and affiliated domestic or foreign entities for the purpose of detecting and deterring ML/TF offences, and assessing the risk of ML/TF offences. This coordinated approach makes for effective customer due diligence (CDD) and ML/TF risk management.

Provision of the Act	Description	Classification of Violation
9.8(1)	Failure of an entity to develop and apply policies and procedures related to the exchange of information between it and affiliated entities	Serious$1-100,000

Table 9—Violation related to policies and procedures for the exchange of information between affiliated entities

5.2.1 Harm done in the case of a violation related to policies and procedures for the exchange of information between affiliated entities Failing to develop and apply policies and procedures for the exchange of information between affiliated entities could leave Canada's financial system vulnerable to abuse. The objectives set out in the Act are not being met when measures are not taken to detect ML/TF activities (paragraph 3(a)), to assist in fulfilling Canada's international commitments to fight transnational crime (paragraph 3(c)), and to enhance Canada's capacity to take targeted measures to protect its financial system and mitigate the risk of being used for ML/TF activities (paragraph 3(d)).

5.2.2 Penalty determination for a violation related to policies and procedures for the exchange of information between affiliated entities If there are no policies and procedures in place for the exchange of information between affiliated entities, the RE could be vulnerable to ML/TF risks through the affiliated entities' compliance gaps. When the required policies and procedures are non-existent, the maximum prescribed penalty amount of $100,000 applies because this poses the highest level of risk.

FINTRAC will consider mitigating factors when determining the penalty. For example, after considering the completeness of policies and procedures on the exchange of information, the roles and responsibilities for the exchange of information, and the timeliness and frequency of exchanges, it may consider a penalty that is lower than the maximum prescribed.

5.3 Violations related to record keeping and notification for foreign branches and subsidiaries

In order to mitigate the potential ML/TF risks to Canada's financial system stemming from financial interactions with foreign entities, REs must ensure that their overseas operations hold AML/ATF compliance standards similar to those of Canada. However, it is possible that the laws in a foreign jurisdiction may prohibit or conflict with the record keeping, identity verification or other compliance requirements of the Act and its regulations. When this is the case, an exception to applying similar AML/ATF compliance standards is justifiable. REs must keep a record of the facts and reasons why the foreign branch or subsidiary cannot apply a compliance policy. They are also required to notify FINTRAC and their principal supervisory/regulatory body under federal or provincial law of these facts and reasons within a reasonable time. The record of the facts and reasons demonstrates the RE's compliance with the requirement and allows the RE the opportunity to thoroughly assess the types of ML/TF risks associated with its foreign branches/subsidiaries, the reasons why a compliance policy cannot be applied, and the mitigation measures needed. Notifying FINTRAC and other government supervisory/regulatory bodies of the facts and reasons also fulfills the international commitment to support the fight against ML/TF crimes.

Provision of the Act	Description	Classification of Violation
9.7(4)	Failure to keep and retain a record of the fact that a foreign branch or foreign subsidiary cannot apply a policy and of the reasons why it cannot do so or to notify the Centre and the principal supervisory or regulating agency or body within a reasonable time	Minor$1-$1,000

Provision of the Act	Description	Classification of Violation
11.44(2)	Failure to keep and retain a record of the fact that a foreign branch or foreign subsidiary cannot comply with a ministerial directive and of the reasons why it cannot do so or to notify the Centre and the principal supervisory or regulating agency or body within a reasonable time	Serious$1-$100,000

Table 10—Violations related to record keeping and notification for foreign branches and subsidiaries

5.3.1 Harm done in the case of violations related to record keeping and notification for foreign branches and subsidiaries Failing to keep a record of the fact that a foreign branch or subsidiary cannot comply with and AML/ATF policies and the reasons why it cannot do so, and failing to report it to FINTRAC and the supervisory/regulatory body, can result in ML/TF risks and AML/ATF gaps through the RE's operations in foreign jurisdictions. When the non-compliance of a foreign branch or subsidiary is not detected, understood, assessed and mitigated, it presents significant risk. This failure could interfere with Canada's understanding of the ML/TF and compliance risks associated with a foreign jurisdiction and could affect Canada's international commitments to fight against ML/TF.

5.3.2 Penalty determination for violations related to record keeping and notification for foreign branches and subsidiaries FINTRAC has identified four levels of harm related to these violations based on the RE's and Canada's ability to understand, assess and mitigate ML/TF risks related to foreign operations. The above-mentioned penalty ranges ($1 to $1,000 for compliance policy violations, and $1 to $100,000 for Minister's directive violations) are divided into four even intervals to show the various levels of harm. The highest harm category for both violations is assigned the prescribed maximum amounts of $1,000 and $100,000. The lowest of the four levels of harm has a penalty determination of $250 and $25,000. Penalty amounts may be reduced

based on mitigating factors; however, they must be enough to encourage a change in compliance behaviour.

The table below details the levels of harm, the types of non-compliance and the description of harm along with their corresponding penalties.

When deficiencies fall into more than one harm category, the penalty is determined at the highest harm category, and is not cumulative.

Level of harm	Type of non-compliance	Harm description	Penalty (not considering mitigating factors)
Compliance policy:	Minister's directive:		
Level 1	No record of fact and reasons; FINTRAC and supervisor/regulator not notified	Completely impedes Canadian authorities' and the RE's ability to assess the exception and consider associated risks for mitigation measures at both the national and RE level	$1,000
Level 2	Record of facts and reasons exists but FINTRAC and supervisor/regulator are not notified	Impedes all Canadian authorities' ability to assess the exception and consider the associated risks for mitigation measures at a national level.	$750

Level of harm	Type of non-compliance	Harm description	Penalty (not considering mitigating factors)
Level 3	No record of fact and reasons but FINTRAC and supervisor/regulator are notified	Although the proper Canadian authorities are made aware of the exceptions, documentation deficiencies can lead to inaccurate or incomplete ML/TF risk assessments of the exceptions, leading to ineffective measures at the RE level	$500
Level 4	Record of facts and reasons exists; FINTRAC and supervisor/regulator notified but not within a reasonable time	Diminishes the Canadian authorities' ability to assess the exception and consider the associated risks in an efficient manner	$250

Table 11—Levels of harm and penalties for violations related to record keeping and notification for foreign branches and subsidiaries

5.3.3 Level 1 harm—No record of fact and reasons; FINTRAC and supervisor/regulator not notified When an RE makes no effort to understand the facts and reasons why a foreign branch or subsidiary cannot comply with AML/ATF standards similar to those of Canada, does not record those facts and reasons, and fails to notify FINTRAC and its supervisor or regulator; this poses the highest level of risk because the RE is not able to detect, assess and mitigate the ML/TF risk, and Canada cannot evaluate the risk on the regime at large. Therefore, the penalty is determined at the prescribed maximum, $1,000 for compliance policy violations, and $100,000 for a minister's directive violations.

5.3.4 Level 2 harm—Record of facts and reasons exists but FINTRAC and supervisor/regulator are not notified When FINTRAC and other supervisory or regulatory bodies are not notified of the facts and reasons why a foreign branch or subsidiary cannot comply, while mitigation measures may be in place at the RE, partners in Canada's AML/ATF regime would not be aware of the risks, nor would they be able to coordinate their compliance efforts and take measures to mitigate ML/TF risks for Canada. If the foreign compliance exception had regime-wide implications, FINTRAC would not have the opportunity to consider risk mitigation measures with other stakeholders such as the Department of Finance. Therefore, the penalty is set at $750 for compliance policy violations, and $75,000 for minister's directive violations.

5.3.5 Level 3 harm—No record of fact and reasons although FINTRAC and supervisor/regulator are notified If an RE notifies FINTRAC and its principal supervisory or regulatory body but fails to keep a record that contains accurate, complete and up-to-date information on the facts and reasons, the harm done is lesser because the proper government bodies are made aware of the exceptions. However, documentation deficiencies can lead to inaccurate or incomplete ML/TF risk assessments of the exceptions, leading to ineffective measures at the RE level. Therefore, the penalty is set at $500 for compliance policy violations, and $50,000 for ministerial directive violations.

5.3.6 Level 4 harm—Record of facts and reasons exists; FINTRAC and supervisor/regulator notified but not within a reasonable time If a record of the facts and reasons is kept, and FINTRAC and the principal supervisory or regulatory bodies are notified, but not in a timely manner, the efficient use of the information for risk assessment and compliance purposes, at a national level, would be affected. Therefore, the penalty is set at $250 for compliance policy violations, and $25,000 for minister's directive violations.

6. Violations related to including prescribed information in prescribed electronic funds transfers (travel rule)

REs that conduct EFTs in the course of their activities must make sure that each transfer includes the name, address and account number, or other reference number of the requesting client. When an RE receives an EFT in the course of its activities, it must take reasonable measures to ensure that any transfer includes the same information.

Information that identifies the parties to a transaction is essential in establishing the origin and the flow of funds which are needed for analysis, investigations and the prosecution of ML/TF offences. The information can be used by the RE for risk assessment, transaction reporting and other compliance requirements, where applicable.

Provision of the Act	Provision of the PCMLTFR	Description	Classification of Violation
9.5(a)	66.1(1) and (2)	Failure of a prescribed person or entity to include prescribed information in prescribed electronic funds transfers	Minor$1-$1,000
9.5(b)	66.1(1) and (2)	Failure of a prescribed person or entity to take reasonable measures to ensure that any transfer that the person or entity receives includes prescribed information	Minor$1-$1,000

Table 12—Violations related to including prescribed information in prescribed EFTs (travel rule)

6.1 Harm done in the case of violations related to including prescribed information in prescribed EFTs (travel rule)

If the prescribed information is missing from a transfer, the harm is the same as the harm posed by not keeping a record. See the guide on harm done assessment for record keeping violations for the harm rationale.

6.2 Penalty determination for violations related to including prescribed information in prescribed EFTs (travel rule)

The harm of not including prescribed information in a prescribed EFT is the same as the harm posed by not keeping a record, therefore the same penalty applies. See the guide on harm done assessment for record keeping violations for the penalty determination.

7. Violations related to the requirement to assist FINTRAC

This section outlines FINTRAC's approach to the violations related to the requirement to assist FINTRAC in its mandate of ensuring compliance, including the harm assessment and penalty calculation.

7.1 Violations related to the requirement to provide an authorized person with reasonable assistance and information reasonably required, or provide information in accordance with a notice

FINTRAC is mandated to ensure REs' compliance with Parts 1 and 1.1 of the Act. In order to fulfill this mandate, it is essential for FINTRAC to have reasonable assistance from REs and access to reasonably required information when conducting compliance activities, like examinations.

Provision of the Act	Description	Classification of Violation
62(2)	Failure to give reasonable assistance and information reasonably required to an authorized person	Serious$1-$100,000
63.1(2)	Failure to provide, in accordance with a notice, documents or other information reasonably required by an authorized person	Serious$1-$100,000

Table 13—Violations related to the requirement to provide an authorized person with reasonable assistance and information reasonably required, or provide information in accordance with a notice

7.2 Harm done in the case of violations related to the requirement to provide an authorized person with reasonable assistance and information reasonably required, or provide information in accordance with a notice

Failing to give an authorized person reasonable assistance and to provide them with any information with respect to the administration of Part 1 and 1.1 of the Act and its regulations, or in accordance with a served notice, interferes with FINTRAC's compliance activities and its mandate under subsection 40(e) of the Act. These activities include examination planning and outreach. If FINTRAC is unable to ensure compliance, the regime's ability to detect, prevent and deter

ML/TF and to mitigate risk is affected. FINTRAC cannot maintain a database of transaction reports or it cannot ensure the proper client identification and record keeping measures are in place in support of financial intelligence for investigations and prosecutions of ML/TF offences.

7.3 Penalty determination for violations related to the requirement to provide an authorized person with reasonable assistance and information reasonably required, or provide information in accordance with a notice

When an RE does not give reasonable assistance, the information reasonably required, or provide the information reasonably required in accordance with a notice, FINTRAC's ability to effectively and efficiently ensure compliance with the Act and its regulations is affected. This shows an RE's unwillingness to cooperate, or an attempt to operate outside of the Act and its requirements. Therefore, this violation results in the prescribed maximum penalty of $100,000. FINTRAC will consider mitigating factors in its determination of the penalty.# Administrative monetary penalties policy

The purpose of FINTRAC's Administrative monetary penalties (AMPs) program is to encourage future compliance with the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (the Act) and its regulations, and to promote a change in behaviour. The AMP program supports FINTRAC's mandate by providing a measured and proportionate response to particular instances of non-compliance. FINTRAC is committed to working with reporting entities (REs) to help them achieve compliance. AMPs are not issued automatically in response to non-compliance, as typically other compliance actions are taken to change behaviour before a penalty is considered.

Purpose

The purpose of this policy is to provide a framework for the determination of an AMP; and to summarize the principles and guidelines that are used by FINTRAC to issue an AMP.

Our operating principles and framework

The purpose of the AMP program is to support FINTRAC's efforts to ensure compliance with the Act and its regulations by providing a measured response to non-compliance issues. The program's guiding principles are:

Objectivity: FINTRAC officers will conduct themselves professionally during an assessment and in their communications with an RE. FINTRAC officers will make objective assessments based on the facts and circumstances of each case, ensuring fair and reasonable decisions.

Reasonableness: FINTRAC officers will exercise professional judgement when

assessing an RE's compliance with the Act and its regulations. This involves considering the circumstances and all relevant factors prior to considering an AMP.

Transparency: FINTRAC officers will make sure that the expectations about compliance are communicated in a clear manner throughout the assessment process. REs will be provided with FINTRAC's findings and observations, and will be given the opportunity to ask questions and respond to the non-compliance identified before the findings are finalized.

Fairness: An RE has the right to understand the case being made for an AMP, and will have a fair opportunity to respond.

Consistency: FINTRAC officers follow established policies and procedures to make sure that similar REs, with the same types and extent of non-compliance, can expect to be treated in a similar manner.

Documentation: FINTRAC officers will rely on facts and document those facts and any other information to support their analysis and findings.

Background and application

FINTRAC works with businesses and law enforcement to combat money laundering (ML) and terrorist activity financing (TF). By effectively identifying clients and keeping records, REs help deter criminal activity and are able to provide law enforcement with evidence for the investigation and prosecution of ML/TF offenses. By reporting the required financial transactions to FINTRAC, REs are supplying it with the information that it needs to carry out its mandate, support law enforcement partners, and contribute to the protection of the integrity of Canada's financial system and the safety of Canadians.

FINTRAC's compliance framework recognizes that the success of Canada's Anti-Money Laundering / Anti-Terrorist Financing (AML/ATF) regime depends on the concrete application of the regulatory measures designed to detect, prevent and deter ML/TF activity. Our own compliance effort aims to bring awareness and understanding of the requirements under the Act and its regulations, to deter non-compliance, and to assist in the detection of ML/TF in support of the efforts of the police and intelligence communities. FINTRAC's risk-based compliance program includes activities of increasing intensity across a range of options (see Figure 1 below). We focus our efforts on promoting awareness, providing assistance and conducting compliance assessments where they will be most effective, but may enforce penalties in the case of non-compliance.

Figure 1 – FINTRAC compliance activities

The graphic shows the awareness, assistance as well as assessment and enforcement compliance activities from low intensity to high intensity.

Awareness activities include: outreach and compliance assessment reports (CARs).

Assistance activities include: engagement, support, policy interpretations and money services business registry.

Assessment and enforcement activities include: CARs, observation letters, reporting entity validations, reports monitoring, compliance meetings, desk exams, onsite exams, follow-up exams, administrative monetary penalties and non-compliance disclosures.

Assessing non-compliance

In the normal course of our compliance activities, we identify instances of non-compliance with the Act and its regulations. We assess the severity of each non-compliance issue by understanding both the extent and the root cause of the non-compliance. Each non-compliance issue is assessed for its impact on FINTRAC's mandate and on the achievement of the objectives of the Act. To determine a suitable response to address a non-compliance result, we will consider the result in a holistic context, including other factors such as the RE's compliance history.

Addressing non-compliance

Following the completion of a compliance assessment, and depending on the extent of the non-compliance identified, FINTRAC may decide:

1. to take no further action;
2. to conduct follow-up compliance activities;
3. to issue an AMP to encourage a change in behaviour; or
4. to disclose relevant information to law enforcement for investigation and prosecution of non-compliance offences under the Act and its regulations.

Authority to issue an AMP

The following outlines the framework applicable when FINTRAC has decided that an AMP is the most suitable option to address a specific non-compliance result.

FINTRAC may issue an AMP and serve a notice of violation when it has **reasonable grounds to believe** that an RE has violated a requirement of the Act and its regulations.

AMPs are not issued automatically in response to non-compliance. AMPs are one tool that is available to FINTRAC and are used to address repeated non-compliant behaviour. AMPs may also be used when there are significant issues of non-compliance or a high impact on FINTRAC's mandate or on the objectives of the Act and its regulations. An AMP is generally used when other compliance options have failed.

Categories of violations

The Proceeds of Crime (Money Laundering) and Terrorist Financing Administrative Monetary Penalties Regulations (AMP Regulations) list the non-compliance violations that could be the basis of an AMP. The AMP Regulations categorize violations by degree of importance, and assign the following penalty ranges:

Minor violation	$1 to $1,000 per violation
Serious violation	$1 to $100,000 per violation
Very serious violation	$1 to $100,000 per violation for an individual $1 to $500,000 per violation for an entity

Categories of violations

The limits above apply to each violation, and multiple violations can result in a total amount that exceeds these limits.

Criteria for determining an AMP amount

The Act and the AMP Regulations set out three criteria that must be taken into account when determining a penalty amount:

- The purpose of AMPs, which is to encourage compliance, not to punish (non-punitive);
- The harm done by the violation; and
- The RE's history of compliance.

We present the methods that we use to determine the penalty amount, along with the factors that we consider in our assessment when we issue an AMP.

FINTRAC will take a reasonable approach in the calculation of penalty amounts. We consider an AMP to be effective when the penalty amount is proportional to the harm done and prompts a change in behaviour toward future compliance. These amounts are in keeping with the type and extent of the violations, given the circumstances of each case.

The following guidelines are in place as benchmarks to assist FINTRAC officers in the calculation of a penalty amount, while taking into consideration the circumstances of each case. As a result, relevant mitigating factors will be carefully considered at each step and may reduce the actual penalty determined.

Step 1: Harm done assessment FINTRAC defines "harm" as the degree to which a violation interferes with achieving the objectives of the Act (section 3, Act) or with FINTRAC's ability to carry out its mandate (section 40, Act).

The AMP Regulations classify all violations by degree of importance. They also determine the minimum and maximum penalty amounts for each level.

In assessing the harm done by a violation, FINTRAC considers both the potential and the resulting harm. "Resulting harm" means separate violations that come from the original violation. For example, when the compliance policies and procedures do not address how to report large cash transactions, the resulting harm is the unreported large cash transactions.

The first test to assess the harm done when calculating a penalty amount is to determine whether the reporting entity has completely failed to meet a requirement or only in part. For some violations, this is obvious; the requirement was met or it was not met. Other violations require further analysis. For example, when a client is not identified under the prescribed circumstances, the requirement is not met. When compliance policies and procedures are missing a component, the requirement is met in part.

When an RE has completely failed to meet a requirement, the base penalty amount that is typically considered for that violation is the maximum amount set out by the AMP Regulations. This is because completely failing to meet a statutory requirement is what interferes the most with achieving the objectives of the Act and FINTRAC's ability to fulfil its mandate.

When an RE has failed to meet part of a requirement, the base penalty amount determined for each violation depends on the part that is non-compliant and the extent of the failure. The extent of the failure is measured using assessment criteria that have been established based on the level of interference with achieving the objectives of the Act and FINTRAC's mandate.

Step 2: Compliance history and non-punitive adjustment The second step in a penalty calculation looks at both the compliance history of the RE and the AMP's purpose, which is to encourage compliance, not to punish (non-punitive).

FINTRAC adjusts the penalty amount for each violation (determined in Step 1 above), based on whether or not the RE has previously been levied an AMP for the violation.

For a first-time violation, the penalty is typically reduced by two-thirds. For a violation occurring a second time (meaning that the RE had been penalized for this very same violation on a previous occasion), the penalty is typically reduced by one-third. For violations occurring a third time or more (again, meaning that the RE had been penalized for the same violation on two or more previous occasions), the full base penalty amount will typically be applied.

AMP program – roles and responsibilities within FINTRAC

FINTRAC's AMP program is centralized at our headquarters in Ottawa. This helps to ensure policies and processes are applied consistently across the country and to maintain the required separation of duties between compliance assessment such as compliance examinations and enforcement. This approach also

helps us monitor our program's effectiveness and allows us to quickly make policy and process improvements at the national level.

Following a compliance examination by FINTRAC regional offices located in Vancouver, Montreal and Toronto, we will review the findings to determine the most appropriate action to address the non-compliance. If the deficiencies and non-compliant behaviour justify an AMP consideration, the relevant regional office will make a recommendation, including the reasons, to headquarters. Upon receipt of the recommendation, headquarters undertakes an independent assessment of the findings and related information to determine whether we will proceed with an AMP.

AMP process

The AMP process begins with the issuance of a notice of violation and continues as outlined below:

Notice of violation

An RE subject to an AMP will receive a notice of violation that will include the following:

- The name and address of the RE that is subject to the AMP;
- The penalty amount;
- Payment instructions;
- Information on the right to make written representations to FINTRAC's Director and Chief Executive Officer (CEO), up to 30 days after receiving the notice of violation;
- Instructions on how to make representations to FINTRAC's Director and CEO, and where to obtain additional information on the AMP program;
- A list of the violations committed which will include the related legislative and regulatory provisions;
- The details of the penalty calculation, including the factors considered and the reasons; and
- A list of all the instances of the committed violations, including relevant references such as account numbers, transaction numbers, report numbers, etc.

A notice of violation must be issued no more than 2 years from the date when the non-compliance became known to FINTRAC.

In some cases, FINTRAC may exercise its discretion to offer to enter into a compliance agreement with the RE, which will include specific terms and conditions.

Payment of penalty

Upon receipt of a notice of violation, a person or entity can pay the penalty by completing the remittance form and submitting it with the payment in Canadian funds to:

FINTRAC

Finance Unit

24th Floor, 234 Laurier Avenue West

Ottawa, ON K1P 1H7

All payments of penalty amounts are to be made payable to the Receiver General for Canada. Payments can be made in the form of a certified cheque, money order, or bank draft.

If an RE pays the penalty indicated in the notice of violation, the RE is deemed to have committed the violations specified, and the AMP process ends.

Representations to FINTRAC's Director and CEO

An RE may request a review of a notice of violation. This can be done by making written representations on the violations or the penalty or both at the same time, to the Director and CEO of FINTRAC, within 30 days of receiving the notice of violation.

If an RE requests a review, FINTRAC's Director and CEO will decide on the balance of probabilities whether the RE committed the violation or not; and may impose the penalty proposed in the notice of violation, a lesser penalty or no penalty. A notice of decision will be issued to communicate the Director and CEO's decision and the reasons behind it.

Failure to pay or make representations and notice of penalty

If you receive a notice of violation and do not pay or make representations to FINTRAC's Director and CEO within 30 days, the AMP process will end, the violations will be upheld and a notice of penalty will be issued.

Notice of decision and right of appeal

An RE that receives a notice of decision from FINTRAC's Director and CEO has 30 days to exercise its right of appeal to the Federal Court of Canada.

The AMP process ends when an RE pays the penalty imposed in the notice of decision, or does not appeal the Director and CEO's decision within 30 days.

Should the Director and CEO not issue a notice of decision within 90 days of receiving your representation for review, you may appeal the proposed penalty in Federal Court within 30 days.

Federal Courts

The Federal Courts have the power to confirm, set aside or change a notice of decision issued by FINTRAC's Director and CEO. As long as the AMP is before the Federal Court, the Federal Court of Appeal, or the Supreme Court of Canada, the AMP process is considered to be ongoing.

Public notice

FINTRAC must make public, as soon as feasible, the name of the RE, the nature of the violation or default, and the amount of the penalty imposed in the following cases:

- An RE pays the penalty issued in a notice of violation.
- An RE neither pays the penalty issued in a notice of violation nor makes representations to FINTRAC's Director and Chief Executive Officer.
- An RE receives a notice of decision indicating that a violation has been committed.
- An RE enters into a compliance agreement with FINTRAC.
- An RE does not comply with a compliance agreement.

When publicizing the nature of the violation, FINTRAC may also include the reasons for its decision, including the relevant facts, analysis and considerations that formed part of the decision.

You can review the AMPs imposed by FINTRAC on the Public notice page.

Collection of penalties

The penalty amount is due 30 days after the notice of violation or notice of decision is received. Interest would begin to accrue on the day after the penalty was due. Any penalty that becomes payable is an outstanding debt to the Crown. FINTRAC will pursue outstanding AMP payments.# Guidance glossary

The glossary defines certain terms used throughout FINTRAC's guidance.

Definitions

Accountant

A chartered accountant, a certified general accountant, a certified management accountant or, if applicable, a chartered professional accountant. (comptable)

Accounting firm

An entity that is engaged in the business of providing accounting services to the public and has at least one partner, employee or administrator that is an accountant. (cabinet d'expertise comptable)

Act

The Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA). (la Loi)

Administrative monetary penalties (AMPs)

Civil penalties that may be issued to reporting entities by FINTRAC for non-compliance with the PCMLTFA and associated Regulations. (pénalité administrative pécuniaire [PAP])

Affiliate

An entity is affiliated with another entity if one of them is wholly owned by the other, if both are wholly owned by the same entity or if their financial statements are consolidated. (entité du même groupe)

Annuity

Has the same meaning as in subsection 248(1) of the Income Tax Act. (rente)

Armoured cars

Persons or entities that are engaged in the business of transporting currency, money orders, traveller's cheques or other similar negotiable instruments. (Véhicules blindés)

As soon as practicable

A time period that falls in-between immediately and as soon as possible, within which a suspicious transaction report (STR) must be submitted to FINTRAC. The completion and submission of the STR should take priority over other tasks. In this context, the report must be completed promptly, taking into account the facts and circumstances of the situation. While some delay is permitted, it must have a reasonable explanation. (aussitôt que possible)

Attempted transaction

Occurs when an individual or entity starts to conduct a transaction that is not completed. For example, a client or a potential client walks away from conducting a $10,000 cash deposit. (opération tentée)

Authentic

In respect of verifying identity, means genuine and having the character of an original, credible, and reliable document or record. (authentique)

Authorized person

A person who is authorized under subsection 45(2). (personne autorisée)

Authorized user

A person who is authorized by a holder of a prepaid payment product account to have electronic access to funds or virtual currency available in the account by means of a prepaid payment product that is connected to it. (utilisateur autorisé)

Beneficial owner(s)

Beneficial owners are the individuals who are the trustees, and known beneficiaries and settlors of a trust, or who directly or indirectly own or control 25% or more of i) the shares of a corporation or ii) an entity other than a corporation or trust, such as a partnership. The ultimate beneficial owner(s) cannot be another corporation or entity; it must be the actual individual(s) who owns or controls the entity. (bénéficiaire effectif)

Beneficiary

A beneficiary is the individual or entity that will benefit from a transaction or to which the final remittance is made. (bénéficiaire)

Branch

A branch is a part of your business at a distinct location other than your main office. (succursale)

British Columbia notary corporation

An entity that carries on the business of providing notary services to the public in British Columbia in accordance with the Notaries Act, R.S.B.C. 1996, c. 334. (société de notaires de la Colombie-Britannique)

British Columbia notary public

A person who is a member of the Society of Notaries Public of British Columbia. (notaire public de la Colombie-Britannique)

Cash

Coins referred to in section 7 of the Currency Act, notes issued by the Bank of Canada under the Bank of Canada Act that are intended for circulation in Canada or coins or bank notes of countries other than Canada. (espèces)

Casino

A government, organization, board or operator that is referred to in any of paragraphs 5(k) to (k.3) of the Act. (casino)

Certified translator

An individual that holds the title of professional certified translator granted by a Canadian provincial or territorial association or body that is competent under Canadian provincial or territorial law to issue such certification. (traducteur agréé)

Clarification request

A clarification request is a method used to communicate with money services businesses (MSBs) or foreign money services businesses (FMSBs) when FINTRAC needs more information about their registration form. This request is usually sent by email. (demande de précisions)

Client

A person or entity that engages in a financial transaction with another person or entity. (client)

Client identification information

The identifying information that you have obtained on your clients, such as name, address, telephone number, occupation or nature of principal business, and date of birth for an individual. (renseignements d'identification du client)

Competent authority

For the purpose of the criminal record check submitted with an application for registration, a competent authority is any person or organization that has the legally delegated or invested authority, capacity, or power to issue criminal record checks. (autorité compétente)

Completed transaction

Is a transaction conducted by a person or entity, that is completed and results in the movement of funds, virtual currency, or the purchase or sale of an asset. (opération effectuée)

Completing action

With respect to a reportable transaction, information related to the instructions provided by the person or entity making the request to the reporting entity to

complete a transaction. For example, an individual arrives at a bank and requests to purchase a bank draft. The completing action is the details of how the reporting entity fulfilled the person or entity's instructions which led to the transaction being completed. This includes what the funds or virtual currency initially brought to the reporting entity was used for (see "disposition"). A transaction may have one or more completing actions depending on the instructions provided by the person or entity. (action d'achèvement)

Compliance officer

The individual, with the necessary authority, that you appoint to be responsible for the implementation of your compliance program. (agent de conformité)

Compliance policies and procedures

Written methodology outlining the obligations applicable to your business under the PCMLTFA and its associated Regulations and the corresponding processes and controls you put in place to address your obligations. (politiques et procédures de conformité)

Compliance program

All elements (compliance officer, policies and procedures, risk assessment, training program, effectiveness review) that you, as a reporting entity, are legally required to have under the PCMLTFA and its associated Regulations to ensure that you meet all your obligations. (programme de conformité)

Context

Clarifies a set of circumstances or provides an explanation of a situation or financial transaction that can be understood and assessed. (contexte)

Correspondent banking relationship

A relationship created by an agreement or arrangement under which an entity referred to in any of paragraphs 5(a), (b), (d),(e) and (e.1) or an entity that is referred to in section 5 and that is prescribed undertakes to provide to a prescribed foreign entity prescribed services or international electronic funds transfers, cash management or cheque clearing services. (relation de correspondant bancaire)

Country of residence

The country where an individual has lived continuously for 12 months or more. The individual must have a dwelling in the country concerned. For greater certainty, a person only has one country of residence no matter how many dwelling places they may have, inside or outside of that country. (pays de résidence)

Credit card acquiring business

A credit card acquiring business is a financial entity that has an agreement with a merchant to provide the following services:

- enabling a merchant to accept credit card payments by cardholders for goods and services and to receive payments for credit card purchases;
- processing services, payment settlements and providing point-of-sale equipment (such as computer terminals); and
- providing other ancillary services to the merchant.

Credit union central

A central cooperative credit society, as defined in section 2 of the Cooperative Credit Associations Act, or a credit union central or a federation of credit unions or caisses populaires that is regulated by a provincial Act other than one enacted by the legislature of Quebec. (centrale de caisses de crédit)

Crowdfunding platform

A website or an application or other software that is used to raise funds or virtual currency through donations. (plateforme de sociofinancement)

Crowdfunding platform services

The provision and maintenance of a crowdfunding platform for use by other persons or entities to raise funds or virtual currency for themselves or for persons or entities specified by them. (services de plateforme de sociofinancement)

Current

In respect of a document or source of information that is used to verify identity, is up to date, and, in the case of a government-issued photo identification document, must not have been expired when the ID was verified. (à jour)

Dealer in precious metals and stones

A person or entity that, in the course of their business activities, buys or sells precious metals, precious stones or jewellery. It includes a department or an agent of His Majesty in right of Canada or an agent or mandatary of His Majesty in right of a province when the department or the agent or mandatary carries out the activity, referred to in subsection 65(1), of selling precious metals to the public. (négociant en métaux précieux et pierres précieuses)

Deferred profit sharing plan

Has the same meaning as in subsection 248(1) of the Income Tax Act. (régime de participation différée aux bénéfices)

Deposit slip

A record that sets out:

1. (a) the date of the deposit;
2. (b) the name of the person or entity that makes the deposit;
3. (c) the amount of the deposit and of any part of it that is made in cash;
4. (d) the method by which the deposit is made; and
5. (e) the number of the account into which the deposit is made and the name of each account holder.

(relevé de dépôt)

Directing services

A business is directing services at persons or entities in Canada if at least one of the following applies:

- The business's marketing or advertising is directed at persons or entities located in Canada;
- The business operates a ".ca" domain name; or,
- The business is listed in a Canadian business directory.

Additional criteria may be considered, such as if the business describes its services being offered in Canada or actively seeks feedback from persons or entities in Canada. (diriger des services)

Distributed ledger

For the purpose of section 151 of the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFR), a digital ledger that is maintained by multiple persons or entities and that can only be modified by a consensus of those persons or entities. (registres distribués)

Disposition

With respect to a reportable transaction, the disposition is what the funds or virtual currency was used for. For example, an individual arrives at a bank with cash and purchases a bank draft. The disposition is the purchase of the bank draft. (répartition)

Electronic funds transfer

The transmission—by any electronic, magnetic or optical means—of instructions for the transfer of funds, including a transmission of instructions that is initiated and finally received by the same person or entity. In the case of SWIFT messages,

only SWIFT MT-103 messages and their equivalent are included. It does not include a transmission or instructions for the transfer of funds:

1. (a) that involves the beneficiary withdrawing cash from their account;
2. (b) that is carried out by means of a direct deposit or pre-authorized debit;
3. (c) that is carried out by cheque imaging and presentment
4. (d) that is both initiated and finally received by persons or entities that are acting to clear or settle payment obligations between themselves; or
5. (e) that is initiated or finally received by a person or entity referred to in paragraphs 5(a) to (h.1) of the Act for the purpose of internal treasury management, including the management of their financial assets and liabilities, if one of the parties to the transaction is a subsidiary of the other or if they are subsidiaries of the same corporation.

(télévirement)

Employees profit sharing plan

Has the same meaning as in subsection 248(1) of the Income Tax Act. (régime de participation des employés aux bénéfices)

Entity

A body corporate, a trust, a partnership, a fund or an unincorporated association or organization. (entité)

Facts

Actual events, actions, occurrences or elements that exist or are known to have happened or existed. Facts are not opinions. For example, facts surrounding a transaction or multiple transactions could include the date, time, location, amount or type of transaction or could include the account details, particular business lines, or the client's financial history. (faits)

Family member

For the purposes of subsection 9.3(1) of the Act, a prescribed family member of a politically exposed foreign person, a politically exposed domestic person or a head of an international organization is:

1. (a) their spouse or common-law partner;
2. (b) their child;
3. (c) their mother or father;

4. (d) the mother or father of their spouse or common-law partner; or

5. (e) a child of their mother or father.

(membre de la famille)

Fiat currency

A currency that is issued by a country and is designated as legal tender in that country. (monnaie fiduciaire)

Final receipt

In respect of an electronic funds transfer, means the receipt of the instructions by the person or entity that is to make the remittance to a beneficiary. (destinataire)

Financial entity

Means:

1. (a) an entity that is referred to in any of paragraphs 5(a), (b) and (d) to (f) of the Act;

2. (b) a financial services cooperative;

3. (c) a life insurance company, or an entity that is a life insurance broker or agent, in respect of loans or prepaid payment products that it offers to the public and accounts that it maintains with respect to those loans or prepaid payment products, other than:

4. (i) loans that are made by the insurer to a policy holder if the insured person has a terminal illness that significantly reduces their life expectancy and the loan is secured by the value of an insurance policy;

5. (ii) loans that are made by the insurer to the policy holder for the sole purpose of funding the life insurance policy; and

6. (iii) advance payments to which the policy holder is entitles that are made to them by the insurer;

7. (d) a credit union central when it offers financial services to a person, or to an entity that is not a member of that credit union central; and

8. (e) a department, or an entity that is an agent of His Majesty in right of Canada or an agent or mandatary of His Majesty in right of a province, when it carries out an activity referred to in section 76.

(entité financière)

Financial Action Task Force

The Financial Action Task Force on Money Laundering established in 1989. (Groupe d'action financière)

Financial services cooperative

A financial services cooperative that is regulated by an Act respecting financial services cooperatives, CQLR, c. C-67.3 or the Act respecting the Mouvement Desjardins, S.Q. 2000, c. 77, other than a caisse populaire. (coopérative de services financiers)

Foreign currency

A fiat currency that is issued by a country other than Canada. (devise)

Foreign currency exchange transaction

An exchange, at the request of another person or entity, of one fiat currency for another. (opération de change en devise)

Foreign currency exchange transaction ticket

A record respecting a foreign currency exchange transaction—including an entry in a transaction register—that sets out:

1. (a) the date of the transaction;
2. (b) in the case of a transaction of $3,000 or more, the name and address of the person or entity that requests the exchange, the nature of their principal business or their occupation and, in the case of a person, their date of birth;
3. (c) the type and amount of each of the fiat currencies involved in the payment made and received by the person or entity that requests the exchange;
4. (d) the method by which the payment is made and received;
5. (e) the exchange rates used and their source;
6. (f) the number of every account that is affected by the transaction, the type of account and the name of each account holder; and
7. (g) every reference number that is connected to the transaction and has a function equivalent to that of an account number.

(fiche d'opération de change en devise)

Foreign money services business

Persons and entities that do not have a place of business in Canada, that are engaged in the business of providing at least one of the following services that is directed at persons or entities in Canada, and that provide those services to their clients in Canada:

1. (i) foreign exchange dealing,
2. (ii) remitting funds or transmitting funds by any means or through any person, entity or electronic funds transfer network,
3. (iii) issuing or redeeming money orders, traveller's cheques or other similar negotiable instruments except for cheques payable to a named person or entity,
4. (iv) dealing in virtual currencies, or
5. (v) any prescribed service.

(entreprise de services monétaires étrangère)

Foreign state

Except for the purposes of Part 2, means a country other than Canada and includes any political subdivision or territory of a foreign state. (État étranger)

Funds

Means:

1. (a) cash and other fiat currencies, and securities, negotiable instruments or other financial instruments that indicate a title or right to or interest in them; or
2. (b) a private key of a cryptographic system that enables a person or entity to have access to a fiat currency other than cash.

For greater certainty, it does not include virtual currency. (fonds)

Head of an international organization

A person who, at a given time, holds—or has held within a prescribed period before that time—the office or position of head of

1. a) an international organization that is established by the governments of states;
2. b) an institution of an organization referred to in paragraph (a); or
3. c) an international sports organization.

Immediately

In respect of submitting a Terrorist Property Report (TPR), the time period within which a TPR must be submitted, which does not allow for any delay prior to submission. (immédiatement)

Information record

A record that sets out the name and address of a person or entity and:

1. (a) in the case of a person, their date of birth and the nature of their principal business or their occupation; and
2. (b) in the case of an entity, the nature of its principal business.

(dossier de renseignements)

Initiation

In respect of an electronic funds transfer, means the first transmission of the instructions for the transfer of funds. (amorcer)

Institutional trust

For the purpose of section 15 of the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFR), means a trust that is established by a corporation or other entity for a particular business purpose and includes a pension plan trust, a pension master trust, a supplemental pension plan trust, a mutual fund trust, a pooled fund trust, a registered retirement savings plan trust, a registered retirement income fund trust, a registered education savings plan trust, a group registered retirement savings plan trust, a deferred profit sharing plan trust, an employee profit sharing plan trust, a retirement compensation arrangement trust, an employee savings plan trust, a health and welfare trust, an unemployment benefit plan trust, a foreign insurance company trust, a foreign reinsurance trust, a reinsurance trust, a real estate investment trust, an environmental trust and a trust established in respect of endowment, a foundation or a registered charity. (fiducie institutionnelle)

International electronic funds transfer

An electronic funds transfer other than for the transfer of funds within Canada. (télévirement international)

Inter vivos trust

A personal trust, other than a trust created by will. (fiducie entre vifs)

Jewellery

Objects that are made of gold, silver, palladium, platinum, pearls or precious stones and that are intended to be worn as a personal adornment. (bijou)

Large cash transaction record

A record that indicates the receipt of an amount of $10,000 or more in cash in a single transaction and that contains the following information:

1. (a) the date of the receipt;
2. (b) if the amount is received for deposit into an account, the number of the account, the name of each account holder and the time of the deposit or an indication that the deposit is made in a night deposit box outside the recipient's normal business hours;
3. (c) the name and address of every other person or entity that is involved in the transaction, the nature of their principal business or their occupation and, in the case of a person, their date of birth;
4. (d) the type and amount of each fiat currency involved in the receipt;
5. (e) the method by which the cash is received;
6. (f) if applicable, the exchange rates used and their source;
7. (g) the number of every other account that is affected by the transaction, the type of account and the name of each account holder
8. (h) every reference number that is connected to the transaction and has a function equivalent to that of an account number;
9. (i) the purpose of the transaction;
10. (j) the following details of the remittance of, or in exchange for, the cash received:
    1. (i) the method of remittance;
    2. (ii) if the remittance is in funds, the type and amount of each type of funds involved;
    3. (iii) if the remittance is not in funds, the type of remittance and its value, if different from the amount of cash received; and
    4. (iv) the name of every person or entity involved in the remittance and their account number or policy number or, if they have no account number or policy number, their identifying number; and
11. (k) if the amount is received by a dealer in precious metals and precious stones for the sale of precious metals, precious stones or jewellery:
    1. (i) the type of precious metals, precious stones or jewellery;

2. (ii) the value of the precious metals, precious stones or jewellery, if different from the amount of cash received, and

3. (iii) the wholesale value of the precious metals, precious stones or jewellery.

Large virtual currency transaction record

A record that indicates the receipt of an amount of $10,000 or more in virtual currency in a single transaction and that contains the following information:

1. (a) the date of the receipt;

2. (b) if the amount is received for deposit into an account, the name of each account holder;

3. (c) the name and address of every other person or entity that is involved in the transaction, the nature of their principal business or their occupation and, in the case of a person, their date of birth;

4. (d) the type and amount of each virtual currency involved in the receipt;

5. (e) the exchange rates used and their source;

6. (f) the number of every other account that is affected by the transaction, the type of account and the name of each account holder;

7. (g) every reference number that is connected to the transaction and has a function equivalent to that of an account number;

8. (h) every transaction identifier, including the sending and receiving addresses; and

9. (i) if the amount is received by a dealer in precious metals and precious stones for the sale of precious metals, precious stones or jewellery:

10. (i) the type of precious metals, precious stones or jewellery;

11. (ii) the value of the precious metals, precious stones or jewellery, if different from the amount of virtual currency received; and

12. (iii) the wholesale value of the precious metals, precious stones or jewellery.

Life insurance broker or agent

A person or entity that is authorized under provincial legislation to carry on the business of arranging contracts of life insurance. (représentant d'assurance-vie)

Life insurance company

A life company or foreign life company to which the Insurance Companies Act applies or a life insurance company regulated by a provincial Act. (société

d'assurance-vie)

Listed person

Has the same meaning as in section 1 of the Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism. (personne inscrite)

Managing general agents (MGAs)

Life insurance brokers or agents that act as facilitators between other life insurance brokers or agents and life insurance companies. MGAs typically offer services to assist with insurance agents contracting and commission payments, facilitate the flow of information between insurer and agent, and provide training to, and compliance oversight of, insurance agents. (agent général de gestion)

Mandatary

A person who acts, under a mandate or agreement, for another person or entity. (mandataire)

Marketing or advertising

When a person or entity uses promotional materials such as advertisements, graphics for websites or billboards, etc., with the intent to promote money services business (MSB) services and to acquire business from persons or entities in Canada. (marketing ou publicité)

Minister

In relation to sections 24.1 to 39, the Minister of Public Safety and Emergency Preparedness and, in relation to any other provision of this Act, the Minister of Finance. (ministre)

Money laundering offence

An offence under subsection 462.31(1) of the Criminal Code. The United Nations defines money laundering as "any act or attempted act to disguise the source of money or assets derived from criminal activity." Essentially, money laundering is the process whereby "dirty money"—produced through criminal activity—is transformed into "clean money," the criminal origin of which is difficult to trace. (infraction de recyclage des produits de la criminalité)

Money laundering and terrorist financing indicators (ML/TF indicators)

Potential red flags that could initiate suspicion or indicate that something may be unusual in the absence of a reasonable explanation.

Money services business

A person or entity that has a place of business in Canada and that is engaged in the business of providing at least one of the following services:

1. (i) foreign exchange dealing,
2. (ii) remitting funds or transmitting funds by any means or through any person, entity or electronic funds transfer network,
3. (iii) issuing or redeeming money orders, traveller's cheques or other similar negotiable instruments except for cheques payable to a named person or entity,
4. (iv) dealing in virtual currencies, or
5. (v) any prescribed service.

(entreprise de services monétaires)

Money services business agent

An individual or entity authorized to deliver services on behalf of a money services business (MSB). It is not an MSB branch. (mandataire d'une entreprise de services monétaires)

Mortgage administrator

A person or entity, other than a financial entity, that is engaged in the business of servicing mortgage agreements on real property or hypothec agreements on immovables on behalf of a lender. (administrateur hypothécaire)

Mortgage broker

A person or entity that is authorized under provincial legislation to act as an intermediary between a lender and a borrower with respect to loans secured by mortgages on real property or hypothecs on immovables. (courtier hypothécaire)

Mortgage lender

A person or entity, other than a financial entity, that is engaged in the business of providing loans secured by mortgages on real property or hypothecs on immovables. (prêteur hypothécaire)

Nature of principal business

An entity's type or field of business. Also applies to an individual in the case of a sole proprietorship. (nature de l'entreprise principale)

New developments

Changes to the structure or operations of a business when new services, activities, or locations are put in place. For example, changes to a business model or business restructuring. (nouveaux développements)

New technologies

The adoption of a technology that is new to a business. For example, when a business adopts new systems or software such as transaction monitoring systems or client onboarding and identification tools. (nouvelles technologies)

No apparent reason

There is no clear explanation to account for suspicious behaviour or information. (sans raison apparente)

Occupation

The job or profession of an individual. (profession ou métier)

Person

An individual. (personne)

Person authorized to give instructions

In respect of an account, means a person who is authorized to instruct on the account or make changes to the account, such as modifying the account type, updating the account contact details, and in the case of a credit card account, requesting a limit increase or decrease, or adding or removing card holders. A person who is only able to conduct transactions on the account is not considered a person authorized to give instructions. (personne habilitée à donner des instructions)

Politically exposed domestic person

A person who, at a given time, holds—or has held within a prescribed period before that time—one of the offices or positions referred to in any of paragraphs (a) and (c) to (j) in or on behalf of the federal government or a provincial government or any of the offices or positions referred to in paragraphs (b) and (k):

1. (a) Governor General, lieutenant governor or head of government;
2. (b) member of the Senate or House of Commons or member of a legislature of a province;
3. (c) deputy minister or equivalent rank;

4. (d) ambassador, or attaché or counsellor of an ambassador;
5. (e) military officer with a rank of general or above;
6. (f) president of a corporation that is wholly owned directly by His Majesty in right of Canada or a province;
7. (g) head of a government agency;
8. (h) judge of an appellate court in a province, the Federal Court of Appeal or the Supreme Court of Canada;
9. (i) leader or president of a political party represented in a legislature;
10. (j) holder of any prescribed office or position; or
11. (k) mayor, reeve or other similar chief officer of a municipal or local government.

(national politiquement vulnérable)

Politically exposed foreign person

A person who holds or has held one of the following offices or positions in or on behalf of a foreign state:

1. (a) head of state or head of government;
2. (b) member of the executive council of government or member of a legislature;
3. (c) deputy minister or equivalent rank;
4. (d) ambassador, or attaché or counsellor of an ambassador;
5. (e) military officer with a rank of general or above;
6. (f) president of a state-owned company or a state-owned bank;
7. (g) head of a government agency;
8. (h) judge of a supreme court, constitutional court or other court of last resort;
9. (i) leader or president of a political party represented in a legislature; or
10. (j) holder of any prescribed office or position.

(étranger politiquement vulnérable)

Possibility

In regards to completing a suspicious transaction report (STR), the likelihood that a transaction may be related to a money laundering/terrorist financing (ML/TF) offence. For example, based on your assessment of facts, context and ML/TF indicators you have reasonable grounds to suspect that a transaction

is related to the commission or attempted commission of an ML/TF offence. (possibilité)

Precious metal

Gold, silver, palladium or platinum in the form of coins, bars, ingots or granules or in any other similar form. (métal précieux)

Precious stones

Diamonds, sapphires, emeralds, tanzanite, rubies or alexandrite. (pierre précieuse)

Prepaid payment product

A product that is issued by a financial entity and that enables a person or entity to engage in a transaction by giving them electronic access to funds or virtual currency paid to a prepaid payment product account held with the financial entity in advance of the transaction. It excludes a product that:

1. (a) enables a person or entity to access a credit or debit account or one that is issued for use only with particular merchants; or
2. (b) is issued for single use for the purposes of a retail rebate program.

(produit de paiement prépayé)

Prepaid payment product account

An account – other than an account to which only a public body or, if doing so for the purposes of humanitarian aid, a registered charity as defined in subsection 248(1) of the Income Tax Act, can add funds or virtual currency – that is connected to a prepaid payment product and that permits:

1. (a) funds or virtual currency that total $1,000 or more to be added to the account within a 24-hour period; or
2. (b) a balance of funds or virtual currency of $1,000 or more to be maintained.

(compte de produit de paiement prépayé)

Prescribed

Prescribed by regulations made by the Governor in Council. (Version anglaise seulement)

Probability

The likelihood in regards to completing a suspicious transaction report (STR) that a financial transaction is related to a money laundering/terrorist financing (ML/TF) offence. For example, based on facts, having reasonable grounds to believe that a transaction is probably related to the commission or attempted commission of an ML/TF offence. (probabilité)

Production order

A judicial order that compels a person or entity to disclose records to peace officers or public officers. (ordonnance de communication)

Public body

Means

1. (a) a department or an agent of His Majesty in right of Canada or an agent or mandatary of His Majesty in right of a province;
2. (b) an incorporated city or town, village, metropolitan authority, township, district, county, rural municipality or other incorporated municipal body in Canada or an agent or mandatary in Canada of any of them; and
3. (c) an organization that operates a public hospital and that is designated by the Minister of National Revenue as a hospital authority under the Excise Tax Act, or an agent or mandatary of such an organization.

(organisme public)

Real estate broker or sales representative

A person or entity that is authorized under provincial legislation to act as an agent or mandatary for purchasers or vendors in respect of the purchase or sale of real property or immovables. (courtier ou agent immobilier)

Real estate developer

A person or entity that, in any calendar year after 2007, has sold to the public, other than in the capacity of a real estate broker or sales representative:

1. (a) five or more new houses or condominium units;
2. (b) one or more new commercial or industrial buildings; or
3. (c) one or more new multi-unit residential buildings each of which contains five or more residential units, or two or more new multi-unit residential buildings that together contain five or more residential units.

(promoteur immobilier)

Reasonable measures

Steps taken to achieve a desired outcome, even if they do not result in the desired outcome. For example, this can include doing one or more of the following:

- asking the client,
- conducting open source searches,
- retrieving information already available, including information held in non-digital formats, or
- consulting commercially available information.

(mesures raisonnables)

Receipt of funds record

A record that indicates the receipt of an amount of funds and that contains the following information:

1. (a) the date of the receipt;
2. (b) if the amount is received from a person, their name, address and date of birth and the nature of their principal business or their occupation;
3. (c) if the amount is received from or on behalf of an entity, the entity's name and address and the nature of their principal business;
4. (d) the amount of the funds received and of any part of the funds that is received in cash;
5. (e) the method by which the amount is received;
6. (f) the type and amount of each fiat currency involved in the receipt;
7. (g) if applicable, the exchange rates used and their source;
8. (h) the number of every account that is affected by the transaction in which the receipt occurs, the type of account and the name of each account holder;
9. (i) the name and address of every other person or entity that is involved in the transaction, the nature of their principal business or their occupation and, in the case of a person, their date of birth;
10. (j) every reference number that is connected to the transaction and has a function equivalent to that of an account number; and
11. (k) the purpose of the transaction.

(relevé de réception de fonds)

Registered pension plan

Has the same meaning as in subsection 248(1) of the Income Tax Act. (régime de pension agréé)

Registered retirement income fund

Has the same meaning as in subsection 248(1) of the Income Tax Act. (fonds enregistré de revenu de retraite)

Reliable

In respect of information that is used to verify identity, means that the source is well known, reputable, and is considered one that you trust to verify the identity of the client. (fiable)

Representative for service

An individual in Canada that has been appointed by a person or entity that is a foreign money services business (FMSB), pursuant to the PCMLTFA, to receive notices and documents on behalf of the FMSB. (représentant du service)

Risk assessment

The review and documentation of potential money laundering/terrorist financing risks in order to help a business establish policies, procedures and controls to detect and mitigate these risks and their impact. (évaluation des risques)

Sanctions evasion

Sanctions evasion offence means an offence arising from the contravention of a restriction or prohibition established by an order or a regulation made under the United Nations Act, the Special Economic Measures Act or the Justice for Victims of Corrupt Foreign Officials Act (Sergei Magnitsky Law). (contournement des sanctions)

Securities dealer

A person or entity that is referred to in paragraph 5(g) of the Act. (courtier en valeurs mobilières)

Senior officer

In respect of an entity, means:

1. (a) a director of the entity who is one of its full-time employees;

2. (b) the entity's chief executive officer, chief operating officer, president, secretary, treasurer, controller, chief financial officer, chief accountant, chief auditor or chief actuary, or any person who performs any of those functions; or

3. (c) any other officer who reports directly to the entity's board of directors, chief executive officer or chief operating officer.

(cadre dirigeant)

Service agreement

An agreement between a money services business (MSB) and an organization according to which the MSB will provide any of the following MSB services on an ongoing basis:

- money transfers;
- foreign currency exchange;
- issuing or redeeming money orders, traveller's cheques or anything similar; or
- dealing in virtual currencies.
- Crowdfunding
- Armoured Cars

(accord de relation commerciale)

Settlor

A settlor is an individual or entity that creates a trust with a written trust declaration. The settlor ensures that legal responsibility for the trust is given to a trustee and that the trustee is provided with a trust instrument document that explains how the trust is to be used for the beneficiaries. A settlor includes any individual or entity that contributes financially to that trust, either directly or indirectly. (constituant)

Shell bank

A foreign financial institution that:

1. (a) does not have a place of business that:

2. (i) is located at a fixed address—where it employs one or more persons on a full-time basis and maintains operating records related to its banking activities—in a country in which it is authorized to conduct banking activities; and

3. (ii) is subject to inspection by the regulatory authority that licensed it to conduct banking activities; and

4. (b) is not controlled by, or under common control with, a depository institution, credit union or foreign financial institution that maintains

a place of business referred to in paragraph (a) in Canada or in a foreign country.

(banque fictive)

Signature

Includes an electronic signature or other information in electronic form that is created or adopted by a client of a person or entity referred to in section 5 of the Act and that is accepted by the person or entity as being unique to that client. (signature)

Signature card

In respect of an account, means a document that is signed by a person who is authorized to give instructions in respect of the account, or electronic data that constitutes the signature of such a person. (fiche-signature)

Source

The issuer or provider of information or documents for verifying identification. (source)

Source of funds or of virtual currency (VC)

The origin of the particular funds or VC used to carry out a specific transaction or to attempt to carry out a transaction. It is how the funds were acquired, not where the funds may have been transferred from. For example, the source of funds could originate from activities or occurrences such as employment income, gifts, the sale of a large asset, criminal activity, etc. (origine des fonds ou de la monnaie virtuelle (MV))

Source of wealth

The origin of a person's total assets that can be reasonably explained, rather than what might be expected. For example, a person's wealth could originate from an accumulation of activities and occurrences such as business undertakings, family estates, previous and current employment income, investments, real estate, inheritance, lottery winnings, etc. (origine de la richesse)

Starting action

With respect to a reportable transaction, information related to the instructions provided by the person or entity making the request to the reporting entity to start a transaction. For example, an individual arrives at a bank and requests to purchase a bank draft. The starting action is the details of the instructions for the purchase which includes the funds or virtual currency that the requesting

person or entity brought to the reporting entity. A transaction must have at least one starting action. (action d'amorce)

SWIFT

The Society for Worldwide Interbank Financial Telecommunication. (SWIFT)

Terrorist activity

Has the same meaning as in subsection 83.01(1) of the Criminal Code. (activité terroriste)

Terrorist activity financing offence

An offence under section 83.02, 83.03 or 83.04 of the Criminal Code or an offence under section 83.12 of the Criminal Code arising out of a contravention of section 83.08 of that Act.

A terrorist financing offence is knowingly collecting or giving property (such as money) to carry out terrorist activities. This includes the use and possession of any property to help carry out the terrorist activities. The money earned for terrorist financing can be from legal sources, such as personal donations and profits from a business or charitable organization or from criminal sources, such as the drug trade, the smuggling of weapons and other goods, fraud, kidnapping and extortion. (infraction de financement des activités terroristes)

Third party

Any individual or entity that instructs another individual or entity to act on their behalf for a financial activity or transaction. (tiers)

Threats to the security of Canada

Has the same meaning as in section 2 of the Canadian Security Intelligence Service Act. (menaces envers la sécurité du Canada)

Training program

A written and implemented program outlining the ongoing training for your employees, agents or other individuals authorized to act on your behalf. It should contain information about all your obligations and requirements to be fulfilled under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and its associated Regulations. (programme de formation)

Trust

A right of property held by one individual or entity (a trustee) for the benefit of another individual or entity (a beneficiary). (fiducie)

Trust company

A company that is referred to in any of paragraphs 5(d) to (e.1) of the Act. (société de fiducie)

Trustee

A trustee is the individual or entity authorized to hold or administer the assets of a trust. (fiduciaire)

Tutor

In the context of civil law, a person who has been lawfully appointed to the care of the person and property of a minor. (tuteur)

Two year effectiveness review

A review, conducted every two years (at a minimum), by an internal or external auditor to test the effectiveness of your policies and procedures, risk assessment, and training program. (examen bisannuel de l'efficacité)

Valid

In respect of a document or information that is used to verify identity, appears legitimate or authentic and does not appear to have been altered or had any information redacted. The information must also be valid according to the issuer, for example if a passport is invalid because of a name change, it is not valid for FINTRAC purposes. (valide)

Verify identity

To refer to certain information or documentation, in accordance with the prescribed methods, to identify a person or entity (client). (vérifier l'identité)

Very large corporation or trust

A corporation or trust that has minimum net assets of $75 million CAD on its last audited balance sheet. The corporation's shares or units have to be traded on a Canadian stock exchange or on a stock exchange designated under subsection 262(1) of the Income Tax Act. The corporation or trust also has to operate in a country that is a member of the Financial Action Task Force (FATF). (personne morale ou fiducie dont l'actif est très important)

Violation

A contravention of the Act or the regulations that is designated as a violation by regulations made under subsection 73.1(1). (violation)

Virtual currency

Means:

1. (a) a digital representation of value that can be used for payment or investment purposes that is not a fiat currency and that can be readily exchanged for funds or for another virtual currency that can be readily exchanged for funds; or
2. (b) a private key of a cryptographic system that enables a person or entity to have access to a digital representation of value referred to in paragraph (a).

(monnaie virtuelle)

Virtual currency exchange transaction

An exchange, at the request of another person or entity, of virtual currency for funds, funds for virtual currency or one virtual currency for another. (opération de change en monnaie virtuelle)

Virtual currency exchange transaction ticket

A record respecting a virtual currency exchange transaction—including an entry in a transaction register—that sets out:

1. (a) the date of the transaction;
2. (b) in the case of a transaction of $1,000 or more, the name and address of the person or entity that requests the exchange, the nature of their principal business or their occupation and, in the case of a person, their date of birth;
3. (c) the type and amount of each type of funds and each of the virtual currencies involved in the payment made and received by the person or entity that requests the exchange;
4. (d) the method by which the payment is made and received;
5. (e) the exchange rates used and their source;
6. (f) the number of every account that is affected by the transaction, the type of account and the name of each account holder;
7. (g) every reference number that is connected to the transaction and has a function equivalent to that of an account number; and
8. (h) every transaction identifier, including the sending and receiving addresses.

(fiche d'opération de change en monnaie virtuelle)

Working days

In respect of an electronic funds transfer (EFT) report or a large virtual currency transaction report, a working day is a day between and including Monday to Friday. It excludes Saturday, Sunday, and a public holiday. (jour ouvrable)# Politically exposed persons and heads of international organizations guidance for account-based reporting entity sectors

Overview

Financial entities(FEs), securities dealers and casinos (account-based reporting entities) have politically exposed persons (PEPs) and heads of international organizations (HIOs) requirements under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and associated Regulations. However, some requirements and the examples given in this guidance only apply to certain reporting entities (REs).

References to PEPs in this guidance include both foreign and domestic PEPs, unless otherwise specified.

1. When or for whom must I make a PEP, HIO, family member or close associate determination?

You must take reasonable measures to make an account related PEP, HIO, family member or close associate (of foreign PEP only, in certain circumstances) determination:

- when you open an account;
- for authorized users of prepaid payment product accounts (PPPAs) (FEs only);
- when you conduct periodic monitoring of existing account holders;
- when you conduct periodic monitoring of authorized users of PPPAs (FEs only);
- when you detect a fact about existing account holders that indicates a PEP or HIO connection; and
- when you detect a fact about authorized users of PPPAs that indicates a PEP or HIO connection (FEs only).

See Account-related PEP or HIO determination below, for an explanation of your requirements in these instances.

If you are an FE or a casino then you must also take reasonable measures to make PEP, HIO, family member or close associate determinations for the following transactions:

- initiation of an international electronic funds transfer (EFT) in the amount of $100,000 or more;
- final receipt of an international EFT in the amount of $100,000 or more;

- receipt of cash or an amount of VC equivalent to $100,000 or more (casinos only);
- transfers of an amount of VC equivalent to $100,000 or more (FEs only);
- receipt of an amount of VC equivalent to $100,000 or more for remittance to a beneficiary (FEs only); and
- payment(s) of $100,000 or more to a PPPA (FEs only).

See Transaction-related PEP or HIO determination below, for an explanation of your requirements in these instances.

Account-related PEP or HIO determinations

Account opening As an FE, a securities dealer, or a casino, you must take reasonable measures to determine whether a person for whom you open an account is a PEP, HIO, family member of one of those persons, or close associate of a foreign PEP.Footnote 1

Authorized user of PPPA (FEs only) As an FE, you must take reasonable measures to determine whether a person identified as an authorized user of a PPPA is a PEP, HIO, family member of one of those persons, or close associate of a foreign PEP.Footnote 2

Periodic monitoring of existing account holders and authorized users of PPPAs As an FE, a securities dealer, or a casino, you must periodically take reasonable measures to determine whether a person who holds an account is a PEP, HIO, family member of one of those persons, or close associate of a foreign PEP.Footnote 3

As an FE, you must also periodically take reasonable measures to determine whether an authorized user of a PPPA is a PEP, HIO, family member of one of those persons, or close associate of a foreign PEP.Footnote 4

Detecting a fact about existing account holders and authorized users of PPPAs As an FE, a securities dealer, or a casino, if you or any of your employees or officers detect a fact that constitutes reasonable grounds to suspect that a person who holds an account is a PEP, HIO, or family member or close associate of one of these persons, you must take reasonable measures to determine whether they are such a person.Footnote 5

As an FE, if you or any of your employees or officers detect a fact that constitutes reasonable grounds to suspect that an authorized user of a PPPA is a PEP, HIO, or family member or close associate of one of these persons, you must take reasonable measures to determine whether they are such a person.Footnote 6

For more information about what it means to detect a fact about a PEP or HIO, see FINTRAC's Politically exposed persons and heads of international organizations guidance.

Transaction-related PEP or HIO determinations

Initiation of an international electronic funds transfer (EFT) in the amount of $100,000 or more As an FE or a casino, you must take reasonable measures to determine whether a person who requests that you initiate an international EFT in the amount of $100,000 or more is a PEP, HIO, or family member or close associate of one of these persons.Footnote 7

Final receipt of an international EFT in the amount of $100,000 or more As an FE or a casino, you must take reasonable measures to determine whether a beneficiary for whom you finally receive an international EFT in the amount of $100,000 or more is a PEP, HIO, or family member or close associate of one of these persons.Footnote 8

Receipt of cash or an amount of VC equivalent to $100,000 or more (casinos only) As a casino, you must take reasonable measures to determine whether a person from whom you receive cash or an amount of VC equivalent to $100,000 or more is a PEP, HIO, or family member or close associate of one of these persons.Footnote 9

Transfer of an amount of VC equivalent to $100,000 or more (FEs only) As an FE, you must take reasonable measures to determine whether a person who requests that you transfer an amount of VC equivalent to $100,000 or more is a PEP, HIO, or family member or close associate of one of these persons.Footnote 10

Receipt of an amount of VC equivalent to $100,000 or more for remittance to a beneficiary (FEs only) As an FE, you must take reasonable measures to determine whether a beneficiary for whom you receive an amount of VC equivalent to $100,000 or more is a PEP, HIO, or family member or close associate of one of these persons.Footnote 11

Payment in the amount of $100,000 or more to a PPPA (FEs only) As an FE, you must take reasonable measures to determine whether a person who makes a payment in the amount of $100,000 or more to a PPPA is a PEP, HIO, or family member or close associate of one of these persons.Footnote 12

2. What are the exceptions to making a PEP, HIO, family member or close associate determination?

You do not have to make a PEP, HIO, family member or close associate determination (as applicable) for the following:

1. If you previously determined that a person is a foreign PEP or a family member of a foreign PEP.Footnote 13

2. If you are an **FE** or **securities dealer** you do not need to determine if a person who is a member of a group plan account is a PEP, HIO or a family member or close associate of a PEP or HIO, if:Footnote 14
    - the person's member contributions are made by the sponsor of the group plan or by payroll deduction; **and**
    - the identity of the entity that is the plan sponsor has been verified in accordance with subsection 109(1) or 112(1) of the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations.
3. If you are an **FE**, you do not have to make a PEP determination or keep the associated records for your activities in respect of the processing of payments by credit card or by prepaid payment products for a merchant.Footnote 15
4. If you are an **FE** or **casino**, that initiates or is the final recipient of an international EFT of $100,000 or more, by means of a credit/debit card or a prepaid payment product where the beneficiary has an agreement with the payment service provider that permits payment by that means for the provision of goods and services, you do not need to determine if the person is a PEP, HIO or a family member or close associate of a PEP or HIO.Footnote 16

3. What measures do I need to take after making a PEP, HIO, family member or close associate determination?

Account-related measures

Foreign PEPs As an FE, a securities dealer or a casino, when you **open an account**, **conduct periodic monitoring**, or **detect a fact,** and you determine that a person who holds an account or is an authorized user of a PPPA (FEs only) is a foreign PEP or family member or close associate of a foreign PEP, you must:Footnote 17

- take reasonable measures to establish the source of the funds or source of the VC that is or is expected to be deposited into the account in question and to establish the source of the person's wealth;
- obtain the approval of a member of senior management to keep the account open; and
- take your enhanced measures, including taking additional measures to verify the person's identity, conducting enhanced ongoing monitoring and taking any other enhanced measures to mitigate the risks posed by the person.

Domestic PEPs or HIOs As an FE, a securities dealer or a casino, when you **open an account**, **conduct periodic monitoring**, or **detect a fact,** and you determine that a person who holds an account or is an authorized user (FEs) is a domestic PEP, HIO, or family member or close associate, of a domestic PEP or HIO, **and** based on your risk assessment, you consider there

to be a **high risk** of a money laundering (ML) or terrorist activity financing (TF) offence being committed, you must:Footnote 18

- take reasonable measures to establish the source of the funds or source of the VC that is or is expected to be deposited into the account in question and to establish the source of the person's wealth;
- obtain the approval of a member of senior management to keep the account open; and
- take your enhanced measures, including taking additional measures to verify the person's identity, conducting enhanced ongoing monitoring and taking any other enhanced measures to mitigate the risks posed by the person.

When you **detect a fact about an existing account,** and determine that a person is a close associate of a domestic PEP or HIO, **and** based on your risk assessment, you consider there to be a **high risk** of an ML or TF offence being committed, you must:Footnote 19

- take reasonable measures to establish the source of the funds or source of the VC that is or is expected to be deposited into the account in question and to establish the source of the person's wealth;
- obtain the approval of a member of senior management to keep the account open; and
- take your enhanced measures, including taking additional measures to verify the person's identity, conducting enhanced ongoing monitoring and taking any other enhanced measures to mitigate the risks posed by the person.

Prescribed timing for taking measures When you **open an account** for or **detect a fact** about a PEP, HIO, or family member or close associate of one of these persons, you have **30 days** after the day on which you open the account or you detect a fact to, as applicable:Footnote 20

- take reasonable measures to establish the source of the funds or source of the VC that is or is expected to be deposited into the account in question and to establish the source of the person's wealth; and
- obtain the approval of a member of senior management to keep the account open.

Transaction-related measures

Foreign PEPs

FEs When you **initiate an international EFT** for a personin the amount **of $100,000 or more** or you **process a payment to a PPPA** for a person in the amount **of $100,000 or more** and determine that the person is a foreign PEP, or a family member or close associate of a foreign PEP, you must:Footnote 21

- take reasonable measures to establish the source of the funds used for the transaction and to establish the source of the person's wealth; and
- ensure that a member of senior management reviews the transaction.

When you **transfer an amount of VC** equivalent to **$100,000 or more** for a person that you determine is a foreign PEP, or a family member or close associate of a foreign PEP, you must:Footnote 22

- take reasonable measures to establish the source of the VC used for the transaction and to establish the source of the person's wealth; and
- ensure that a member of senior management reviews the transaction.

When you **receive for a beneficiary an international EFT or an amount of VC** equivalent to **$100,000 or more** and determine that the beneficiary is a foreign PEP, or a family member or close associate of a foreign PEP, you must ensure that a member of senior management reviews the transaction.Footnote 23

Casinos When you **initiate an international EFT** in the amount **of $100,000 or more, finally receive an international EFT for a beneficiary** in the amount **of $100,000 or more**, or **receive cash, or an amount of VC equivalent to, $100,000 or more,** and determine that a person is a foreign PEP, or a family member or close associate of a foreign PEP, you must:Footnote 24

- take reasonable measures to establish the source of the funds or source of the VC used for the transaction and to establish the source of the person's wealth; and
- ensure that a member of senior management reviews the transaction.

Domestic PEPs or HIOs

FEs When you **initiate an international EFT** in the amount **of $100,000 or more** or **process a payment to a PPPA** in the amount **of $100,000 or more**, for a person that you determine is a domestic PEP, HIO, or family member or close associate of a domestic PEP or HIO **and,** based on your risk assessment, you consider there to be a **high risk** of an ML or TF offence being committed, you must:Footnote 25

- take reasonable measures to establish the source of the funds used for the transaction and to establish the source of the person's wealth; and
- ensure that a member of senior management reviews the transaction.

When you **transfer an amount of VC** equivalent to **$100,000 or more,** and determine that a person is a domestic PEP, HIO, or family member or close associate of a domestic PEP or HIO, **and** based on your risk assessment, you consider there to be a **high risk** of an ML or TF offence being committed, you must:Footnote 26

- take reasonable measures to establish the source of the VC used for the transaction and to establish the source of the person's wealth; and
- ensure that a member of senior management reviews the transaction.

When you **receive for a beneficiary an international EFT or an amount of VC equivalent to $100,000 or more** and determine that the beneficiary is a domestic PEP, HIO, or family member or close associate of a domestic PEP or HIO, **and** based on your risk assessment, you consider there to be a **high risk** of an ML or TF offence being committed, you must ensure that a member of senior management reviews the transaction.Footnote 27

Casinos When you **initiate an international EFT** in the amount **of $100,000 or more**, **finally receive for a beneficiary an international EFT** in the amount **of $100,000 or more,** or **receive cash or an amount of VC** equivalent to **$100,000 or more,** and determine that a person is a domestic PEP, HIO, or family member or close associate of a domestic PEP or HIO, **and** based on your risk assessment, you consider there to be a **high risk** of an ML or TF offence being committed, you must:Footnote 28

- take reasonable measures to establish the source of the funds or source of the VC used for the transaction and to establish the source of the person's wealth; and
- ensure that a member of senior management reviews the transaction.

Prescribed timing for taking measures As an FE or a casino, for the transactions referred to above, you have **30 days** after the day on which the transaction is conducted to, as applicable:Footnote 29

- take reasonable measures to make a PEP, HIO, family member, or close associate determination, and if applicable, establish the source of the funds or source of the VC used for the transaction and to establish the person's source of wealth, and ensure that a member of senior management reviews the transaction; **or**
- take reasonable measures to make a PEP, HIO, family member, or close associate determination, and if applicable, ensure that a member of senior management reviews the transaction.

4. What PEP, HIO, family member or close associate records do I need to keep?

You must keep the following records related to your determination that a person is a PEP, HIO, or a family member or close associate of a PEP or HIO:

PEP and HIO account records

If you determine that a person is a foreign PEP, a family member, or close associate of a foreign PEP, a high-risk domestic PEP, high-risk HIO or high-

risk family member or high-risk close associate of one of these persons, and you obtained the approval of a member of senior management to keep an account open, you must keep a record of:Footnote 30

- the office or position and the name of the organization or institution of the PEP or HIO;
- the date of the determination;
- the source of the funds or VC, if known, that is or is expected to be deposited into the account or paid to the PPPA;
- the source of the person's wealth, if known;
- the name of the member of senior management who approved keeping the account open; and
- the date of that approval.

In the case of family members and close associates of PEPs and HIOs, you may also want to keep a record of the nature of the relationship between the person and the PEP or HIO, as applicable.

Retention: You must keep PEP and HIO account records for at least five years from the day the account to which they relate is closed.Footnote 31

PEP and HIO transaction records

If as an FE or a casino, you **review** one of the above-mentioned transactions (see Transaction related PEP or HIO determinations) for which you have made a PEP or HIO determination, you must keep a record of:Footnote 32

- the office or position and the name of the organization or institution of the PEP or HIO;
- the date of the determination;
- the source of the funds or source of the VC used for the transaction, if known;
- the source of the person's wealth, if known;
- the name of the member of senior management who reviewed the transaction; and
- the date of that review.

In the case of family members and close associates of PEPs and HIOs, you may also want to include in the record the nature of the relationship between the person and the PEP or HIO, as applicable.

Retention: You must keep transaction records for at least 5 years from the day on which the last business transaction is conducted.Footnote 33# Politically exposed persons and heads of international organizations guidance for non-account-based reporting entity sectors : FINTRAC's compliance guidance

This guidance explains the requirement to make a politically exposed person and head of international organizations determination for non-account-based reporting entity sectors.

1. Who must comply

The following non-account-based reporting entities have requirements regarding politically exposed persons and heads of international organizations under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and associated Regulations:

- Accountants
- Agents of the Crown
- British Columbia notaries
- Dealers in precious metals and precious stones
- Real estate developers, brokers and sales representatives
- Money services businesses, and foreign money services businesses
- Mortgage administrators, mortgage brokers and mortgage lenders

For **life insurance companies, brokers and agents**, consult: Politically exposed persons and heads of international organizations guidance for life insurance companies, brokers and agents.

For more information about your obligations to determine who is a politically exposed person, a head of an international organization, or a person related or closely associated to one of those persons, and clarity on terminology and related considerations (e.g. who is considered a member of senior management), consult: Politically exposed persons and heads of international organizations.

2. When to make a determination

You must take reasonable measures to determine whether a person with whom you enter into a business relationship is a politically exposed person, a head of an international organization, a family member of one of those persons, or a close associate of a foreign politically exposed person (in certain circumstances) when you:

- enter into a business relationship
- conduct periodic monitoring of a business relationship, and
- detect a fact that constitutes reasonable grounds to suspect they are politically exposed person or head of an international organization , family member, or close associate

You must also take reasonable measures to make a determination regarding politically exposed persons, heads of international organizations, family members or close associates to one of those persons for certain transactions. Consult the Transaction-related politically determinations section of this guidance.

Business relationship-related determinations

Entering into a business relationship You must take reasonable measures to determine whether a person with whom you enter into a business relationship is a politically exposed person, head of an international organization, family

member of one of those persons, or close associate of a foreign politically exposed person.

Periodic monitoring of business relationships You must periodically take reasonable measures to determine whether a person with whom you have a business relationship is a politically exposed person, a head of an international organization, a family member of one of those persons, or close associate of a foreign politically exposed person.

Detecting a fact about existing business relationships If you, or any of your employees or officers, detects a fact that constitutes reasonable grounds to suspect that a person with whom you have a business relationship is a politically exposed person, head of an international organization, or a family member or close associate of one of these persons, you must take reasonable measures to determine whether they are such a person.

Transaction-related determinations

You must take reasonable measures to determine whether a person is a politically exposed person, a head of an international organization, a family member or close associate of one of those persons for certain transactions, as applicable:

Accountants, agents of the Crown, British Columbia notaries, dealers in precious metals and precious stones, mortgage administrators, mortgage brokers and mortgage lenders, and real estate developers, brokers and sale representatives

- Receipt of an amount of $100,000 or more in cash or an amount of virtual currency equivalent to $100,000 or more

Money services businesses and foreign money services businesses You must determine requestor when:

- Initiation of an international electronic funds transfer in the amount of $100,000 or more
- Transfer of an amount of virtual currency equivalent to $100,000 or more
- Transport of an amount of $100,000 or more in cash, money orders, traveler's cheques, or other similar negotiable instruments or an amount of virtual currency equivalent to $100,000 or more

You must determine beneficiary when:

- Final receipt of an international electronic funds transfer in the amount of $100,000 or more
- Receipt of an amount of virtual currency equivalent to $100,000 or more for remittance to a beneficiary

3. What are the exceptions

You do not have to make a politically exposed person or family member determination if you already determined that a person is a foreign politically exposed person or a family member of a foreign politically exposed person.

4. What measures to take

In this section

- Business relationship-related measures
- Transaction-related measures

Business relationship-related measures

Measures for foreign politically exposed persons When you **enter into a business relationship**, **conduct periodic monitoring of business relationships**, or **detect a fact about an existing business relationship,** and determine that a person is a foreign politically exposed person or family member or close associate of a foreign politically exposed person, you must:

- take reasonable measures to establish the person's source of wealth, and
- take enhanced measures, including the following:
  - taking additional measures to verify the person's identity
  - conducting enhanced ongoing monitoring of the business relationship
  - taking any other enhanced measures to mitigate the risks posed by the person

Measures for domestic politically exposed persons or heads of international organizations When you **enter into a business relationship**, **conduct periodic monitoring of business relationships**, or **detect a fact about an existing business relationship,** and determine that a person is a domestic politically exposed person, head of an international organization, or family member of a domestic politically exposed person or head of an international organization, and based on your risk assessment, you consider there to be a **high risk** of a money laundering or terrorist activity financing offence being committed, you must:

- take reasonable measures to establish the person's source of wealth, and
- take enhanced measures, including the following:
  - taking additional measures to verify the person's identity
  - conducting enhanced ongoing monitoring of the business relationship
  - taking any other enhanced measures to mitigate the risks posed by the person

When you **detect a fact about an existing business relationship,** and determine that a person is a close associate of a domestic politically exposed

person or head of an international organization, and based on your risk assessment, you consider there to be a **high risk** of a money laundering or terrorist financing offence being committed, you must:

- take reasonable measures to establish the person's source of wealth, and
- take enhanced measures, including the following:
  - taking additional measures to verify the person's identity
  - conducting enhanced ongoing monitoring of the business relationship
  - taking any other enhanced measures to mitigate the risks posed by the person

Timing to establish the source of wealth When you **enter into a business relationship** with, or **detect a fact** about a politically exposed person, head of an international organization, or family member or close associate of one of these persons, you have **30 days** after the day on which you enter into the business relationship or detect a fact to take reasonable measures to establish the source of a person's wealth, if applicable.

Transaction-related measures

Measures for foreign politically exposed persons Accountants, agents of the Crown, British Columbia notaries, dealers in precious metals and precious stones, mortgage administrators, mortgage brokers or mortgage lenders and real estate developers, brokers or sales representatives

When you receive an amount of $100,000 or more in cash or an amount of virtual currency equivalent to $100,000 or more, and determine that a person is a foreign politically exposed person or family member or close associate of a foreign politically exposed person, you must:

- take reasonable measures to establish the source of the cash or source of the virtual currency used for the transaction and the source of the person's wealth, and
- ensure that a member of senior management reviews the transaction

Money services businesses and foreign money services businesses

When in providing services to people located in Canada, you conduct one of the following transactions:

- initiating an international electronic funds transfer in an amount of $100,000 or more
- transferring an amount of virtual currency equivalent to $100,000 or more
- transporting an amount of $100,000 or more in cash, money orders, traveler's cheques, or other similar negotiable instruments (except for cheques payable to a named person or entity) or an amount of virtual currency equivalent to $100,000 or more

and you determine that the person is a foreign politically exposed person or family member or close associate of a foreign politically exposed person, you must:

- take reasonable measures to establish the source of the funds or virtual currency used for the transaction and to establish the source of the person's wealth, and
- ensure that a member of senior management reviews the transaction

When in providing services to people located in Canada, you:

- finally receive an international electronic funds transfer or an amount of virtual currency equivalent to $100,000 or more for a beneficiary
- and determine that the person is a foreign politically exposed person or family member or close associate of a foreign politically exposed person

You must ensure that a member of senior management reviews the transaction.

Measures for domestic politically exposed persons or heads of international organizations Accountants, agents of the Crown, British Columbia notaries, dealers in precious metals and precious stones, mortgage administrators, mortgage brokers or mortgage lenders, and real estate developers, brokers or sales representatives

When you:

- receive an amount of $100,000 or more in cash or an amount of virtual currency equivalent to $100,000 or more **,** and
- determine that the person is a domestic politically exposed person, head of an international organization, or family member or close associate of a domestic politically exposed person or head of an international organization, **and**
- based on your risk assessment, you consider there to be a **high risk** of a money laundering or terrorist financing offence being committed

You must:

- take reasonable measures to establish the source of the funds or source of the virtual currency used for the transaction and to establish the source of the person's wealth, and
- ensure that a member of senior management reviews the transaction

Money services businesses and foreign money services businesses

When in providing services to people located in Canada, you:

- initiate an international electronic funds transfer in the amount of $100,000 or more at the request of a person, and
- determine that the person is a domestic politically exposed person, head of an international organization, or family member or close associate of a do-

mestic politically exposed person or head of an international organization, **and**
- based on your risk assessment, you consider there to be a **high risk** of a money laundering or terrorist financing offence being committed

You must:

- take reasonable measures to establish the source of the funds used for the transaction and to establish the source of the person's wealth, and
- ensure that a member of senior management reviews the transaction

When in providing services to people located in Canada, you:

- transfer an amount of virtual currency equivalent to $100,000 or more, and
- determine that the person is a domestic politically exposed person, head of an international organization, or family member or close associate of a domestic politically exposed person or head of an international organization, **and**
- based on your risk assessment, you consider there to be a **high risk** of a money laundering or terrorist financing offence being committed

You must:

- take reasonable measures to establish the source of the virtual currency used for the transaction and to establish the source of the person's wealth, and
- ensure that a member of senior management reviews the transaction

When in providing services to people located in Canada, you:

- receive for a beneficiary an international electronic funds transfer or an amount of virtual currency equivalent to $100,000 or more, and
- determine that the beneficiary is a domestic politically exposed person, head of an international organization, or family member or close associate of a domestic politically exposed person or head of an international organization, **and**
- based on your risk assessment, you consider there to be a **high risk** of a money laundering or terrorist financing offence being committed

You must ensure that a member of senior management reviews the transaction.

Prescribed timing for taking measures Accountants, agents of the Crown, British Columbia notaries, dealers in precious metals and precious stones, mortgage administrators, mortgage brokers or mortgage lenders, and real estate developers, brokers or sales representatives

When you **receive an amount of $100,000 or more in cash or an amount of virtual currency equivalent to $100,000 or more**, you have **30 days** after the day on which the transaction is conducted to:

1. take reasonable measures to determine whether a person is a politically exposed person, a head of an international organization, a family member, or close associate, and
2. if you make such a determination, take reasonable measures to:
    - establish the source of the cash or source of the virtual currency used for the transaction
    - establish the person's source of wealth, and
    - ensure that a member of senior management reviews the transaction

Money services businesses and foreign money services businesses

In providing services to people located in Canada, for the applicable transactions referred to above in this section, you have **30 days** after the day on which the transaction is conducted to:

1. take reasonable measures to determine whether a person is a politically exposed person, a head of an international organization, a family member or close associate, and
2. if you make such a determination:
    - establish the source of the funds or source of the virtual currency used for the transaction, and
    - establish the person's source of wealth,
    - and ensure that a member of senior management reviews the transaction

or

1. take reasonable measures to determine whether a person is a politically exposed person, a head of an international organization, a family member or close associate, and
2. if you make such a determination, ensure that a member of senior management reviews the transaction

5. What records to keep

Records on business relationships involving politically exposed persons and heads of international organizations

When you **enter into a business relationship**, **conduct periodic monitoring of business relationships**, or **detect a fact about an existing business relationship,** and determine that the person is a politically exposed person, a head of an international organization, or a family member or close associate of one of those persons, you must keep a record of:

- the office or position and the name of the organization or institution of the politically exposed person or head of an international organization
- the date of the determination, and
- the source of the person's wealth, if known

Retention: You must keep records on business relationships involving politically exposed persons and heads of international organizations for at least five years after the day on which they were created.

Records on transactions involving politically exposed persons and head of international organizations

Accountants, agents of the Crown, British Columbia notaries, dealers in precious metals and precious stones, mortgage administrators, mortgage brokers or mortgage lenders, and real estate developers, brokers or sales representatives

If senior management **reviews** a transaction where you had **received an amount of $100,000 or more in cash or an amount of virtual currency equivalent to $100,000 or more** for which you determined a person was a politically exposed person or a head of an international organization, then you must keep a record of:

- the office or position and the name of the organization or institution of the politically exposed person or head of an international organization or a family member or close associate of one of those persons
- the date of the determination
- the source of the cash or virtual currency used for the transaction, if known
- the source of the person's wealth, if known
- the name of the member of senior management who reviewed the transaction, and
- the date of that review

In the case of family members and close associates of politically exposed persons and heads of international organizations, you may also want to include in the record the nature of the relationship between the person and the politically exposed person or head of an international organization, as applicable.

Retention: If you review a prescribed transaction involving a politically exposed person or a head of an international organization, then you must keep these transaction records for at least 5 years after the day on which they were created.

Money services businesses and foreign money services businesses

If, when providing services to people located in Canada, you review an applicable prescribed transaction listed under Transaction-related politically exposed person or head of an international organization determinations for which you have determined a person is a politically exposed person or a head of an international organization determination, then you must keep a record of:

- the office or position and the name of the organization or institution of the politically exposed person or head of an international organization
- the date of the determination

- the source of the funds or source of the virtual currency used for the transaction (if known)
- the source of the person's wealth (if known)
- the name of the member of senior management who reviewed the transaction, and
- the date of that review

You may also want to include in the record the nature of the relationship between the family member or close associate and the politically exposed person or head of an international organization, as applicable.

Retention: If you review a prescribed transaction involving a politically exposed person or a head of an international organization transaction, then you must keep these transaction records for at least 5 years from the day on which the last business transaction is conducted.# Record keeping requirements for financial entities

Overview

Financial entities (FEs) have record keeping requirements under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and associated Regulations.

This guidance outlines certain record keeping requirements for FEs.

1. What records must I keep and what must they contain?

You must keep the following records:

1. Reports – a copy of every report sent to FINTRAC
    - Suspicious Transaction Reports
    - Terrorist Property Reports
    - Large Cash Transaction Reports
    - Large Virtual Currency Transaction Reports
    - Electronic Funds Transfer Reports
2. Large cash transaction records
3. Large virtual currency transaction records
4. Records of transactions of $3,000 or more
5. Records of electronic funds transfers of $1,000 or more
6. Records of virtual currency transfers in amounts equivalent to $1,000 or more
7. Foreign currency exchange transaction tickets
8. Virtual currency exchange transaction tickets
9. Account records
    - Records for account holders and persons authorized to give instructions
    - Signature cards
    - Intended use of an account

- Applications
- Account operating agreements
- Debit and credit memos
- Deposit slips
- Account statements
- Cleared cheque records
- Credit arrangement records

10. Credit card account and transaction records
11. Prepaid payment product account and transaction records
12. Trust records

****Note:** When you are required to keep records about clients, you should beas descriptive as possible. Being descriptive when recording the nature of the principal business or occupation of a client will help determine whether a transaction or activity is consistent with what would be expected for that client. For example, when the client's occupation is "manager", the record should reflect the area of management, such as "hotel reservations manager" or "retail clothing store manager". When an entity's principal business area is "sales", the record should specify the type of sales, such as "pharmaceutical sales" or "retail sales".

a. Reports – a copy of every report sent to FINTRAC

You must keep a copy of every report that you submit to FINTRAC as a record.

Suspicious Transaction Reports When you submit a Suspicious Transaction Report (STR) to FINTRAC, you must keep a copy of it.Footnote 1

Retention: At least five years after the day the STR was submitted.Footnote 2

Terrorist Property Reports When you submit a Terrorist Property Report (TPR) to FINTRAC, you must keep a copy of it.Footnote 3

Retention: At least five years after the day the TPR was submitted.Footnote 4

Large Cash Transaction Reports When you submit a Large Cash Transaction Report (LCTR) to FINTRAC, you must keep a copy of it.Footnote 5

Retention: At least five years from the date the LCTR was created.Footnote 6

Large Virtual Currency Transaction Reports When you submit a Large Virtual Currency Transaction Report (LVCTR) to FINTRAC, you must keep a copy of it.Footnote 7

Retention: At least five years from the date the LVCTR was created.Footnote 8

Electronic Funds Transfer Reports When you submit an Electronic Funds Transfer Report (EFTR) to FINTRAC, you must keep a copy of it.Footnote 9

Retention: At least five years from the date the EFTR was created.Footnote 10

b. Large cash transaction records

You must keep a large cash transaction record when you receive $10,000 or more in cash.Footnote 11

If you authorize a person or an entity to receive funds on your behalf, and that person or entity receives $10,000 or more in cash in accordance with the authorization, you are deemed to have received the amount when it is received by the person or entity, and you must keep a large cash transaction record.Footnote 12

****Note**: This requirement is subject to the 24-hour rule.Footnote 13

A large cash transaction record must include:Footnote 14

- the date you received the cash;
- if the amount is received for deposit into an account:
  - the account number(s);
  - the name of each account holder—if the cash was deposited into more than one client account, all names must be included in the record; and
  - the time of the deposit, if it was made during your normal business hours, or an indication of "night deposit" if the deposit was made outside of your normal business hours;
- for any person involved in the transaction (including the person from whom you received the cash), their name, address, date of birth, and occupation, or in the case of a sole proprietor, the nature of their principal business;
- for any entity involved in the transaction (including the entity from which you received the cash), their name, address and nature of their principal business;
- the type and amount of each fiat currency received;
- the purpose of the transaction (for example, the cash was used to purchase a money order, etc.);
- the method by which you received the cash (for example, in person, by mail, by armoured car, etc.);
- the exchange rates used and their source (if applicable);
- if other accounts are affected by the transaction, include:
  - the account number and type of account (for example, business, personal, etc.); and
  - the name of each account holder;

- every reference number connected to the transaction that is meant to be similar to an account number;
- the following details about the remittance (i.e. the disposition) of, or exchange for, the cash received:
  - the method of remittance (for example, wire transfer, money order, etc.);
  - if the remittance is in funds, the type and amount of each type of funds involved;
  - if the remittance is not in funds, the type of remittance (for example, virtual currency, etc.) and value if different from the amount received in cash; and
  - the name of every person or entity involved in the remittance, their account number or policy number. If there is no account or policy number, their identifying number.

Retention: At least five years from the date the large cash transaction record was created.Footnote 15

c. Large virtual currency transaction records

You must keep a large virtual currency (VC) transaction record when you receive VC in an amount equivalent to $10,000 or more.Footnote 16

If you authorize a person or an entity to receive VC on your behalf, and that person or entity receives VC in an amount equivalent to $10,000 or more in accordance with the authorization, you are deemed to have received the VC when it is received by the person or entity, and you must keep a large VC transaction record.Footnote 17

****Note**: This requirement is subject to the 24-hour rule.Footnote 18

A large VC transaction record must include:Footnote 19

- the date you received the VC;
- if you received the amount for deposit into an account, the name of each account holder;
- for any person involved in the transaction (including the person from whom you received the VC), their name, address, date of birth, and their occupation, or in the case of a sole proprietor, the nature of their principal business;
- for any entity involved in the transaction (including the entity from which you received the VC), their name, address and the nature of their principal business;
- the type and amount of each VC involved in the receipt;
- the exchange rates used and their source;
- if other accounts are affected by the transaction, include:
  - the account number and type of account; and
  - the name of each account holder;

- every reference number connected to the transaction that is meant to be similar to an account number; and
- every transaction identifier (this may include a transaction hash or similar identifier, if applicable), and every sending and receiving address.

Retention: At least five years from the date the large virtual currency transaction record was created.Footnote 20

d. Records of transactions of $3,000 or more

Issuance of traveller's cheques, money orders or similar negotiable instruments When you receive $3,000 or more in funds or an equivalent amount in VC, from a person or entity, for the issuance of traveller's cheques, money orders or other similar negotiable instruments you must record:Footnote 21

- the date you received the funds or VC;
- if you received the amount from a person, their name, address, date of birth and their occupation, or in the case of a sole proprietor, the nature of their principal business;
- if you receive the amount from an entity, its name, address and nature of its principal business;
- the amount received;
- the type and amount of each type of funds and each type of the VC's involved;
- if an account is affected by the transaction:
  - the account number and account type; and
  - the name of each account holder;
- every reference number that is connected to the transaction that is meant to be similar to an account number;
- if the received amount is in VC, every transaction identifier including transaction hashes or similar identifiers (if applicable), and every sending and receiving addresses.

Redemption of money orders When you redeem one or more money orders, for a total value of $3,000 or more, in funds or in an equivalent amount of VC you must record:Footnote 22

- the date the money orders were redeemed;
- if the client is a person, their name, address, date of birth and their occupation, or in the case of a sole proprietor, the nature of their principal business;
- if the client is an entity, its name, address and nature of its principal business;
- the total amount of the money orders or money orders;
- the name of the issuer of each money order;
- if an account is affected by the redemption:
  - the account number and account type; and

    - the name of each account holder;
- every reference number connected to the redemption that is meant to be similar to an account number; and
- if the redemption involves VC, every transaction identifier, including transaction hashes or similar identifiers (as applicable), and every sending and receiving address.

Retention: At least five years from the date the record for a transaction of $3,000 or more was created.Footnote 23

e. Records of electronic fund transfers of $1,000 or more

Initiating an international electronic funds transfer of $1,000 or more When you initiate, at the request of a person or an entity, an international electronic funds transfer or any other electronic funds transfer (EFT) that is a SWIFT MT-103 message or equivalent valued at $1,000 or more you must record:Footnote 24

- the date the EFT was initiated;
- the type and amount of each type of funds involved in the initiation;
- if the client is a person, their name, address, date of birth, telephone number and their occupation, or in the case of a sole proprietor, the nature of their principal business;
- if the client is an entity, its name, address, telephone number and nature of its principal business;
- the exchange rates used and their source;
- the name and address of each beneficiary;
- if an account is affected by the initiation
    - the account number and account type; and
    - the name of each account holder;
- the number of every account that is affected by the EFT, other than those affected by the initiation; and
- every reference number that is connected to the EFT and is meant to be similar to an account number.

Sending an international EFT of $1,000 or more When you send, as an intermediary, an international EFT of $1,000 or more that was initiated by another reporting entity, you must record:Footnote 25

- the date the EFT was sent;
- if fiat currencies were exchanged in the course of sending the EFT, the type and amount of each fiat currency involved in the exchange;
- the exchange rates used and their source;
- for every account affected by the sending:
    - the account number and account type; and
    - the name of each account holder;

- every reference number connected to sending the EFT that is meant to be similar to an account number;
- the name and address of the person or entity who requested the initiation of the EFT, unless after taking reasonable measures that information was not included with the transfer and it is not otherwise known; and
- the name and address of each beneficiary, unless after taking reasonable measures that information was not included with the transfer and it is not otherwise known.

Final receipt of an international EFT of $1,000 or more When you are the final recipient of an international EFT of $1,000 or more, you must record:Footnote 26

- the date the EFT was finally received;
- the type and amount of each type of funds involved in the final receipt;
- the name, address, date of birth and nature of the principal business, in the case of a sole proprietor, or occupation of each person who is a beneficiary;
- the name, address and nature of the principal business of each entity that is a beneficiary;
- the date of the remittance;
- the exchange rates used for the remittance and their source;
- if the remittance is in funds, the type and amount of each type of funds involved in the remittance;
- if the remittance is not in funds, the type of remittance (for example, virtual currency, precious stones, etc.), and its value, if different from the amount of funds finally received;
- for every account affected by the final receipt or remittance:
  - the account number and account type; and
  - the name of each account holder;
- every reference number connected to the EFT that is meant to be similar to an account number;
- the name and address of the person or entity that requested the initiation of the EFT, unless after taking reasonable measures, that information was not included with the transfer and it is not otherwise known; and
- the number of every account that is affected by the EFT, other than those affected by the final receipt or remittance.

****Note:** When you initiate, send as an intermediary, or finally receive an EFT, you must include with the transfer the prescribed information in accordance with the travel rule. Please see FINTRAC's travel rule guidance for more information.

Retention: At least five years from the date the EFT record was created.Footnote 27

f. Records of virtual currency transfers in amounts equivalent to $1,000 or more

VC transfer in an amount equivalent to $1,000 or more When you transfer VC in an amount equivalent to $1,000 or more at the request of a person or entity, you must record:Footnote 28

- the date of the transfer;
- the type and amount of each VC that is involved in the transfer;
- if the client is a person, their name, address, date of birth and occupation, or in the case of a sole proprietor, the nature of their principal business;
- if the client is an entity, its name, address and the nature of its principal business;
- the name and address of each beneficiary;
- for every account affected by the transfer:
  - the account number and account type; and
  - the name of each account holder;
- every reference number connected to the transaction that is meant to be similar to an account number;
- every transaction identifier including transaction hashes or similar identifiers (if applicable) and every sending and receiving address; and
- the exchange rates used and their source.

Receipt of VC in an amount equivalent to $1,000 or more for remittance to a beneficiary When you receive VC in an amount equivalent to $1,000 or more for remittance to a beneficiary, you must record: Footnote 29

- the date of the receipt;
- the type and amount of each VC that is received;
- if the beneficiary is a person, the name, address, date of birth and occupation, or in the case of a sole proprietor, the nature of their principal business of each beneficiary;
- if the beneficiary is an entity, the name, address and the nature of principal business of each beneficiary;
- the date of the remittance;
- the exchange rates used for the remittance and their source;
- if the remittance is in VC, the type and amount of each VC involved in the remittance;
- if the remittance is not in VC, the type and value of the remittance, if different from the value of the received VC;
- for every account affected by the transaction:
  - the account number and account type; and
  - the name of each account holder;
- every reference number connected to the transaction that is meant to be similar to an account number;
- every transaction identifier, including transaction hashes or similar identifiers (if applicable), and every sending and receiving address; and

- the name and address of the person or entity that requested the transfer, unless that information was not, despite the taking of reasonable measures, included with the transfer and is not otherwise known.

Note: When you transfer VC, you must include with the transfer the prescribed information in accordance with the travel rule. When you receive VC, you must take reasonable measures to ensure that the transfer includes the prescribed information. Please see FINTRAC's travel rule guidance for more information.

Retention: At least five years from the date the VC transfer or VC receipt record was created.Footnote 30

g. Foreign currency exchange transaction tickets

You must keep a transaction ticket, which may take the form of an entry in a transaction register, for every foreign currency exchange transaction you conduct, regardless of the amount.Footnote 31 Each transaction ticket must include:Footnote 32

- the date of the transaction;
- if the transaction was of $3,000 or more and requested by a person, their name, address, date of birth and occupation, or in the case of a sole proprietor, the nature of their principal business;
- if the transaction was of $3,000 or more and requested by an entity, its name, address and the nature of its principal business;
- type and amount of each fiat currency received from the client and the type and amount of each fiat currency given to the client;
- the method by which the payment was made and received;
- the exchange rates used and their source;
- for every account affected by the transaction:
  - the account number and account type; and
  - the name of each account holder;
- every reference number that is connected to the transaction that is meant to be similar to that of an account number.

Retention: At least five years from the date the foreign exchange transaction record was created.Footnote 33

h. VC exchange transaction tickets

You must keep a VC exchange transaction ticket, which may take the form of an entry in a transaction register, for every VC exchange transaction you conduct, regardless of the amount.Footnote 34 Each transaction ticket must include:Footnote 35

- the date of the transaction;

- if the VC transaction was equivalent to $1,000 or more and requested by a person, their name, address, date of birth and occupation, or in the case of a sole proprietor, the nature of their principal business;
- if the VC transaction was equivalent to $1,000 or more and requested by an entity, its name, address and the nature of its principal business;
- the type and amount of each fund and each VC involved in the payment made and received by the client;
- the method (VC currency exchange business) by which the payment was made and received;
- the exchange rates used and their source;
- for every account affected by the transaction:
  - the account number and account type; and
  - the name of each account holder;
- every reference number connected to the transaction that is meant to be similar to that of an account number; and
- every transaction identifier, including transaction hashes or similar identifiers (if applicable), and every sending and receiving address.

Retention: At least five years from the date the VC exchange transaction record was created.Footnote 36

i. Account records

For every account opened for a client, you must keep the following records:

Records for account holders and persons authorized to give instructions You must keep a record for every account holder (person, corporation, or other entity) and for every other person (up to three, in the case of a business account) who is authorized to give instructions in respect of the account.Footnote 37

For a **person,** the record must include their name, address, date of birth and their occupation, or in the case of a sole proprietor, the nature of their principal business.Footnote 38

For an account holder that is **a corporation or an entity other than a corporation**, the record must include its name, address and the nature of its principal business.Footnote 39

For a **corporation**, you must also keep a copy of the part of its official corporate records that contains any provision relating to the power to bind the corporation regarding the account.Footnote 40 This could be found in, for example:

- the articles of incorporation; or
- the bylaws of the corporation that set out the officers duly authorized to sign on behalf of the corporation, such as the president, treasurer, vice-president, comptroller, etc.

Retention: At least five years from the date the record was created. However, if this information is kept in one of the other account records, then the retention of that other record applies – at least five years from the date the account is closed.Footnote 41

Signature cards You must keep a signature card for every person authorized to give instructions on an account you open.Footnote 42 It can include the person's handwritten signature or an electronic signature that was created or adopted by the person.

An electronic signature can be numeric, character-based, or biometric, so long as it is unique to the person and a record can be kept. An electronic signature may also be encrypted. For example, a client's personal identification number (PIN) can be used as an electronic signature. FINTRAC's expectation is that it will be possible to review a signature card record during an examination, but the electronic signature does not need to be unencrypted.

You can keep a single signature card for a client that holds multiple accounts; you do not need to create a new signature card every time a client opens a subsequent account.

Retention: At least five years from the date the account was closed.Footnote 43

Intended use of an account You must keep a record of the intended use of an account.Footnote 44

Examples of the intended use of personal accounts include, but are not limited to:

- general chequing services, such as payment of family and household expenses;
- saving to fund a large purchase, retirement, or for a child's education; or
- receiving directly deposited employment or pension income.

Examples of the intended use of business accounts include, but are not limited to:

- depositing of daily business receipts (sales, etc.);
- making payments to employees (payroll);
- general business operating expenses; or
- making payments to suppliers.

Retention: At least five years from the date the account was closed.Footnote 45

Applications You must also keep a record of every application in respect of an account.Footnote 46

Retention: At least five years from the date the account was closed.Footnote 47

Account operating agreements You must keep every account operating agreement that you create or receive. An account operating agreement is a document that outlines the agreement between you and your client about the account's operation. For example, an application for a deposit account or a mortgage can include a reference to a separate document setting out the terms and conditions of the account's operation. The account operating agreement record in that case would include both the application and the separate document.Footnote 48

Retention: At least five years from the date the account was closed.Footnote 49

Debit and credit memos You must keep every debit and credit memo that you create or receive regarding an account. However, you do not need to keep a debit memo that relates to another account held at the same branch.Footnote 50 That is, you do not have to keep duplicate debit memos. If you have kept a debit memo in relation to two accounts at a given branch, you are only required to keep one memo on record.

Retention: At least five years from the date the debit or credit memo was created.Footnote 51

Deposit slips You must keep a deposit slip for every deposit to an account.Footnote 52 A deposit slip means a record that includes: Footnote 53

- the date of the deposit;
- the name of the person or entity that made the deposit;
- the amount of the deposit, and any part of the deposit that was made in cash;
- the method by which the deposit was made; and
- the number of the account the deposit went into and the name of each account holder.

Retention: At least five years from the date the deposit slips were created.Footnote 54

Account statements You must keep a copy of every account statement you send to an account holder.Footnote 55

Retention: At least five years from the date the account statements were created.Footnote 56

Cleared cheque records You must keep a record of every cleared cheque drawn on an account, and a copy of every cleared cheque that is deposited to an account.Footnote 57

This does not apply to cheques drawn from an account and deposited to an account at the same branch.

It also does not apply if an image of the cheque has been recorded electronically or on microfilm, which can be readily reproduced, and it can be readily ascertained where the image is recorded.

Retention: At least five years from the date the cleared cheques records were created and at least five years from the date the image was recorded in the case of a microfilm or electronic medium.Footnote 58

Credit arrangement records You are required to keep the following information with respect to a credit arrangement that you have entered into with a client: Footnote 59

- a record of the client's financial capacity;
- the terms of the credit arrangement;
- the nature of the client's principal business or their occupation; and
- if the client is a person, the name and address of their business or place of work.

Retention: At least five years from the date the account was closed.Footnote 60

j. Credit card account and related transaction records

Records for account holders and persons authorized to give instructions You must keep a record for every credit card account holder (person, corporation, or other entity) and for every other person (up to three, in the case of a business account) that is authorized to give instructions in respect of the account.Footnote 61

For a **person,** the record must include their name, address, date of birth and occupation or, in the case of a sole proprietor, the nature of their principal business.Footnote 62

For an account holder that is **a corporation or an entity other than a corporation**, the record must include its name, address and the nature of its principal business.Footnote 63

For **a corporation**, you must also keep a copy of the part of its official corporate records that contains provisions relating to the power to bind the corporation in respect of the credit card account or credit card transactions.Footnote 64 This could be found in, for example:

- the articles of incorporation; or

- the bylaws of the corporation that set out the officers duly authorized to sign on behalf of the corporation, such as the president, treasurer, vice-president, comptroller, etc.

Retention: At least five years from the date the record was created. However, if this information is kept in one of the other credit card account records, then the retention of that other record applies – at least five years from the date the account is closed. Footnote 65

Other account records You must keep the following records for every credit card account:

- every credit card application related to the account;Footnote 66 and
- a copy of every credit card statement that you sent to an account holder.Footnote 67

Retention: You must keep a credit card application for at least five years from the date the account was closed and credit card statements for at least five years from the day they were created.Footnote 68

Transaction records You must keep the following records when transactions are related to a credit card account:

- a foreign currency exchange transaction ticket for every foreign currency exchange transaction (See Foreign currency exchange transaction tickets);Footnote 69
- a VC exchange transaction ticket for every VC exchange transaction (See VC exchange transaction tickets);Footnote 70
- a record of the initiation of an international EFT of $1,000 or more that was requested by a person or an entity and for which the funds were transferred from the account (See Initiating an EFT of $1,000 or more);Footnote 71and
- a record of the final receipt of an international EFT of $1,000 or more that was remitted to a beneficiary by payment to the credit card account (See Final receipt of an international EFT of $1,000 or more).Footnote 72

Retention: At least five years from the date the transaction records were created.Footnote 73

k. Prepaid payment product account and transaction records

Records for account holders and authorized users You must keep a record for every prepaid payment product (PPP) account holder (person, corporation, or other entity) and for every authorized user.Footnote 74

For a **person,** the record must include their name, address, date of birth, occupation and in the case of a sole proprietor, the nature of their principal business.Footnote 75

For each PPP account holder that is **a corporation or an entity other than a corporation**, the record must include its name, address and the nature of its principal business.Footnote 76

When you open a PPP account for a **corporation**, you must also keep a copy of the part of its official corporate records that contains any provision relating to the power to bind the corporation in respect of the PPP account or PPP account transactions.Footnote 77

Retention: At least five years from the date the record was created. However, if this information is kept in one of the other account records, then the retention of that other record applies – at least five years from the date the account is closed.Footnote 78

Other account records You must keep the following records for every PPP account:

- every application related to the PPP account;Footnote 79
- every debit and credit memo you created or received related to the PPP account;Footnote 80
- a copy of every account statement sent to the holder of the PPP account;Footnote 81 and
- a prepaid payment product slip for every payment made to the PPP accountFootnote 82 that includes:
  - the date of the payment;
  - the name of the person or entity that made the payment;
  - the type and amount of each type of funds or each of the VC's involved in the payment;
  - the method by which the payment was made;
  - the name of each PPP account holder; and
  - the account number and, if different, the number that identifies the PPP that is connected to the account.Footnote 83

Retention: You must keep PPP account applications for at least five years from the date the account was closed and the other records listed above for at least five years from the date they were created.Footnote 84

PPP account transaction records You must keep the following records when transactions are related to a PPP account:

- a foreign currency exchange transaction ticket for every foreign currency exchange transaction (See Foreign currency exchange transaction tickets);Footnote 85
- a VC exchange transaction ticket for every VC exchange transaction (See VC exchange transaction tickets);Footnote 86

- a record of the initiation of an international EFT of $1,000 or more that was requested by a person or an entity for which the funds were transferred from a PPP account (See Initiating an EFT of $1,000 or more);Footnote 87
- a record of the final receipt of an international EFT of $1,000 or more that was remitted to a beneficiary by payment to a PPP account (See Final receipt of an EFT of $1,000 or more);Footnote 88
- a record of the transfer of VC in amount equivalent to $1,000 or more from a PPP account (See VC transfer in an amount equivalent to $1,000 or more);Footnote 89 and
- a record of the receipt of VC in an amount equivalent to $1,000 or more that was remitted to a beneficiary by payment to a PPP account (See Receipt of VC in an amount equivalent to $1,000 or more).Footnote 90

Retention: At least five years from the date the transaction records were created.Footnote 91

** **Note**: Please see FINTRAC's Prepaid payment products and prepaid payment product accounts guidance for more information.

l. Trust records

A trust company is an FE that is regulated by the Trust and Loan Companies Act or by an equivalent provincial Act. Trust companies have record keeping obligations related to the trusts for which they are the trustee.

A trust is a legal agreement by which financial assets are held by a person or an entity (a trustee) in trust for the benefit of another person, group of persons or entity (beneficiaries). The settlor of a trust is the person or entity that creates a trust with a written trust declaration.

You must keep the following records for every trust for which you are trustee, in addition to the transaction and account records listed previously in this guidance:Footnote 92

- a copy of the trust deed;
- if the settlor is a person, their name, address, date of birth and occupation or, in the case of a sole proprietor, the nature of their principal business; and
- if the settlor is an entity, its name, address and nature of its principal business.

You may also have record keeping obligations for certain institutional and inter vivos trusts. Institutional trusts are established by a corporation, partnership or other entity for a particular business purpose. Whereas, inter vivos trusts are established by a living person for the benefit of another person, such as a trust created by a parent for a child so that the trust's assets can be distributed to the child (beneficiary) during or after the parent's (settlor) lifetime.

If the trust is an institutional trust and the settlor is a corporation, you have to keep a copy of the part of the official corporate records that contains provisions relating to the power to bind the settlor/corporation in respect of the trust.

If the trust is an inter vivos trust (personal trust other than a trust created by a will), you have to keep a record about each of the beneficiaries that are known to you which must include:Footnote 93

- if the beneficiary is a person, their name, date of birth, address, telephone number and occupation or, in the case of a sole proprietor, the nature of their principal business;
- if the beneficiary is an entity, its name, address, telephone number and the nature of its principal business.

This information needs to be recorded for each beneficiary known to you at the time you become trustee of the trust.

2. What are my responsibilities when maintaining records?

In order to comply with your record keeping requirements, you must keep records in such a manner that they can be provided to FINTRAC within 30 days of a request.Footnote 94 The records may also be requested through a judicial order by law enforcement to support an investigation of money laundering or terrorist activity financing. A record (or a copy) may be kept in a machine-readable or electronic form, so long as a paper copy can easily be produced.Footnote 95

Employees who keep records for you are not required to keep them after their employment ends. The same is true for persons in a contractual relationship with you, when the contractual relationship ends, they no longer have to keep records for you.Footnote 96 You have to obtain and keep the records that were kept for you by an employee or a contractor before the end of the person's employment or contract.

There may be situations where you are required to keep records for purposes other than complying with your obligations under the PCMLTFA. For example, a federal or provincial regulator may require you to keep records in addition to those described in this guidance. If this is the case, you must still meet the requirements described in this guidance. For example, the retention period for your records can be longer than what is described, but it cannot be shorter.

3. What are the exceptions to the record keeping requirements?

If you are required to keep a record with information that is readily available in other records, you do not have to record the information again.Footnote 97

For example, when you keep a copy of a large cash transaction report (LCTR) you may choose to use this as your large cash transaction record for the same

transaction, so long as **all of the information** that would otherwise be kept in the large cash transaction record is captured within the report. Any requirement related to keeping the large cash transaction record would still apply, such as verifying identity.

EFTs conducted by credit/debit card or PPP You do not need to keep the following records associated with a credit/debit card or PPP transaction if the beneficiary has an agreement with the payment service provider that allows for the payment of goods and services by those means when you:Footnote 98

- initiate, send or are the final recipient of an international EFT of $1,000 or more; or
- initiate or are the final recipient of an international EFT of $1,000 or more where the funds are transferred from or to a credit card or PPP account.

Payment card processing activities

If you are processing credit card or PPP payments on behalf of a merchant (for example, credit card acquiring), the record keeping requirements described in this guidance do not apply to those activities.Footnote 99

A credit card acquiring business is an FE that has an agreement with a merchant to provide the following services:

- enabling the merchant to accept credit card payments by cardholders for goods and services and to receive payment for credit card purchases;
- processing services, payment settlements and providing point-of-sale equipment (such as computer terminals); and
- providing other ancillary services to the merchant.

Financial entities, public bodies, and very large corporations or trusts

You do not have to keep a large cash transaction record or a large VC transaction record if the cash or VC was received from another FE, a public body, or a person who is acting on behalf of a client that is an FE or public body.Footnote 100

If you receive $3,000 or more from a client that is an FE, or a person who is acting on behalf of a client that is an FE, for the issuance of traveller's cheques, money orders or other similar negotiable instruments, you are not required to keep a record of the transaction.Footnote 101

If you open an account, a credit card account, a PPP account, or conduct a transaction for a public body, a very large corporation or trust, or a subsidiary of those entities if the financial statements of the subsidiary are consolidated with those of the public body, very large corporation or trust, you are not required to keep the following records:Footnote 102

- Records of transactions of $3,000 or more;
- Records of EFTs of $1,000 or more;

- Records of VC transfers and receipt equivalent to $1,000 or more;
- Foreign currency exchange transaction records;
- VC exchange transaction records;
- Account records;
- PPP account records;
- Credit card account records; and
- Trust records.

Virtual currency

When you transfer or receive VC as compensation for the validation of a transaction that is recorded in a distributed ledger, **or** when you exchange, transfer, or receive a nominal amount of VC for the sole purpose of validating a different transaction or a transfer of information, you do not need to keep a record of: Footnote 103

- large VC transactions;
- transfers of $1,000 or more in VC at the request of a person or entity;
- receipt of $1,000 or more in VC for remittance to a beneficiary; or
- VC exchange transaction tickets.

Other record keeping exempted activities You do not have to keep the transaction and account records identified in this guidance for the following activities:Footnote 104

- the sale of an exempt policy as defined in subsection 306(1) of the Income Tax Regulations;
- the sale of a group life insurance policy that does not provide for a cash surrender value or a savings component;
- the sale of an immediate or deferred annuity that is paid for entirely with funds that are directly transferred from a registered pension plan or from a pension plan that is required to be registered under the Pension Benefits Standards Act, 1985, or similar provincial legislation;
- the sale of a registered annuity policy or a registered retirement income fund;
- the sale of an immediate or deferred annuity that is paid for entirely with the proceeds of a group life insurance policy;
- a transaction that is part of a reverse mortgage or a structured settlement;
- the opening of an account for the deposit and sale of shares from a corporate demutualization or the privatization of a Crown corporation;
- the opening of an account in the name of an affiliate of an FE, if that affiliate carries out activities that are similar to those of persons and entities referred to in paragraphs 5(a) to (g) of the PCMLTFA;
- the opening of a registered plan account, including a locked-in retirement plan account, a registered retirement savings plan account and a group registered retirement savings plan account;

- the opening of an account established in accordance with the escrow requirements of a Canadian securities regulator, the Canadian stock exchange, or any provincial legislation;
- the opening of an account where the account holder or settlor is a pension fund that is regulated under federal or provincial legislation;
- the opening of an account in the name of or in respect of which, instructions are authorized to be given by an FE, a securities dealer or a life insurance company or by an investment fund that is regulated under provincial securities legislation; or
- an account opened solely to provide customer accounting services to a securities dealer.

These exceptions do not apply to large cash transactions, large VC transactions, or suspicious transactions.

Group Plans If you open a group plan account (other than those for which exceptions already apply) you do **not** have to keep a signature card for a person who is a member of the plan if:

- the identity of the entity that is the plan sponsor has been verified; and
- the individual member contributions are made by the sponsor of the plan or by payroll deductions.Footnote 105# When to verify the identity of persons and entities—Financial entities

Overview

This guidance on client identification describes **when** financial entities (FEs) must verify the identity of persons and entities as required by the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and associated Regulations.

Who is this guidance for

- Financial entities

1. When do I have to verify the identity of persons and entities?

As an FE, you must verify the identity of clients for the following:

1. Large cash transactions
2. Large virtual currency (VC) transactions
3. Suspicious transactions
4. Issuing or redeeming money orders, traveller's cheques or other similar negotiable instruments of $3,000 or more

5. Initiating an international electronic funds transfer (EFT)—or any other EFT that is a SWIFT MT-103 message or its equivalent—of $1,000 or more
6. Remitting funds to the beneficiary of an international EFT of $1,000 or more
7. Transferring VC in an amount equivalent to $1,000 or more
8. Remitting VC to a beneficiary in an amount equivalent to $1,000 or more
9. Foreign currency exchange transactions of $3,000 or more
10. VC exchange transactions in amounts equivalent to $1,000 or more
11. Accounts—account holders and persons authorized to give instructions
12. Credit card accounts—account holders
13. Prepaid payment product (PPP) accounts
    - Account holders
    - Authorized users
    - Payments of $1,000 or more to PPP account
14. Trusts—settlors or co-trustees of a trust

a. Large cash transactions

You must verify the identity of every person or entity from which you receive $10,000 or more in cash when the transaction takes place.Footnote 1 This includes a situation where you are deemed to have received cash because you have authorized another person or entity to receive it on your behalf.

****Note**: This obligation is subject to the 24-hour rule.

b. Large virtual currency (VC) transactions

You must verify the identity of every person or entity from which you receive VC in an amount equivalent to $10,000 or more when the transaction takes place.Footnote 4 This includes a situation where you are deemed to have received VC because you have authorized another person or entity to receive it on your behalf.Footnote 5

****Note**: This obligation is subject to the 24-hour rule.

c. Suspicious transactions

You must take reasonable measures to verify the identity of every person or entity that conducts or attempts to conduct a suspicious transaction, regardless of the transaction amount, and including transactions that would normally be exempt from client identification requirements, before sending a Suspicious Transaction Report (STR).Footnote 7

d. Issuing or redeeming money orders, traveller's cheques or other similar negotiable instruments of $3,000 or more

You must verify the identity of every person who requests that you issue or redeem money orders, traveller's cheques or similar negotiable instruments of $3,000 or more when the transaction is being requested. Footnote 8

e. Initiating an international electronic funds transfer (EFT)—or any other EFT that is a SWIFT MT-103 message or its equivalent—of $1,000 or more

You must verify the identity of every person who requests the initiation of an international EFT or any other EFT that is a SWIFT MT-103 or its equivalent, including domestic SWIFT MT-103, of $1,000 or more when the transaction is being requested.Footnote 9

f. Remitting funds to the beneficiary of an international EFT of $1,000 or more

You must verify the identity of every person you remit funds to who is the beneficiary of an international EFT of $1,000 or more when the transaction takes place.Footnote 10

g. Transferring VC in an amount equivalent to $1,000 or more

You must verify the identity of every person who requests the transfer of VC in an amount equivalent to $1,000 or more when the transaction is being requested.Footnote 11

h. Remitting VC to a beneficiary in an amount equivalent to $1,000 or more

You must verify the identity of every person you remit VC to as the beneficiary of a transfer that is equivalent to $1,000 or more when the transaction takes place.Footnote 12

i. Foreign currency exchange transactions of $3,000 or more

You must verify the identity of every person who requests a foreign currency exchange of $3,000 or more when the transaction takes place.Footnote 13

j. VC exchange transactions in amounts equivalent to $1,000 or more

You must verify the identity of every person who requests that you exchange VC for funds, funds for VC, or one VC for another, in an amount equivalent to $1,000 or more when the transaction is being requested.Footnote 14

k. Accounts—Account holders and persons authorized to give instructions

Account holders You must verify the identity of every person, corporation, and entity other than a corporation for which you open an account.Footnote 15 You must do this **before** the first transaction other than when the initial deposit is carried out.Footnote 16

Persons authorized to give instructions You must verify the identity of every person authorized to give instructions on an account before the first transaction, other than the initial deposit, is carried out on the account.Footnote 17

This includes verifying the identity of the individual members of a **group plan account** who are authorized to give instructions **,** when a contribution to the plan is made in respect of the member.Footnote 18

You cannot open an account for a person, corporation, or other entity if you cannot verify their identity in accordance with the Regulations.Footnote 19

l. Credit card accounts—account holders

You must verify the identity of every person, corporation, and other entity for which you open a credit card accountFootnote 20 before the credit card can be activated.Footnote 21 If credit cards are issued for persons other than the account holder, you must record their information if they are authorized to give instructions on an account, but you do not have to verify their identity.

For example, a parent applying for a credit card account requests that a credit card be issued on that account for their child, and that child be authorized to give instructions on that account. In this example, the parent's identity has to be verified because the parent is the account holder, the child's identity does not need to be verified.

If there are two or more co-applicants for a credit card account (in other words, if a credit card account is opened in the name of more than one person), the identification requirement applies to all co-applicants.

m. Prepaid payment product (PPP) accounts

Account holders You must verify the identity of every person, corporation, and other entity for which you open a PPP accountFootnote 22 before the PPP account is activated.Footnote 23

Authorized users You must also verify the identity of every authorized user of the PPP accountFootnote 24 before the first transaction is carried out.Footnote 25

Payments of $1,000 or more to PPP Accounts You must verify the identity of every person, corporation, and other entity that makes a payment of $1,000 or more to a PPP accountFootnote 26 when the transaction takes place.Footnote 27

n. Trusts—settlors or co-trustees of a trust

If you are a trust company, you must verify the identity of every person who is the **settlor** of an inter vivos trust for which you are a trustee.Footnote 28

You must also verify the identity of a corporation or an entity other than a corporation that is the **settlor** of an institutional trust for which you are a trustee.Footnote 29

You must verify the identity of any person who is authorized to act as **co-trustee** of a trust.Footnote 30 If an entity is authorized to act as **co-trustee** of a trust, you must verify its identity and the identity of all persons authorized to give instructions on its behalf (up to three).Footnote 31

You must verify the identity of a person or an entity within 15 days after the day on which the trust company becomes the trustee.Footnote 32

2. What is the difference between verifying identity and keeping client identification information up to date?

As part of your ongoing monitoring requirements for business relationships, you must keep client identification information up to date, at a frequency that will vary based on your risk assessment, and as outlined in your policies and procedures.Footnote 33 This does not require you to re-identify clients in accordance with the methods to verify identity. As explained in the ongoing monitoring guidance, the requirement is only for you to keep client identification information up to date. This is understood to be information that you have about your client such as their name and address. In the case of a person, this would also include, but is not limited to, the nature of their principal business or their occupation; and in the case of an entity, the nature of its principal business.

3. What are the exceptions to client identification requirements?

You do not have to re-identify a person or an entity if you previously did so using the methods specified by the Regulations in place at the time, and kept the associated records, so long as you have no doubts about the information used.Footnote 34

Large cash transactions

You do not have to verify the identity of a person or entity that conducts a large cash transaction if:

- you receive the cash from another FE or a public body, or from a person who is acting on behalf of a client that is an FE or a public body;Footnote 35 or
- the amount received is deposited to a business account or is deposited in an automated banking machine (including a quick drop or night deposit).Footnote 36

Large VC transactions

You do not have to verify the identity of a person or entity that conducts a large VC transaction if you receive the VC from a client that is an FE or a public body, or from a person acting on behalf of a client that is an FE or public body.Footnote 37

When you transfer or receive VC as compensation for the validation of a transaction that is recorded in a distributed ledger **or** you exchange, transfer or receive a nominal amount of VC for the sole purpose of validating another transaction or a transfer of information – you do not need to keep a large VC transaction record and do not need to verify identity.Footnote 38

Suspicious transactions

You do not have to take reasonable measures to verify the identity of the person or entity that conducts or attempts to conduct a suspicious transaction if:

- you have already verified the identity of the person or entity and have no doubts about the identification information;Footnote 39 or
- you believe that verifying the identity of the person or entity would inform them that you are submitting an STR.Footnote 40

EFT by credit/debit card or PPP

Your client identification requirements do not apply when you carry out the following transactions for a person by means of a credit/debit card or PPP, if the beneficiary has an agreement with the payment service provider that permits payments by those means for goods and services:Footnote 41

- initiate an international EFT of $1,000 or more; or
- are the final recipient of an international EFT, or of a VC transfer equivalent to $1000 or more and remit the funds to the beneficiary.

Payment card processing activities

Client identification requirements do not apply to processing credit card or PPP payments on behalf of a merchant.Footnote 42

Public bodies, very large corporations and trusts

When opening an account, including a credit card account, PPP account or trust account, you do not have to verify the identity of a person or entity if it is for:Footnote 43

- a public body;
- a very large corporation or trust; or
- a subsidiary of those types of entities, if the financial statements of the subsidiary are consolidated with those of the public body, or very large corporation or trust.

Account openings

You do not have to verify the identity of the person that opens an account, is authorized to give instructions in respect of an account, opens a credit card account, or is the settlor or co-trustee of a trust in the following circumstances:Footnote 44

- if the person already has an account with you and opens a subsequent account;
- if the person is authorized on a business account, so long as you have verified the identity of at least three persons authorized to give instructions on the account. If one of the three identified persons leaves the business, you must verify the identity of another person authorized on the account;
- an account that is opened for the sale of mutual funds where there are reasonable grounds to believe that the client's identity has been verified by a securities dealer in accordance with the Regulations in respect of:
  - the sale of the mutual funds for which the account has been opened, or
  - a transaction that is part of a series of transactions that includes that sale; and
- an account that is opened at the request of an entity for the deposit, by a life insurance company affiliated with that entity, of a death benefit under a life insurance policy or annuity where:
  - the account is opened in the name of a beneficiary that is a person;
  - only the death benefit may be deposited in the account, and;
  - the policy or annuity contract, under which the death benefit claim was made, has been in existence for at least two years before the death benefit claim was made.

Other activities exempted from client identification requirements

You do not have to verify the identity of persons and entities, as listed in this guidance, for the following:Footnote 45

- the sale of an exempt policy as defined in subsection 306(1) of the Income Tax Regulations;

- the sale of a group life insurance policy that does not provide for a cash surrender value or a savings component;
- the sale of an immediate or deferred annuity that is paid for entirely with funds that are directly transferred from a registered pension plan or from a pension plan that must be registered under the Pension Benefits Standards Act, 1985 or similar provincial legislation;
- the sale of a registered annuity policy or a registered retirement income fund;
- the sale of an immediate or deferred annuity that is paid for entirely with funds from the proceeds of a group life insurance policy;
- a transaction that is part of a reverse mortgage (a loan based on the equity of a home) or a structured settlement (a financial or insurance arrangement to resolve a personal injury claim);
- the opening of an account for the deposit and sale of shares from a corporate demutualization or the privatization of a Crown corporation;
- the opening of an account in the name of an affiliate of an FE, if that affiliate carries out activities that are similar to those of persons and entities referred to in paragraphs 5(a) to (g) of the Act;
- the opening of a registered plan account, including a locked-in retirement plan account, a registered retirement savings plan account, and a group registered retirement savings plan account;
- the opening of an account established pursuant to the escrow requirements of a Canadian securities regulator or Canadian stock exchange or any provincial legislation;
- the opening of an account where the account holder or settlor is a pension fund that is regulated under federal or provincial legislation;
- the opening of an account in the name of, or in respect of which instructions are authorized to be given by an FE, a securities dealer, a life insurance company, or an investment fund that is regulated under provincial securities legislation; and
- the opening of an account solely to provide customer accounting services to a securities dealer.

These exceptions do not apply to large cash transactions, large VC transactions, or suspicious transactions.

Group Plans

If you open a group plan account, other than those for which exceptions already apply, you do **not** have to verify the identity of the individual members of the plan if:

- the identity of the entity that is the plan sponsor has been verified; and
- the individual member contributions are made by the sponsor of the plan or by payroll deduction.# Correspondent banking relationship requirements : FINTRAC's compliance guidance

From: Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)

This guidance explains the correspondent banking relationship requirements under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (the Act) and associated Regulations that apply to financial entities.

In this guidance

Related links

Related acts and regulations

- Proceeds of Crime (Money Laundering) and Terrorist Financing Act
- Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations
- Proceeds of Crime (Money Laundering) and Terrorist Financing Suspicious Transaction Reporting Regulations

Related guidance

- Compliance program requirements
- Risk assessment guidance
- Reporting suspicious transactions to FINTRAC
- Special Bulletin on financial activity associated with suspected sanctions evasion
- Report suspected sanctions evasion
- Reporting terrorist property to FINTRAC
- Voluntary self-declaration of non-compliance

Related resources

- Policy interpretations database
- Penalties for non-compliance
- Guidance glossary
- Learning resources for businesses

1. Who must comply

The following Canadian financial entities are subject to the correspondent banking requirement if it enters into a correspondent banking relationship:

- bank
- cooperative credit society
- credit union
- caisse populaire
- federally or provincially regulated trust or loan company
- unregulated trust company
- financial services cooperative
- life insurance company, or an entity that is a life insurance broker or agent, that offers loans or prepaid payment products to the public, **or** maintains accounts for these loans or prepaid payment products, other than:
  - loans made by the insurer to a policy holder if the insured person has a terminal illness that significantly reduces their life expectancy and the loan is secured by the value of an insurance policy
  - loans made by the insurer to a policy holder for the sole purpose of funding the life insurance policy
  - advance payments made by the insurer to a policy holder who is entitled to them
- credit union central when it offers financial services to non-members
- an agent of the Crown when it accepts deposit liabilities while providing financial services to the public
- loan companies regulated by a Provincial Act

Legal references

- Proceeds of Crime (Money Laundering) and Terrorist Financing Act, S.C. 2000, Chapter.17, paragraphs 5(a),(b), (d), (e), (e.1), and (f)
- Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations, SOR/2002-184, section 16(1)

2. What is a correspondent banking relationship

A correspondent banking relationship is created by an agreement or arrangement between a prescribed foreign financial institution and a Canadian financial entity (as defined above). In this relationship, the Canadian financial entity provides prescribed services to the foreign financial institution or international electronic funds transfers, cash management, or cheque clearing services.

Legal references

- Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations, SOR/2002-184, subsection 9.4 (3)

3. What must I do to meet the requirements

Before you enter into a correspondent banking relationship, you **must**:

- Obtain information about the foreign financial institution and its activities to fulfil the related **verifying** and **record keeping requirements** outlined in this guidance.
- Ensure that the foreign financial institution is not a shell bank.
  - If it is a shell bank, you **cannot** enter into the correspondent banking relationship.
- Obtain the approval of senior management to enter into the correspondent banking relationship.
- Set out in writing your obligations and the foreign financial institution's obligations for the correspondent banking services (for example, your correspondent banking agreement or arrangement, or product agreements).

When you enter into a correspondent banking relationship, you **must also** do the following:

- Periodically conduct ongoing monitoring of the correspondent banking relationship, at a frequency appropriate to the level of risk determined in your risk assessment, for the purpose of:
  - detecting any suspicious transactions that you are required to report to FINTRAC
  - keeping the information that is required to enter into a correspondent banking relationship up to date
  - ensure that the foreign financial institution has appropriate anti-money laundering and anti-terrorist financing measures in place
  - reassessing the level of risk associated with the foreign financial institution's transactions, and
  - determining whether the transactions or activities are consistent with the information obtained about the foreign financial institution and with your risk assessment
- Verify the name and address of the foreign financial institution by examining a copy of:
  - the foreign financial institution's banking licence
  - its banking charter
  - the authorization or certification to operate that is issued by the competent authority under the legislation of the jurisdiction in which the foreign financial institution was incorporated
  - its certificate of incorporation, or

  - a similar document.

- Take reasonable measures to verify, based on publicly available information, if civil or criminal penalties have been imposed on the foreign financial institution for not respecting anti-money laundering, or anti-terrorist financing requirements, and
  - **if penalties have been imposed**, you must monitor all transactions conducted in the context of the correspondent banking relationship to detect any suspicious transactions that must be reported to FINTRAC.
- Take reasonable measures to assess, based on publicly available information:
  - the reputation of the foreign financial institution with respect to its compliance with anti-money laundering and anti-terrorist financing requirements, and
  - the quality of the anti-money laundering and anti-terrorist financing supervision of the jurisdiction in which the foreign financial institution was incorporated, and the jurisdiction that it conducts transactions in the context of the correspondent banking relationship.
- Take reasonable measures to determine the nature of the clientele and markets served by the foreign financial institution.
- Take reasonable measures to ascertain whether the foreign financial institution has anti-money laundering, and anti-terrorist financing policies and procedures in place, including procedures for the approval of the opening of new accounts, and
  - **if the reasonable measures you took were unsuccessful or the policies and procedures are not in place**, you must take reasonable measures to monitor all transactions conducted in the context of the correspondent banking relationship for the purpose of detecting suspicious transactions.
- As part of your risk assessment within your compliance program, you must assess and document money laundering, or terrorist activity financing risks related to your correspondent banking relationships.

Legal references

- Proceeds of Crime (Money Laundering) and Terrorist Financing Act
  - section 7
  - subsection 9.31(1)
  - subsection 9.4(1)
- Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations, SOR/2002-184

  - subsection 16(3.1)
  - paragraphs 90(a), 90(b) and 90(c)
  - subsection 16(3)
  - paragraph 156(c) (i)

- Proceeds of Crime (Money Laundering) and Terrorist Financing Suspicious Transaction Reporting Regulations, SOR/2001-317
  - section 9

4. What correspondent banking relationship records do I need to keep

When you enter into a correspondent banking relationship, you must keep the following records:

- A record of the foreign financial institution's name and address, primary business line and the names of its directors.
- A copy of the foreign financial institution's most recent annual report or audited financial statement.
- A copy of one of the following:
  - the foreign financial institution's banking license, banking charter, authorization or certification to operate issued by the competent authority under the legislation of the jurisdiction in which it was incorporated
  - its certificate of incorporation, or
  - a similar document.
- A copy of the correspondent banking agreement or arrangement, or product agreements, defining the respective responsibilities of your financial entity and of the foreign financial institution.
- A record of the anticipated correspondent banking account activity of the foreign financial institution, including the products or services to be used.
- A written statement from the foreign financial institution that it does not have, directly or indirectly, a correspondent banking relationship with a shell bank.
- A written statement from the foreign financial institution that it is in compliance with anti-money laundering, and anti-terrorist financing legislation in every jurisdiction in which it operates.
- A record of measures taken to determine the nature of the clientele and markets served by the foreign financial institution.
- A record of the measures taken to ascertain whether any civil or criminal penalties have been imposed on the foreign financial institution for not re-

specting anti-money laundering, and anti-terrorist financing requirements, and the results of those measures.

- A record of the measures taken to assess the reputation of the foreign financial institution with respect to its compliance with anti-money laundering and anti-terrorist financing requirements and the result of those measures.
- A record of the measures taken to assess the quality of the anti-money laundering and anti-terrorist financing supervision of the jurisdiction in which the foreign financial institution is incorporated and the jurisdiction in which it conducts transactions in the context of the correspondent banking relationship, and the results of those measures.
- A copy of every Suspicious Transaction Report and Terrorist Property Report sent to FINTRAC as a result of your correspondent banking relationship(s).

Retention: At least five years after the day on which the last business transaction is conducted.

Legal references

- Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations, SOR/2002-184
  - subsection 16(2)
  - paragraph 148 (1)(b)

5. What must I do if the client of a foreign financial institution has direct access to the services I provide

If, as part of a correspondent banking relationship, a client of the foreign financial institution has direct access to services you provide, you must take reasonable measures to verify whether the foreign financial institution:

- has met requirements that are consistent with your requirements for verifying client identification for this client, and
- has agreed to provide relevant client identification information to you upon request.

Legal references

- Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations, SOR/2002-184
  - section 91

6. What are the exceptions to correspondent banking relationship requirements

For a correspondent banking relationship, you do not need to keep account opening and transaction records (other than what is included in this Guidance) when you open an account for a foreign financial institution.

Also, certain correspondent banking relationship requirements do not apply to your activities related to the processing of payments by credit card or prepaid payment product for a merchant, including:

- Keeping correspondent banking relationships records (as listed under What correspondent banking relationship records do I need to keep)
- Taking reasonable measures to determine whether the foreign financial institution has anti-money laundering and anti-terrorist financing policies and procedures in place, including procedures for the approval of the opening of new accounts, and
  - **if the reasonable measures you took were unsuccessful or the policies and procedures are not in place**, you must take reasonable measures to monitor all transactions conducted in the context of the correspondent banking relationship for the purpose of detecting suspicious transactions and terrorist activities.
- Periodically conducting ongoing monitoring of the correspondent banking relationship, at a frequency appropriate to the level of risk determined in your risk assessment, for the purpose of:
  - detecting any suspicious or terrorist activity financing transactions that you are required to report to FINTRAC
  - keeping the information that is required to enter a correspondent banking relationship (see above) up to date
  - reassessing the level of risk associated with the foreign financial institution's transactions and activities related to the correspondent banking relationship, and
  - determining whether transactions and activities are consistent with the information obtained, through the risk assessment, of the foreign financial institution

Legal references

- Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations, SOR/2002-184
  - section 16
  - section 150

For assistance

If you have questions on your requirements, please contact FINTRAC by email at guidelines-lignesdirectrices@fintrac-canafe.gc.ca.

Definitions

Accountant

A chartered accountant, a certified general accountant, a certified management accountant or, if applicable, a chartered professional accountant. (comptable)

Reference:

Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFR), SOR/2002-184, s. 1(2).

Accounting firm

An entity that is engaged in the business of providing accounting services to the public and has at least one partner, employee or administrator that is an accountant. (cabinet d'expertise comptable)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Act

The Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA). (la Loi)

Reference:

Proceeds of Crime (Money Laundering) and Terrorist Financing Administrative Monetary Penalties Regulations (PCMLTFAMPR), SOR/2007-292, s. 1, Proceeds of Crime (Money Laundering) and Terrorist Financing Registration Regulations (PCMLTFRR), SOR/2007-121, s. 1, PCMLTFR, SOR/2002-184, s. 1(2), and Proceeds of Crime (Money Laundering) and Terrorist Financing Suspicious Transaction Reporting Regulations (PCMLTFSTRR), SOR/2001-317, s. 1(2).

Administrative monetary penalties (AMPs)

Civil penalties that may be issued to reporting entities by FINTRAC for non-compliance with the PCMLTFA and associated Regulations. (pénalité administrative pécuniaire [PAP])

Affiliate

An entity is affiliated with another entity if one of them is wholly owned by the other, if both are wholly owned by the same entity or if their financial statements are consolidated. (entité du même groupe)

Reference:

PCMLTFR, SOR/2002-184, s. 4.

Annuity

Has the same meaning as in subsection 248(1) of the Income Tax Act. (rente)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Armoured cars

Persons or entities that are engaged in the business of transporting currency, money orders, traveller's cheques or other similar negotiable instruments. (Véhicules blindés)

As soon as practicable

A time period that falls in-between immediately and as soon as possible, within which a suspicious transaction report (STR) must be submitted to FINTRAC. The completion and submission of the STR should take priority over other tasks. In this context, the report must be completed promptly, taking into account the facts and circumstances of the situation. While some delay is permitted, it must have a reasonable explanation. (aussitôt que possible)

Attempted transaction

Occurs when an individual or entity starts to conduct a transaction that is not completed. For example, a client or a potential client walks away from conducting a $10,000 cash deposit. (opération tentée)

Authentic

In respect of verifying identity, means genuine and having the character of an original, credible, and reliable document or record. (authentique)

Authorized person

A person who is authorized under subsection 45(2). (personne autorisée)

Reference:

Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA), S.C. 2000, c 17, s. 2(1).

Authorized user

A person who is authorized by a holder of a prepaid payment product account to have electronic access to funds or virtual currency available in the account by means of a prepaid payment product that is connected to it. (utilisateur autorisé)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Beneficial owner(s)

Beneficial owners are the individuals who are the trustees, and known beneficiaries and settlors of a trust, or who directly or indirectly own or control 25% or more of i) the shares of a corporation or ii) an entity other than a corporation or trust, such as a partnership. The ultimate beneficial owner(s) cannot be another corporation or entity; it must be the actual individual(s) who owns or controls the entity. (bénéficiaire effectif)

Beneficiary

A beneficiary is the individual or entity that will benefit from a transaction or to which the final remittance is made. (bénéficiaire)

Branch

A branch is a part of your business at a distinct location other than your main office. (succursale)

British Columbia notary corporation

An entity that carries on the business of providing notary services to the public in British Columbia in accordance with the Notaries Act, R.S.B.C. 1996, c. 334. (société de notaires de la Colombie-Britannique)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

British Columbia notary public

A person who is a member of the Society of Notaries Public of British Columbia. (notaire public de la Colombie-Britannique)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Cash

Coins referred to in section 7 of the Currency Act, notes issued by the Bank of Canada under the Bank of Canada Act that are intended for circulation in Canada or coins or bank notes of countries other than Canada. (espèces)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2) and PCMLTFSTRR, SOR/2001-317, s. 1(2).

Casino

A government, organization, board or operator that is referred to in any of paragraphs 5(k) to (k.3) of the Act. (casino)

Reference:

PCMLTFR, SOR/2002-184, s 1(2) and PCMLTFSTRR, SOR/2001-317, s. 1(2).

Certified translator

An individual that holds the title of professional certified translator granted by a Canadian provincial or territorial association or body that is competent under Canadian provincial or territorial law to issue such certification. (traducteur agréé)

Clarification request

A clarification request is a method used to communicate with money services businesses (MSBs) or foreign money services businesses (FMSBs) when FINTRAC needs more information about their registration form. This request is usually sent by email. (demande de précisions)

Client

A person or entity that engages in a financial transaction with another person or entity. (client)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 2(1).

Client identification information

The identifying information that you have obtained on your clients, such as name, address, telephone number, occupation or nature of principal business, and date of birth for an individual. (renseignements d'identification du client)

Competent authority

For the purpose of the criminal record check submitted with an application for registration, a competent authority is any person or organization that has the legally delegated or invested authority, capacity, or power to issue criminal record checks. (autorité compétente)

Completed transaction

Is a transaction conducted by a person or entity, that is completed and results in the movement of funds, virtual currency, or the purchase or sale of an asset. (opération effectuée)

Completing action

With respect to a reportable transaction, information related to the instructions provided by the person or entity making the request to the reporting entity to complete a transaction. For example, an individual arrives at a bank and requests to purchase a bank draft. The completing action is the details of how the reporting entity fulfilled the person or entity's instructions which led to the transaction being completed. This includes what the funds or virtual currency

initially brought to the reporting entity was used for (see "disposition"). A transaction may have one or more completing actions depending on the instructions provided by the person or entity. (action d'achèvement)

Compliance officer

The individual, with the necessary authority, that you appoint to be responsible for the implementation of your compliance program. (agent de conformité)

Compliance policies and procedures

Written methodology outlining the obligations applicable to your business under the PCMLTFA and its associated Regulations and the corresponding processes and controls you put in place to address your obligations. (politiques et procédures de conformité)

Compliance program

All elements (compliance officer, policies and procedures, risk assessment, training program, effectiveness review) that you, as a reporting entity, are legally required to have under the PCMLTFA and its associated Regulations to ensure that you meet all your obligations. (programme de conformité)

Context

Clarifies a set of circumstances or provides an explanation of a situation or financial transaction that can be understood and assessed. (contexte)

Correspondent banking relationship

A relationship created by an agreement or arrangement under which an entity referred to in any of paragraphs 5(a), (b), (d),(e) and (e.1) or an entity that is referred to in section 5 and that is prescribed undertakes to provide to a prescribed foreign entity prescribed services or international electronic funds transfers, cash management or cheque clearing services. (relation de correspondant bancaire)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 9.4(3) and PCMLTFR, SOR/2002-184, s. 16(1)(b).

Country of residence

The country where an individual has lived continuously for 12 months or more. The individual must have a dwelling in the country concerned. For greater certainty, a person only has one country of residence no matter how many dwelling places they may have, inside or outside of that country. (pays de résidence)

Credit card acquiring business

A credit card acquiring business is a financial entity that has an agreement with a merchant to provide the following services:

- enabling a merchant to accept credit card payments by cardholders for goods and services and to receive payments for credit card purchases;
- processing services, payment settlements and providing point-of-sale equipment (such as computer terminals); and
- providing other ancillary services to the merchant.

(entreprise d'acquisition de cartes de crédit)Credit union central

A central cooperative credit society, as defined in section 2 of the Cooperative Credit Associations Act, or a credit union central or a federation of credit unions or caisses populaires that is regulated by a provincial Act other than one enacted by the legislature of Quebec. (centrale de caisses de crédit)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Crowdfunding platform

A website or an application or other software that is used to raise funds or virtual currency through donations. (plateforme de sociofinancement)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Crowdfunding platform services

The provision and maintenance of a crowdfunding platform for use by other persons or entities to raise funds or virtual currency for themselves or for persons or entities specified by them. (services de plateforme de sociofinancement)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Current

In respect of a document or source of information that is used to verify identity, is up to date, and, in the case of a government-issued photo identification document, must not have been expired when the ID was verified. (à jour)

Dealer in precious metals and stones

A person or entity that, in the course of their business activities, buys or sells precious metals, precious stones or jewellery. It includes a department or an agent of His Majesty in right of Canada or an agent or mandatary of His Majesty in right of a province when the department or the agent or mandatary carries out the activity, referred to in subsection 65(1), of selling precious metals to the public. (négociant en métaux précieux et pierres précieuses)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Deferred profit sharing plan

Has the same meaning as in subsection 248(1) of the Income Tax Act. (régime de participation différée aux bénéfices)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Deposit slip

A record that sets out:

1. (a) the date of the deposit;
2. (b) the name of the person or entity that makes the deposit;
3. (c) the amount of the deposit and of any part of it that is made in cash;
4. (d) the method by which the deposit is made; and
5. (e) the number of the account into which the deposit is made and the name of each account holder.

(relevé de dépôt)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Directing services

A business is directing services at persons or entities in Canada if at least one of the following applies:

- The business's marketing or advertising is directed at persons or entities located in Canada;
- The business operates a ".ca" domain name; or,
- The business is listed in a Canadian business directory.

Additional criteria may be considered, such as if the business describes its services being offered in Canada or actively seeks feedback from persons or entities in Canada. (diriger des services)

Distributed ledger

For the purpose of section 151 of the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFR), a digital ledger that is maintained by multiple persons or entities and that can only be modified by a consensus of those persons or entities. (registres distribués)

Reference:

PCMLTFR, SOR/2002-184, s. 151(2).

Disposition

With respect to a reportable transaction, the disposition is what the funds or virtual currency was used for. For example, an individual arrives at a bank with cash and purchases a bank draft. The disposition is the purchase of the bank draft. (répartition)

Electronic funds transfer

The transmission—by any electronic, magnetic or optical means—of instructions for the transfer of funds, including a transmission of instructions that is initiated and finally received by the same person or entity. In the case of SWIFT messages, only SWIFT MT-103 messages and their equivalent are included. It does not include a transmission or instructions for the transfer of funds:

1. (a) that involves the beneficiary withdrawing cash from their account;
2. (b) that is carried out by means of a direct deposit or pre-authorized debit;
3. (c) that is carried out by cheque imaging and presentment
4. (d) that is both initiated and finally received by persons or entities that are acting to clear or settle payment obligations between themselves; or
5. (e) that is initiated or finally received by a person or entity referred to in paragraphs 5(a) to (h.1) of the Act for the purpose of internal treasury management, including the management of their financial assets and liabilities, if one of the parties to the transaction is a subsidiary of the other or if they are subsidiaries of the same corporation.

(télévirement)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Employees profit sharing plan

Has the same meaning as in subsection 248(1) of the Income Tax Act. (régime de participation des employés aux bénéfices)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Entity

A body corporate, a trust, a partnership, a fund or an unincorporated association or organization. (entité)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 2(1).

Facts

Actual events, actions, occurrences or elements that exist or are known to have happened or existed. Facts are not opinions. For example, facts surrounding a transaction or multiple transactions could include the date, time, location, amount or type of transaction or could include the account details, particular business lines, or the client's financial history. (faits)

Family member

For the purposes of subsection 9.3(1) of the Act, a prescribed family member of a politically exposed foreign person, a politically exposed domestic person or a head of an international organization is:

1. (a) their spouse or common-law partner;
2. (b) their child;
3. (c) their mother or father;
4. (d) the mother or father of their spouse or common-law partner; or
5. (e) a child of their mother or father.

(membre de la famille)

Reference:

PCMLTFR, SOR/2002-184, s. 2(1).

Fiat currency

A currency that is issued by a country and is designated as legal tender in that country. (monnaie fiduciaire)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2) and PCMLTFSTRR, SOR/2001-317, s. 1(2).

Final receipt

In respect of an electronic funds transfer, means the receipt of the instructions by the person or entity that is to make the remittance to a beneficiary. (destinataire)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Financial entity

Means:

1. (a) an entity that is referred to in any of paragraphs 5(a), (b) and (d) to (f) of the Act;
2. (b) a financial services cooperative;

3. (c) a life insurance company, or an entity that is a life insurance broker or agent, in respect of loans or prepaid payment products that it offers to the public and accounts that it maintains with respect to those loans or prepaid payment products, other than:

4. (i) loans that are made by the insurer to a policy holder if the insured person has a terminal illness that significantly reduces their life expectancy and the loan is secured by the value of an insurance policy;

5. (ii) loans that are made by the insurer to the policy holder for the sole purpose of funding the life insurance policy; and

6. (iii) advance payments to which the policy holder is entitles that are made to them by the insurer;

7. (d) a credit union central when it offers financial services to a person, or to an entity that is not a member of that credit union central; and

8. (e) a department, or an entity that is an agent of His Majesty in right of Canada or an agent or mandatary of His Majesty in right of a province, when it carries out an activity referred to in section 76.

(entité financière)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Financial Action Task Force

The Financial Action Task Force on Money Laundering established in 1989. (Groupe d'action financière)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 2(1).

Financial services cooperative

A financial services cooperative that is regulated by an Act respecting financial services cooperatives, CQLR, c. C-67.3 or the Act respecting the Mouvement Desjardins, S.Q. 2000, c. 77, other than a caisse populaire. (coopérative de services financiers)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Foreign currency

A fiat currency that is issued by a country other than Canada. (devise)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Foreign currency exchange transaction

An exchange, at the request of another person or entity, of one fiat currency for another. (opération de change en devise)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Foreign currency exchange transaction ticket

A record respecting a foreign currency exchange transaction—including an entry in a transaction register—that sets out:

1. (a) the date of the transaction;
2. (b) in the case of a transaction of $3,000 or more, the name and address of the person or entity that requests the exchange, the nature of their principal business or their occupation and, in the case of a person, their date of birth;
3. (c) the type and amount of each of the fiat currencies involved in the payment made and received by the person or entity that requests the exchange;
4. (d) the method by which the payment is made and received;
5. (e) the exchange rates used and their source;
6. (f) the number of every account that is affected by the transaction, the type of account and the name of each account holder; and
7. (g) every reference number that is connected to the transaction and has a function equivalent to that of an account number.

(fiche d'opération de change en devise)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Foreign money services business

Persons and entities that do not have a place of business in Canada, that are engaged in the business of providing at least one of the following services that is directed at persons or entities in Canada, and that provide those services to their clients in Canada:

1. (i) foreign exchange dealing,
2. (ii) remitting funds or transmitting funds by any means or through any person, entity or electronic funds transfer network,
3. (iii) issuing or redeeming money orders, traveller's cheques or other similar negotiable instruments except for cheques payable to a named person or entity,

4. (iv) dealing in virtual currencies, or

5. (v) any prescribed service.

(entreprise de services monétaires étrangère)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 5(h.1), PCMLTFRR, SOR/2007-121, s. 1 and PCMLTFR, SOR/2002-184, s. 1(2).

Foreign state

Except for the purposes of Part 2, means a country other than Canada and includes any political subdivision or territory of a foreign state. (État étranger)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 2(1).

Funds

Means:

1. (a) cash and other fiat currencies, and securities, negotiable instruments or other financial instruments that indicate a title or right to or interest in them; or

2. (b) a private key of a cryptographic system that enables a person or entity to have access to a fiat currency other than cash.

For greater certainty, it does not include virtual currency. (fonds)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2) and PCMLTFSTRR, SOR/2001-317, s. 1(2).

Head of an international organization

A person who, at a given time, holds—or has held within a prescribed period before that time—the office or position of head of

1. a) an international organization that is established by the governments of states;

2. b) an institution of an organization referred to in paragraph (a); or

3. c) an international sports organization.

(dirigeant d'une organisation internationale)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 9.3(3).

Immediately

In respect of submitting a Terrorist Property Report (TPR), the time period within which a TPR must be submitted, which does not allow for any delay prior to submission. (immédiatement)

Information record

A record that sets out the name and address of a person or entity and:

1. (a) in the case of a person, their date of birth and the nature of their principal business or their occupation; and
2. (b) in the case of an entity, the nature of its principal business.

(dossier de renseignements)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Initiation

In respect of an electronic funds transfer, means the first transmission of the instructions for the transfer of funds. (amorcer)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Institutional trust

For the purpose of section 15 of the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFR), means a trust that is established by a corporation or other entity for a particular business purpose and includes a pension plan trust, a pension master trust, a supplemental pension plan trust, a mutual fund trust, a pooled fund trust, a registered retirement savings plan trust, a registered retirement income fund trust, a registered education savings plan trust, a group registered retirement savings plan trust, a deferred profit sharing plan trust, an employee profit sharing plan trust, a retirement compensation arrangement trust, an employee savings plan trust, a health and welfare trust, an unemployment benefit plan trust, a foreign insurance company trust, a foreign reinsurance trust, a reinsurance trust, a real estate investment trust, an environmental trust and a trust established in respect of endowment, a foundation or a registered charity. (fiducie institutionnelle)

Reference:

PCMLTFR, SOR/2002-184, s. 15(2).

International electronic funds transfer

An electronic funds transfer other than for the transfer of funds within Canada. (télévirement international)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Inter vivos trust

A personal trust, other than a trust created by will. (fiducie entre vifs)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Jewellery

Objects that are made of gold, silver, palladium, platinum, pearls or precious stones and that are intended to be worn as a personal adornment. (bijou)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Large cash transaction record

A record that indicates the receipt of an amount of $10,000 or more in cash in a single transaction and that contains the following information:

1. (a) the date of the receipt;
2. (b) if the amount is received for deposit into an account, the number of the account, the name of each account holder and the time of the deposit or an indication that the deposit is made in a night deposit box outside the recipient's normal business hours;
3. (c) the name and address of every other person or entity that is involved in the transaction, the nature of their principal business or their occupation and, in the case of a person, their date of birth;
4. (d) the type and amount of each fiat currency involved in the receipt;
5. (e) the method by which the cash is received;
6. (f) if applicable, the exchange rates used and their source;
7. (g) the number of every other account that is affected by the transaction, the type of account and the name of each account holder
8. (h) every reference number that is connected to the transaction and has a function equivalent to that of an account number;
9. (i) the purpose of the transaction;
10. (j) the following details of the remittance of, or in exchange for, the cash received:
    1. (i) the method of remittance;
    2. (ii) if the remittance is in funds, the type and amount of each type of funds involved;

3. (iii) if the remittance is not in funds, the type of remittance and its value, if different from the amount of cash received; and

4. (iv) the name of every person or entity involved in the remittance and their account number or policy number or, if they have no account number or policy number, their identifying number; and

11. (k) if the amount is received by a dealer in precious metals and precious stones for the sale of precious metals, precious stones or jewellery:

1. (i) the type of precious metals, precious stones or jewellery;

2. (ii) the value of the precious metals, precious stones or jewellery, if different from the amount of cash received, and

3. (iii) the wholesale value of the precious metals, precious stones or jewellery.

(relevé d'opération importante en espèces)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Large virtual currency transaction record

A record that indicates the receipt of an amount of $10,000 or more in virtual currency in a single transaction and that contains the following information:

1. (a) the date of the receipt;

2. (b) if the amount is received for deposit into an account, the name of each account holder;

3. (c) the name and address of every other person or entity that is involved in the transaction, the nature of their principal business or their occupation and, in the case of a person, their date of birth;

4. (d) the type and amount of each virtual currency involved in the receipt;

5. (e) the exchange rates used and their source;

6. (f) the number of every other account that is affected by the transaction, the type of account and the name of each account holder;

7. (g) every reference number that is connected to the transaction and has a function equivalent to that of an account number;

8. (h) every transaction identifier, including the sending and receiving addresses; and

9. (i) if the amount is received by a dealer in precious metals and precious stones for the sale of precious metals, precious stones or jewellery:

10. (i) the type of precious metals, precious stones or jewellery;

11. (ii) the value of the precious metals, precious stones or jewellery, if different from the amount of virtual currency received; and

12. (iii) the wholesale value of the precious metals, precious stones or jewellery.

(relevé d'opération importante en monnaie virtuelle)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Life insurance broker or agent

A person or entity that is authorized under provincial legislation to carry on the business of arranging contracts of life insurance. (représentant d'assurance-vie)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Life insurance company

A life company or foreign life company to which the Insurance Companies Act applies or a life insurance company regulated by a provincial Act. (société d'assurance-vie)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Listed person

Has the same meaning as in section 1 of the Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism. (personne inscrite)

Reference:

PCMLTFSTRR, SOR/2001-317, s. 1(2).

Managing general agents (MGAs)

Life insurance brokers or agents that act as facilitators between other life insurance brokers or agents and life insurance companies. MGAs typically offer services to assist with insurance agents contracting and commission payments, facilitate the flow of information between insurer and agent, and provide training to, and compliance oversight of, insurance agents. (agent général de gestion)

Mandatary

A person who acts, under a mandate or agreement, for another person or entity. (mandataire)

Marketing or advertising

When a person or entity uses promotional materials such as advertisements, graphics for websites or billboards, etc., with the intent to promote money

services business (MSB) services and to acquire business from persons or entities in Canada. (marketing ou publicité)

Minister

In relation to sections 24.1 to 39, the Minister of Public Safety and Emergency Preparedness and, in relation to any other provision of this Act, the Minister of Finance. (ministre)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 2(1).

Money laundering offence

An offence under subsection 462.31(1) of the Criminal Code. The United Nations defines money laundering as "any act or attempted act to disguise the source of money or assets derived from criminal activity." Essentially, money laundering is the process whereby "dirty money"—produced through criminal activity—is transformed into "clean money," the criminal origin of which is difficult to trace. (infraction de recyclage des produits de la criminalité)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 2(1).

Money laundering and terrorist financing indicators (ML/TF indicators)

Potential red flags that could initiate suspicion or indicate that something may be unusual in the absence of a reasonable explanation. [Indicateurs de blanchiment d'argent (BA) et de financement du terrorisme (FT) (indicateurs de BA/FT)]

Money services business

A person or entity that has a place of business in Canada and that is engaged in the business of providing at least one of the following services:

1. (i) foreign exchange dealing,
2. (ii) remitting funds or transmitting funds by any means or through any person, entity or electronic funds transfer network,
3. (iii) issuing or redeeming money orders, traveller's cheques or other similar negotiable instruments except for cheques payable to a named person or entity,
4. (iv) dealing in virtual currencies, or
5. (v) any prescribed service.

(entreprise de services monétaires)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 5(h), PCMLTFRR, SOR/2007-121, s. 1 and PCMLTFR, SOR/2002-184, s. 1(2).

Money services business agent

An individual or entity authorized to deliver services on behalf of a money services business (MSB). It is not an MSB branch. (mandataire d'une entreprise de services monétaires)

Mortgage administrator

A person or entity, other than a financial entity, that is engaged in the business of servicing mortgage agreements on real property or hypothec agreements on immovables on behalf of a lender. (administrateur hypothécaire)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 5(i), PCMLTFRR,SOR/2002-184, subsection 1(2)

Mortgage broker

A person or entity that is authorized under provincial legislation to act as an intermediary between a lender and a borrower with respect to loans secured by mortgages on real property or hypothecs on immovables. (courtier hypothécaire)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 5(i), PCMLTFRR,SOR/2002-184, subsection 1(2)

Mortgage lender

A person or entity, other than a financial entity, that is engaged in the business of providing loans secured by mortgages on real property or hypothecs on immovables. (prêteur hypothécaire)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 5(i), PCMLTFRR,SOR/2002-184, subsection 1(2)

Nature of principal business

An entity's type or field of business. Also applies to an individual in the case of a sole proprietorship. (nature de l'entreprise principale)

New developments

Changes to the structure or operations of a business when new services, activities, or locations are put in place. For example, changes to a business model or business restructuring. (nouveaux développements)

New technologies

The adoption of a technology that is new to a business. For example, when a business adopts new systems or software such as transaction monitoring systems or client onboarding and identification tools. (nouvelles technologies)

No apparent reason

There is no clear explanation to account for suspicious behaviour or information. (sans raison apparente)

Occupation

The job or profession of an individual. (profession ou métier)

Person

An individual. (personne)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 2(1).

Person authorized to give instructions

In respect of an account, means a person who is authorized to instruct on the account or make changes to the account, such as modifying the account type, updating the account contact details, and in the case of a credit card account, requesting a limit increase or decrease, or adding or removing card holders. A person who is only able to conduct transactions on the account is not considered a person authorized to give instructions. (personne habilitée à donner des instructions)

Politically exposed domestic person

A person who, at a given time, holds—or has held within a prescribed period before that time—one of the offices or positions referred to in any of paragraphs (a) and (c) to (j) in or on behalf of the federal government or a provincial government or any of the offices or positions referred to in paragraphs (b) and (k):

1. (a) Governor General, lieutenant governor or head of government;
2. (b) member of the Senate or House of Commons or member of a legislature of a province;
3. (c) deputy minister or equivalent rank;
4. (d) ambassador, or attaché or counsellor of an ambassador;
5. (e) military officer with a rank of general or above;
6. (f) president of a corporation that is wholly owned directly by His Majesty in right of Canada or a province;
7. (g) head of a government agency;

8. (h) judge of an appellate court in a province, the Federal Court of Appeal or the Supreme Court of Canada;
9. (i) leader or president of a political party represented in a legislature;
10. (j) holder of any prescribed office or position; or
11. (k) mayor, reeve or other similar chief officer of a municipal or local government.

(national politiquement vulnérable)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 9.3(3).

Politically exposed foreign person

A person who holds or has held one of the following offices or positions in or on behalf of a foreign state:

1. (a) head of state or head of government;
2. (b) member of the executive council of government or member of a legislature;
3. (c) deputy minister or equivalent rank;
4. (d) ambassador, or attaché or counsellor of an ambassador;
5. (e) military officer with a rank of general or above;
6. (f) president of a state-owned company or a state-owned bank;
7. (g) head of a government agency;
8. (h) judge of a supreme court, constitutional court or other court of last resort;
9. (i) leader or president of a political party represented in a legislature; or
10. (j) holder of any prescribed office or position.

(étranger politiquement vulnérable)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Possibility

In regards to completing a suspicious transaction report (STR), the likelihood that a transaction may be related to a money laundering/terrorist financing (ML/TF) offence. For example, based on your assessment of facts, context and ML/TF indicators you have reasonable grounds to suspect that a transaction is related to the commission or attempted commission of an ML/TF offence. (possibilité)

Precious metal

Gold, silver, palladium or platinum in the form of coins, bars, ingots or granules or in any other similar form. (métal précieux)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 2(1).

Precious stones

Diamonds, sapphires, emeralds, tanzanite, rubies or alexandrite. (pierre précieuse)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Prepaid payment product

A product that is issued by a financial entity and that enables a person or entity to engage in a transaction by giving them electronic access to funds or virtual currency paid to a prepaid payment product account held with the financial entity in advance of the transaction. It excludes a product that:

1. (a) enables a person or entity to access a credit or debit account or one that is issued for use only with particular merchants; or
2. (b) is issued for single use for the purposes of a retail rebate program.

(produit de paiement prépayé)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Prepaid payment product account

An account – other than an account to which only a public body or, if doing so for the purposes of humanitarian aid, a registered charity as defined in subsection 248(1) of the Income Tax Act, can add funds or virtual currency – that is connected to a prepaid payment product and that permits:

1. (a) funds or virtual currency that total $1,000 or more to be added to the account within a 24-hour period; or
2. (b) a balance of funds or virtual currency of $1,000 or more to be maintained.

(compte de produit de paiement prépayé)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Prescribed

Prescribed by regulations made by the Governor in Council. (Version anglaise seulement)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 2(1).

Probability

The likelihood in regards to completing a suspicious transaction report (STR) that a financial transaction is related to a money laundering/terrorist financing (ML/TF) offence. For example, based on facts, having reasonable grounds to believe that a transaction is probably related to the commission or attempted commission of an ML/TF offence. (probabilité)

Production order

A judicial order that compels a person or entity to disclose records to peace officers or public officers. (ordonnance de communication)

Public body

Means

1. (a) a department or an agent of His Majesty in right of Canada or an agent or mandatary of His Majesty in right of a province;
2. (b) an incorporated city or town, village, metropolitan authority, township, district, county, rural municipality or other incorporated municipal body in Canada or an agent or mandatary in Canada of any of them; and
3. (c) an organization that operates a public hospital and that is designated by the Minister of National Revenue as a hospital authority under the Excise Tax Act, or an agent or mandatary of such an organization.

(organisme public)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Real estate broker or sales representative

A person or entity that is authorized under provincial legislation to act as an agent or mandatary for purchasers or vendors in respect of the purchase or sale of real property or immovables. (courtier ou agent immobilier)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Real estate developer

A person or entity that, in any calendar year after 2007, has sold to the public, other than in the capacity of a real estate broker or sales representative:

1. (a) five or more new houses or condominium units;
2. (b) one or more new commercial or industrial buildings; or
3. (c) one or more new multi-unit residential buildings each of which contains five or more residential units, or two or more new multi-unit residential buildings that together contain five or more residential units.

(promoteur immobilier)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Reasonable measures

Steps taken to achieve a desired outcome, even if they do not result in the desired outcome. For example, this can include doing one or more of the following:

- asking the client,
- conducting open source searches,
- retrieving information already available, including information held in non-digital formats, or
- consulting commercially available information.

(mesures raisonnables)Receipt of funds record

A record that indicates the receipt of an amount of funds and that contains the following information:

1. (a) the date of the receipt;
2. (b) if the amount is received from a person, their name, address and date of birth and the nature of their principal business or their occupation;
3. (c) if the amount is received from or on behalf of an entity, the entity's name and address and the nature of their principal business;
4. (d) the amount of the funds received and of any part of the funds that is received in cash;
5. (e) the method by which the amount is received;
6. (f) the type and amount of each fiat currency involved in the receipt;
7. (g) if applicable, the exchange rates used and their source;
8. (h) the number of every account that is affected by the transaction in which the receipt occurs, the type of account and the name of each account holder;
9. (i) the name and address of every other person or entity that is involved in the transaction, the nature of their principal business or their occupation and, in the case of a person, their date of birth;

10. (j) every reference number that is connected to the transaction and has a function equivalent to that of an account number; and

11. (k) the purpose of the transaction.

(relevé de réception de fonds)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Registered pension plan

Has the same meaning as in subsection 248(1) of the Income Tax Act. (régime de pension agréé)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Registered retirement income fund

Has the same meaning as in subsection 248(1) of the Income Tax Act. (fonds enregistré de revenu de retraite)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Reliable

In respect of information that is used to verify identity, means that the source is well known, reputable, and is considered one that you trust to verify the identity of the client. (fiable)

Representative for service

An individual in Canada that has been appointed by a person or entity that is a foreign money services business (FMSB), pursuant to the PCMLTFA, to receive notices and documents on behalf of the FMSB. (représentant du service)

Risk assessment

The review and documentation of potential money laundering/terrorist financing risks in order to help a business establish policies, procedures and controls to detect and mitigate these risks and their impact. (évaluation des risques)

Sanctions evasion

Sanctions evasion offence means an offence arising from the contravention of a restriction or prohibition established by an order or a regulation made under the United Nations Act, the Special Economic Measures Act or the Justice for Victims of Corrupt Foreign Officials Act (Sergei Magnitsky Law). (contournement des sanctions)

Securities dealer

A person or entity that is referred to in paragraph 5(g) of the Act. (courtier en valeurs mobilières)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Senior officer

In respect of an entity, means:

1. (a) a director of the entity who is one of its full-time employees;
2. (b) the entity's chief executive officer, chief operating officer, president, secretary, treasurer, controller, chief financial officer, chief accountant, chief auditor or chief actuary, or any person who performs any of those functions; or
3. (c) any other officer who reports directly to the entity's board of directors, chief executive officer or chief operating officer.

(cadre dirigeant)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Service agreement

An agreement between a money services business (MSB) and an organization according to which the MSB will provide any of the following MSB services on an ongoing basis:

- money transfers;
- foreign currency exchange;
- issuing or redeeming money orders, traveller's cheques or anything similar; or
- dealing in virtual currencies.
- Crowdfunding
- Armoured Cars

(accord de relation commerciale) Settlor

A settlor is an individual or entity that creates a trust with a written trust declaration. The settlor ensures that legal responsibility for the trust is given to a trustee and that the trustee is provided with a trust instrument document that explains how the trust is to be used for the beneficiaries. A settlor includes any individual or entity that contributes financially to that trust, either directly or indirectly. (constituant)

Shell bank

A foreign financial institution that:

1. (a) does not have a place of business that:

2. (i) is located at a fixed address—where it employs one or more persons on a full-time basis and maintains operating records related to its banking activities—in a country in which it is authorized to conduct banking activities; and

3. (ii) is subject to inspection by the regulatory authority that licensed it to conduct banking activities; and

4. (b) is not controlled by, or under common control with, a depository institution, credit union or foreign financial institution that maintains a place of business referred to in paragraph (a) in Canada or in a foreign country.

(banque fictive)

Reference:

PCMLTFR, SOR/2002-184, s. 1(1).

Signature

Includes an electronic signature or other information in electronic form that is created or adopted by a client of a person or entity referred to in section 5 of the Act and that is accepted by the person or entity as being unique to that client. (signature)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Signature card

In respect of an account, means a document that is signed by a person who is authorized to give instructions in respect of the account, or electronic data that constitutes the signature of such a person. (fiche-signature)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Source

The issuer or provider of information or documents for verifying identification. (source)

Source of funds or of virtual currency (VC)

The origin of the particular funds or VC used to carry out a specific transaction or to attempt to carry out a transaction. It is how the funds were acquired, not where the funds may have been transferred from. For example, the source of funds could originate from activities or occurrences such as employment income, gifts, the sale of a large asset, criminal activity, etc. (origine des fonds ou de la monnaie virtuelle (MV))

Source of wealth

The origin of a person's total assets that can be reasonably explained, rather than what might be expected. For example, a person's wealth could originate from an accumulation of activities and occurrences such as business undertakings, family estates, previous and current employment income, investments, real estate, inheritance, lottery winnings, etc. (origine de la richesse)

Starting action

With respect to a reportable transaction, information related to the instructions provided by the person or entity making the request to the reporting entity to start a transaction. For example, an individual arrives at a bank and requests to purchase a bank draft. The starting action is the details of the instructions for the purchase which includes the funds or virtual currency that the requesting person or entity brought to the reporting entity. A transaction must have at least one starting action. (action d'amorce)

SWIFT

The Society for Worldwide Interbank Financial Telecommunication. (SWIFT)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Terrorist activity

Has the same meaning as in subsection 83.01(1) of the Criminal Code. (activité terroriste)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 2(1).

Terrorist activity financing offence

An offence under section 83.02, 83.03 or 83.04 of the Criminal Code or an offence under section 83.12 of the Criminal Code arising out of a contravention of section 83.08 of that Act.

A terrorist financing offence is knowingly collecting or giving property (such as money) to carry out terrorist activities. This includes the use and possession of any property to help carry out the terrorist activities. The money earned for terrorist financing can be from legal sources, such as personal donations and profits from a business or charitable organization or from criminal sources, such as the drug trade, the smuggling of weapons and other goods, fraud, kidnapping and extortion. (infraction de financement des activités terroristes)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 2(1).

Third party

Any individual or entity that instructs another individual or entity to act on their behalf for a financial activity or transaction. (tiers)

Threats to the security of Canada

Has the same meaning as in section 2 of the Canadian Security Intelligence Service Act. (menaces envers la sécurité du Canada)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 2(1).

Training program

A written and implemented program outlining the ongoing training for your employees, agents or other individuals authorized to act on your behalf. It should contain information about all your obligations and requirements to be fulfilled under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and its associated Regulations. (programme de formation)

Trust

A right of property held by one individual or entity (a trustee) for the benefit of another individual or entity (a beneficiary). (fiducie)

Trust company

A company that is referred to in any of paragraphs 5(d) to (e.1) of the Act. (société de fiducie)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Trustee

A trustee is the individual or entity authorized to hold or administer the assets of a trust. (fiduciaire)

Tutor

In the context of civil law, a person who has been lawfully appointed to the care of the person and property of a minor. (tuteur)

Two year effectiveness review

A review, conducted every two years (at a minimum), by an internal or external auditor to test the effectiveness of your policies and procedures, risk assessment, and training program. (examen bisannuel de l'efficacité)

Valid

In respect of a document or information that is used to verify identity, appears legitimate or authentic and does not appear to have been altered or had any information redacted. The information must also be valid according to the

issuer, for example if a passport is invalid because of a name change, it is not valid for FINTRAC purposes. (valide)

Verify identity

To refer to certain information or documentation, in accordance with the prescribed methods, to identify a person or entity (client). (vérifier l'identité)

Very large corporation or trust

A corporation or trust that has minimum net assets of $75 million CAD on its last audited balance sheet. The corporation's shares or units have to be traded on a Canadian stock exchange or on a stock exchange designated under subsection 262(1) of the Income Tax Act. The corporation or trust also has to operate in a country that is a member of the Financial Action Task Force (FATF). (personne morale ou fiducie dont l'actif est très important)

Violation

A contravention of the Act or the regulations that is designated as a violation by regulations made under subsection 73.1(1). (violation)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 2(1).

Virtual currency

Means:

1. (a) a digital representation of value that can be used for payment or investment purposes that is not a fiat currency and that can be readily exchanged for funds or for another virtual currency that can be readily exchanged for funds; or
2. (b) a private key of a cryptographic system that enables a person or entity to have access to a digital representation of value referred to in paragraph (a).

(monnaie virtuelle)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2) and PCMLTFSTRR, SOR/2001-317, s. 1(2).

Virtual currency exchange transaction

An exchange, at the request of another person or entity, of virtual currency for funds, funds for virtual currency or one virtual currency for another. (opération de change en monnaie virtuelle)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Virtual currency exchange transaction ticket

A record respecting a virtual currency exchange transaction—including an entry in a transaction register—that sets out:

1. (a) the date of the transaction;
2. (b) in the case of a transaction of $1,000 or more, the name and address of the person or entity that requests the exchange, the nature of their principal business or their occupation and, in the case of a person, their date of birth;
3. (c) the type and amount of each type of funds and each of the virtual currencies involved in the payment made and received by the person or entity that requests the exchange;
4. (d) the method by which the payment is made and received;
5. (e) the exchange rates used and their source;
6. (f) the number of every account that is affected by the transaction, the type of account and the name of each account holder;
7. (g) every reference number that is connected to the transaction and has a function equivalent to that of an account number; and
8. (h) every transaction identifier, including the sending and receiving addresses.

(fiche d'opération de change en monnaie virtuelle)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Working days

In respect of an electronic funds transfer (EFT) report or a large virtual currency transaction report, a working day is a day between and including Monday to Friday. It excludes Saturday, Sunday, and a public holiday. (jour ouvrable)

Date Modified: 2024-10-11# Money laundering and terrorist financing indicators—Financial entities

From: Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)

Overview

ML/TF indicators are potential red flags that could initiate suspicion or indicate that something may be unusual in the absence of a reasonable explanation. Red flags typically stem from one or more factual characteristics, behaviours,

patterns or other contextual factors that identify irregularities related to financial transactions or attempted transactions. These often present inconsistencies with what is expected of your client based on what you know about them.

The ML/TF indicators in this guidance were developed by FINTRAC through a three-year review of ML/TF cases, a review of high quality STRs, published literature by international organizations such as the Financial Action Task Force (FATF) and the Egmont Group, and consultation with reporting entity sectors. These ML/TF indicators do not cover every possible situation but were developed to provide you with a general understanding of what is or could be unusual or suspicious. On its own, a single ML/TF indicator may not appear suspicious. However, observing an ML/TF indicator could lead you to conduct an assessment of the transaction(s) to determine whether there are further facts, contextual elements or additional ML/TF indicators that assist in establishing reasonable grounds to suspect the commission or attempted commission of an ML/TF offence which requires the submission of an STR.

Criminal organizations often combine various methods in different ways in order to avoid the detection of ML/TF. If you detect unusual or suspicious behaviour or a transaction that prompts the need for an assessment, ML/TF indicators combined with facts and context can help you determine if there are **reasonable grounds to suspect** that the transaction is related to the commission or attempted commission of an ML/TF offence. These ML/TF indicators may also be used to explain or articulate the rationale for your reasonable grounds to suspect in the narrative portion of an STR, as they provide valuable information from a financial intelligence perspective.

Important considerations

One piece of the puzzle

The ML/TF indicators in this guidance are not an exhaustive list of ML/TF indicators to support all suspicious scenarios. These ML/TF indicators should be considered as examples to guide the development of your own process to determine when you have reasonable grounds to suspect that the transaction or attempted transaction is related to the commission or attempted commission of an ML/TF offence. These ML/TF indicators are one piece of the puzzle and are designed to complement your own STR process and can be used in conjunction with other publicly available ML/TF indicators.

During an assessment, FINTRAC will review your compliance policies and procedures to see how you use ML/TF indicators within your STR process. Part of the assessment will include evaluating how the actual policies follow your documented approach and determining its effectiveness with respect to the use of ML/TF indicators. This can include a review of transactions to determine how your STR process identifies potential STRs and assesses them using facts, context and ML/TF indicators. For example, you may be asked to provide an explanation if you have not reported an STR for a client you have assessed

as high risk and that client's activity also matches against multiple ML/TF indicators.

Combination of facts, context and ML/TF indicators

If the context surrounding a transaction is suspicious, it could lead you to assess a client's financial transactions. Facts, context and ML/TF indicators need to be assessed to determine whether there are reasonable grounds to suspect that the transaction is related to the commission or attempted commission of an ML/TF offence. On its own, a single financial transaction or ML/TF indicator may not appear suspicious. However, this does not mean you should stop your assessment. Additional facts or context about the client or their actions may help you reach the reasonable grounds to suspect threshold.

Alert or triggering system

FINTRAC acknowledges that a reporting entity may have developed a system that relies on specific alerts or triggering events to signal when to assess a transaction to determine if an STR should be submitted to FINTRAC. If you rely on such a system, FINTRAC expects that you review the alerts in a timely manner in order to determine if an STR should be submitted. Regardless of how you choose to operationalize these ML/TF indicators, FINTRAC expects that you will be able to demonstrate that you have an effective process to identify, assess and submit STRs to FINTRAC.

General ML/TF indicators

The ML/TF indicators in the following section are applicable to both suspected ML and/or TF. The ability to detect, prevent and deter ML and/or TF begins with properly identifying the person or entity in order to review and report suspicious financial activity.

As a financial entity, you may observe these ML/TF indicators over the course of your business activities with a client. It is important to note that depending on your business activities, some of these ML/TF indicators may not apply.

ML/TF indicators related to identifying the person or entity

The following are examples of ML/TF indicators that you may observe when identifying persons or entities.

- There is an inability to properly identify the client or there are questions surrounding the client's identity.
- When opening an account, the client refuses or tries to avoid providing information required by the financial institution, or provides information that is misleading, vague, or difficult to verify.

- The client refuses to provide information regarding the beneficial owners of an account opened for an entity, or provides information that is false, conflicting, misleading or substantially incorrect.
- The identification document presented by the client cannot be authenticated.
- There are inconsistencies in the identification documents or different identifiers provided by the client, such as name, address, date of birth or phone number.
- Client produces seemingly false information or identification that appears to be counterfeited, altered or inaccurate.
- Client displays a pattern of name variations from one transaction to another or uses aliases.
- Client alters the transaction after being asked for identity documents.
- The client provides only a non-civic address or disguises a post office box as a civic address for the purpose of concealing their physical residence.
- Common identifiers (e.g. addresses, phone numbers, etc.) are used by multiple clients that do not appear to be related.
- Common identifiers (e.g. addresses, phone numbers, etc.) are used by multiple clients conducting similar transactions.
- Use of the same hotel address by one or more clients.
- Transactions involve persons or entities identified by the media, law enforcement and/or intelligence agencies as being linked to criminal activities.
- Attempts to verify the information provided by a new or prospective client are difficult.

ML/TF indicators related to client behaviour

The contextual information acquired through the know your client (KYC) requirements or the behaviour of a client, particularly surrounding a transaction or a pattern of transactions, may lead you to conduct an assessment in order to determine if you are required to submit an STR to FINTRAC. The following are some examples of ML/TF indicators that are linked to contextual behaviour and may be used in conjunction with your assessment and your risk-based approach.

- Client makes statements about involvement in criminal activities.
- Client conducts transactions at different physical locations, or approaches different tellers.
- Evidence of untruthfulness on behalf of the client (e.g. providing false or misleading information).
- Client exhibits nervous behaviour.
- Client refuses to provide information when required, or is reluctant to provide information.
- Client has a defensive stance to questioning.
- Client presents confusing details about the transaction or knows few details about its purpose.

- Client avoids contact with reporting entity employees.
- Client refuses to identify a source of funds or provides information that is false, misleading, or substantially incorrect.
- Client exhibits a lack of concern about higher than normal transaction costs or fees.
- Client makes enquiries/statements indicating a desire to avoid reporting or tries to persuade the reporting entity not to file/maintain required reports.
- Insufficient explanation for the source of funds.
- Client closes account after an initial deposit is made without a reasonable explanation.

ML/TF indicators surrounding the financial transactions in relation to the person/entity profile

Clearly understanding the expected activity of a person or entity will allow you to assess their financial activity with the proper lens. For example, an entity involved in an industry that is not normally cash-intensive receiving excessive cash deposits or a person conducting financial transactions atypical of their financial profile. The following are some examples of ML/TF indicators surrounding the financial transactions related to the person/entity profile.

- The transactional activity far exceeds the projected activity at the time of the account opening or the beginning of the relationship.
- The transactional activity (level or volume) is inconsistent with the client's apparent financial standing, their usual pattern of activities or occupational information (e.g. student, unemployed, social assistance, etc.).
- The volume of transactional activity exceeds the norm for geographical area.
- The transactional activity is inconsistent with what is expected from a declared business (e.g. business account has no normal business-related activities, such as the payment of payrolls or invoices).
- Client appears to be living beyond their means.
- Large and/or rapid movement of funds not commensurate with the client's financial profile.
- Rounded sum transactions atypical of what would be expected from the client.
- Size or type of transactions atypical of what is expected from the client.
- Opening accounts when the client's address or employment address is outside the local service area without a reasonable explanation.
- There is a sudden change in the client's financial profile, pattern of activity or transactions.
- Client uses notes, monetary instruments, or products and/or services that are unusual for such a client.

ML/TF indicators related to products and services

Accounts can take different forms (e.g. chequing, savings, investment, etc.) and for the purposes of this section, the ML/TF indicators below will aim to address the ML/TF risks linked to different types of accounts held by various reporting entities in Canada. There are many ML/TF indicators related to account activity. Your process to evaluate risk for accounts and any other products and services you provide should be documented as part of your KYC and risk assessment requirements. The following ML/TF indicators will focus on products or services that may be applicable within your business.

- Holding multiple accounts at several financial institutions for no apparent reason.
- Suspected use of a personal account for business purposes, or vice-versa.
- Client appears to have recently established a series of new relationships with different financial entities.
- A product and/or service opened on behalf of a person or entity that is inconsistent based on what you know about that client.
- Frequent use of safety deposit box.
- Accounts used for pass-through activities (e.g. to receive and subsequently send funds to beneficiaries).
- Use of multiple foreign bank accounts for no apparent reason.
- Credit card transactions and payments are exceptionally high for what is expected of the client including an excessive amount of cash advance usage, balance transfer requests or transactions involving luxury items.
- Client frequently makes credit card overpayments and then requests a cash advance.
- Frequent and/or atypical transfers between the client's products and accounts for no apparent reason.
- The same person holds signing authority for accounts held by multiple entities where there is no legal reason or sufficient explanation for such an arrangement.
- Accounts held by multiple entities either headquartered at the same location or having the same directors/signing authorities for no apparent reason.

ML/TF indicators related to change in account activity

Certain changes regarding an account may be indicative of ML/TF for a multitude of reasons including, but not limited to, the use of an account to suddenly launder or transmit funds, an increase in volume, changes in ownership of an account, etc. Changes in account activity may trigger a need for further assessment of the person or entity holding the account and some examples to consider are listed below.

- A business account has a change in ownership structure with increases in transactional activity and no apparent explanation.

- An inactive account begins to see financial activity (e.g. deposits, wire transfers, withdrawals).
- Accounts that receive relevant periodical deposits and are inactive at other periods without a logical explanation.
- A sudden increase in credit card usage or applications for new credit.
- Abrupt change in account activity.

ML/TF indicators based on atypical transactional activity

There are certain transactions that are outside the normal conduct of your everyday business. These transactions may be indicative of a suspicious transaction, and would require additional assessment. Some examples of ML/TF indicators based on atypical transactional activity are listed below.

- The client has multiple products, atypical of what would be expected.
- A series of complicated transfers of funds that seems to be an attempt to hide the source and intended use of the funds.
- Transactions displaying financial connections between persons or entities that are not usually connected (e.g. a food importer dealing with an automobile parts exporter).
- Transaction is unnecessarily complex for its stated purpose.
- Client presents notes or financial instruments that are packed, transported or wrapped in an uncommon way.
- A client's transactions have no apparent business or economic purpose.
- Transaction is consistent with a publicly known trend in criminal activity.
- Client deposits musty, odd smelling or extremely dirty bills.
- Transaction involves a suspected shell entity (an entity that does not have an economical or logical reason to exist).
- Client frequently exchanges small bills for larger bills.
- Suspicious pattern emerges from a client's transactions (e.g. transactions take place at the same time of day).
- Atypical transfers by a client on an in-and-out basis, or other methods of moving funds quickly, such as a cash deposit followed immediately by a wire transfer of the funds out.
- Funds transferred in and out of an account on the same day or within a relatively short period of time.

ML/TF indicators related to transactions structured below the reporting or identification requirements

Structuring of transactions to avoid reporting or identification requirements is a common method for committing or attempting to commit an ML/TF offence. There are multiple thresholds which trigger reporting/identification requirements by a reporting entity. Some examples of ML/TF indicators which may be indicative of a person or entity attempting to evade identification and/or reporting thresholds are listed below.

- You become aware of the structuring of deposits at multiple branches or institutions.
- Client appears to be structuring amounts to avoid client identification or reporting thresholds.
- Client appears to be collaborating with others to avoid client identification or reporting thresholds.
- The structuring of deposits through multiple branches of the same financial institution or by groups of persons who enter a single branch at the same time.
- Multiple transactions conducted below the reporting threshold within a short period.
- Client makes enquiries that would indicate a desire to avoid reporting.
- Client conducts transactions at different physical locations or with different representatives in an apparent attempt to avoid detection.
- Client exhibits knowledge of reporting thresholds.

ML/TF indicators involving wire transfers (including electronic funds transfers)

In our current global environment, it is increasingly easier to transfer funds to, from or through multiple jurisdictions (municipal, national or international) in a rapid fashion. This presents an increased ML/TF risk as transactions passing through multiple accounts and/or jurisdictions increase the difficulty for reporting entities and law enforcement to trace illicit funds. Examples of these types of transactions which may require further assessment include the following.

- Client is unaware of details surrounding incoming wire transfers, such as the ordering client details, amounts or reasons.
- Client does not appear to know the sender of the wire transfer from whom the wire transfer was received, or the recipient to whom they are sending the wire transfer.
- Client frequents multiple locations utilizing cash, prepaid credit cards or money orders/cheques/drafts to send wire transfers overseas.
- The client sends wire transfers or receives wire transfers to or from multiple beneficiaries that do not correspond to the expected use of the account type or business account.
- Client is accompanied by persons who appear to be instructing the sending or receiving of wire transfers on their behalf.
- Multiple persons are sending wire transfers that are similar in amounts, receiver names, security questions, addresses or destination country.
- Client attempts to specify the routing of an international wire transfer.
- Client conducts wire transfers that do not include theirs or the beneficiary's requisite information.
- Client utilizes structured cash transactions to send wire transfers in an effort to avoid record keeping requirements.

- Funds are deposited or received into several accounts and then consolidated into one before transferring the funds outside the country.
- Immediately after transferred funds have cleared, the client moves funds, to another account or to another person or entity.
- Multiple clients have sent wire transfers over a short period of time to the same recipient.
- Large wire transfers or high volume of wire transfers are conducted or received through the account that does not fit the expected pattern of that account.
- Large and/or frequent wire transfers between senders and receivers with no apparent relationship.
- Client sending to, or receiving wire transfers from, multiple clients.

ML/TF indicators related to transactions that involve non-Canadian jurisdictions

There are certain types of transactions that may be sent or received from jurisdictions outside of Canada where there is higher ML/TF risk due to more permissible laws or the local ML/TF threat environment. The following are examples to consider when making an assessment of the financial transaction conducted by a person/entity through your business.

- Transactions with jurisdictions that are known to produce or transit drugs or precursor chemicals, or are sources of other types of criminality.
- Transactions with jurisdictions that are known to be at a higher risk of ML/TF.
- Transaction/business activity involving locations of concern, which can include jurisdictions where there are ongoing conflicts (and periphery areas), countries with weak ML/TF controls, or countries with highly secretive banking or other transactional laws.
- Transactions involving any countries deemed high risk or non-cooperative by the FATF.
- Client makes frequent overseas transfers, not in line with their financial profile.

Due to the ever-evolving nature of the ML/TF environment, high risk jurisdictions and trends are often subject to change. To ensure that you are referencing accurate information, FINTRAC encourages you to research publicly available sources on a regular basis to support these ML/TF indicators as part of your STR process. There are multiple sources that identify jurisdictions of concern, including the FATF, which publishes contextual information on high-risk jurisdictions in relation to their risk of ML and TF. You may also observe funds coming from or going to jurisdictions that are reported in the media as locations where terrorists operate/carry out attacks and/or where terrorists have a large support base (state sponsors or private citizens). Identifying high-risk jurisdictions or known trends can also be included as part of your risk-based approach and internal STR process.

ML/TF indicators related to the use of other parties

In the course of a "normal" financial transaction, there are a "normal" number of parties who engage in the transaction, depending on the nature of the transaction at hand. For example, in the instance of depositing cash to a personal bank account, there is generally one party to the transaction: the person who holds the account is depositing into their own account. By contrast, with the deposit of cash to a business account, you can have many different parties, including: persons associated with the business's finance function who hold authority over the account, or an employee who may be charged with depositing the cash.

Transactions that involve parties not typically associated with a transaction can present an elevated risk of ML and/or TF. These additional parties can be used to allow a criminal to avoid being identified or being linked to an asset or account. This section includes examples of how the involvement of other parties may be indicative of the structure of a criminal enterprise. Some examples of such other parties include the use of a third party, nominee or gatekeeper.

Use of third party A third party is any person or entity that instructs someone to act on their behalf for a financial activity or transaction. There are some situations where there is an apparent and discernable rationale for the inclusion of the third party in a transaction and this may not be suspicious. However, you may become suspicious in a situation where the reason for a person or entity acting on behalf of another person or entity does not make sense based on what you know about the client or the third party. Use of third parties is one method that money launderers and terrorist activity financiers use to distance themselves from the proceeds of crime or source of criminally obtained funds. By relying on other parties to conduct transactions they can distance themselves from the transactions that can be directly linked to the suspected ML/TF offence. Some examples of ML/TF indicators related to the use of a third party can be found below.

- Multiple deposits which are made to an account by non-account holders.
- Unrelated parties sending email money transfers or other forms of electronic transfers to the same beneficiary with no apparent relation to the recipient.
- A client conducts a transaction while accompanied, overseen or directed by another party.
- A client makes numerous outgoing payments to unrelated parties shortly after they receive incoming funds.
- Wire transfers, deposits or payments to or from unrelated parties (foreign or domestic).
- Client appears to be or states they are acting on behalf of another party.
- Account is linked to seemingly unconnected parties.

Use of nominee A nominee is a particular type of other party that is authorized to open accounts and conduct transactions on behalf of a person or entity.

There are legitimate reasons for relying on a nominee to conduct financial activity of behalf of someone else. However, this type of activity is particularly vulnerable to ML/TF as it is a common method used by criminals to distance themselves from the transactions that could be linked to suspected ML/TF offences. These are some examples of ML/TF indicators relating to the misuse of nominees.

- A person maintains multiple accounts, or maintains accounts in the names of family members or corporate entities with no apparent business or other purpose.
- A person or entity other than the stated account holder conducts the majority of the transaction activity, which seems unnecessary or excessive.
- Client is involved in transactions or account activities that are suspicious, but refuses or is unable to answer questions related to the account or transactions.

Use of gatekeeper A gatekeeper is a person who controls access to the financial system and can act on behalf of a client. Such services can be abused so that criminals have access to the financial system without being identified. Gatekeepers may include lawyers, accountants and other professions which can access the financial system on behalf of a client. While there are many transactions where it is "normal" to have a gatekeeper represent the interests of a client, such an appearance of normalcy can also be utilized to the advantage of criminals to provide the veneer of legitimacy to their transactions. The use of gatekeepers themselves is not an indicator of an ML/TF offence. However, entities should consider the following examples which can indicate misuse of the financial system access provided to gatekeepers.

- Gatekeeper avoids identifying their client or disclosing their client's identity when such identification would be normal during the course of a transaction.
- Gatekeeper is willing to pay higher fees and seeks to conduct the transaction quickly when there is no apparent need for such expediency.
- Gatekeeper is utilizing their account for transactions not typical of their business (e.g. pass through account, excessive amount of cash, payment to non-clients or parties of transactions).
- Apparent misuse of correspondent accounts by gatekeeper to obscure the origin and/or destination of funds.

Indicators related to TF

In Canada, TF offences make it a crime to knowingly collect or provide property, which can include financial or other related services, for terrorist purposes. This section is focused on examples that are specific to the possible commission of a TF offence. However, please note that the other ML/TF indicators in this guidance may also prove relevant in determining when you have reasonable

grounds to suspect the commission of TF, as the methods used by criminals to evade detection of ML are similar.

Indicators specifically related to TF:

The indicators below are some examples of indicators relating to TF.

- Transactions involving certain high-risk jurisdictions such as locations in the midst of or in proximity to, armed conflict where terrorist groups operate or locations which are subject to weaker ML/TF controls.
- An account opened in the name of an entity, a foundation or association, which may be linked or involved with a suspected terrorist organization.
- The use of funds by a non-profit organization is not consistent with the purpose for which it was established.
- Raising donations in an unofficial or unregistered manner.
- Client identified by media or law enforcement as having travelled, attempted or intended to travel to high-risk jurisdictions (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorist activities and organizations.
- Transactions involve persons or entities identified by media and/or sanctions lists as being linked to a terrorist organization or terrorist activities.
- Law enforcement information provided which indicates persons or entities may be linked to a terrorist organization or terrorist activities.
- Client conducted travel-related purchases (e.g. purchase of airline tickets, travel visa, passport, etc.) linked to high-risk jurisdictions (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorist activities and organizations.
- Person or entity's online presence supports violent extremism or radicalization.
- Client donates to a cause that is subject to derogatory information that is publicly available (e.g. crowdfunding initiative, charity, non-profit organization, non-government organization, etc.).# FINTRAC guidance related to the Ministerial Directive on Financial Transactions Associated with the Islamic Republic of Iran issued on July 25, 2020

This guidance explains the requirements of the Ministerial Directive on Financial Transactions Associated with the Islamic Republic of Iran.

1. Why this Ministerial Directive was issued

The Financial Action Task Force issued a statement in February 2020 which expressed its particular and exceptional concerns regarding Iran's failure to address strategic deficiencies in its anti-money laundering and combatting the financing of terrorism regime, and the serious threat this poses to the integrity of the international financial system. The Financial Action Task Force called

on its members to apply effective counter-measures to protect their financial sectors from such risks.

As such, Canada's Finance Minister issued this Ministerial Directive to ensure the safety and integrity of Canada's financial system.

This Ministerial Directive includes requirements that:

- enhance existing obligations of the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations; and
- extend the obligations of the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations

2. Who needs to apply this Ministerial Directive

This Ministerial Directive came into effect on July 25, 2020, and is applicable to every person or entity referred to in paragraphs 5(a), (b) and (h) of the Act. The specific persons and entities that are to take action in response to this Ministerial Directive are:

- banks
- credit unions
- financial services cooperatives
- caisses populaires
- authorized foreign banks
- money services businesses

3. Requirements of the Ministerial Directive

Every bank, credit union, financial services cooperative, caisse populaire, authorized foreign bank and money services business must:

- treat **every** financial transaction **originating from or bound for Iran**, regardless of its amount, as a high-risk transaction for the purposes of subsection 9.6(3) of the Act
- verify the identity of any client (person or entity) requesting or benefiting from such a transaction in accordance with Part 3 of the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations
- exercise customer due diligence in relation to any such transaction, including ascertaining the source of funds or virtual currency, the purpose of the transaction and the beneficial ownership or control of any entity requesting or benefiting from the transaction
- keep and retain a record of any such transaction, in accordance with the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations, regardless of the monetary thresholds set out in those Regulations; and
- report all such transactions to the Centre

3.1 Determining that a transaction originated from or is bound for Iran

When determining whether a transaction originates from or is bound for Iran, you need to look at a variety of elements because the circumstances of each transaction are different. You must consider the facts, contexts and indicators of a transaction to determine whether it is subject to the Ministerial Directive. **Transactions originating from or bound for Iran may include, but are not limited to:**

- electronic funds transfers, remittances or other transfers that include an Iranian originating or destination address - this may include transactions where the ordering person or entity, beneficiary, or third party details are Iranian
- the activities of representatives of the Government of Iran (for example, transactions on an Embassy of Iran's bank account in Canada)
- receiving Iranian rial as a deposit to an account or for a virtual currency transaction
- conducting a foreign currency or virtual currency exchange transaction that includes Iranian rial (for example, Canadian dollar to Iranian rial, Iranian rial to US dollar, virtual currency to Iranian rial, etc.); and
- issuing or redeeming bank drafts or other negotiable instruments that include an Iranian rial component

This Ministerial Directive **does not** apply to transactions where there is no suspicion or explicit connection with Iran and there is no evidence of the transaction originating from or being bound for Iran. For example:

- a client who has previously sent funds to Iran requests an outgoing electronic funds transfer, where the transaction details do not suggest that this transaction is bound for Iran and you are unable to obtain further details about the transaction destination
- the client's identification information is the only suggestion of a connection to Iran (for example, a transaction where the conductor's identification document is an Iranian passport); or
- the details of a person, who is your client in Canada, are Iranian, but there **are no additional details** on the entity involved, or the sender of, or the recipient to, the transaction, to suggest the transaction is associated with Iran

For further clarity, if the details of your client in Canada include an Iranian address and the client requests that funds be sent to a beneficiary in a country other than Iran, where additional facts, context and indicators (for example, beneficiary account details) point to an association with Iran, then this transaction must be considered as **bound for** Iran, and treated accordingly.

Similarly, if the details of your client in Canada include an Iranian address and this client receives funds into their account from a sending account in a country

other than Iran, but where additional facts, context and indicators (for example, sending account details), point to an association with Iran, then this transaction must be considered as **originating from** Iran, and treated accordingly.

Alternatively, if the details of your client in Canada include an Iranian address and this client requests that funds be sent to a beneficiary in a country other than Iran, for which additional facts, context and indicators **do not** bring to light an association with Iran, then this transaction is not required to be considered for the purpose of the Ministerial Directive.

Unless the transaction is being carried out by, or benefitting, a representative of the Government of Iran in Canada, then the details of your client in Canada are not likely enough to consider the transaction against the obligations of the Ministerial Directive.

Note: When you have determined that a transaction originated from or was bound for Iran, you must apply the measures outlined in the Ministerial Directive.

3.2 Verifying the identity of every client who requests or benefits from a transaction originating from or bound for Iran

Under this Ministerial Directive, you must take enhanced identification measures that go beyond the identification triggers and requirements prescribed under the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations. Transactions that fall below the reporting threshold amounts typically do not require that you verify the identity of clients. However, under this Ministerial Directive, **you must:**

- verify the identity of **every client** (including those you have a business relationship with) that requests or benefits from such a transaction **in any amount** in accordance with the methods prescribed in the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations; and
- for transactions that meet the reporting threshold amounts, apply **enhanced measures** to verify the identity of each client, as described in FINTRAC's ongoing monitoring guidance. Enhanced measures could include obtaining additional information on the client (for example, occupation, volume of assets, information available through public databases, Internet, etc.); gathering additional documents, data or information; or taking additional steps to verify the documents obtained, etc.

3.3 Additional measures required

You must treat **all** transactions originating from or bound for Iran as high risk. In addition to verifying the identity of any client requesting or benefiting from such a transaction, under this Ministerial Directive, you must:

- apply customer due diligence measures to these clients for all transactions (**any amount**)

- assess the client information to determine whether there are reasonable grounds to suspect the commission or attempted commission of a money laundering or terrorist activity financing infraction and to report it through a Reporting suspicious transactions to FINTRAC or Terrorist Property Report to FINTRAC
- apply enhanced measures to **every client** who meets the identification threshold (threshold transactions)
- obtain the purpose and the source of funds or virtual currency of any such transaction; and
- obtain the beneficial ownership or control information of any entity requesting or benefiting from such a transaction

Note: It is the reporting entity that owns the relationship with the client that is required to carry out the additional measures outlined in the Ministerial Directive (i.e., verifying the identity of the client, and exercising the customer due diligence measures).

4. Records you must keep and their retention period

4.1 Records of electronic funds and virtual currency transfers of any amount

For an electronic funds or virtual currency transfer **of any amount** originating from or bound for Iran, you must keep:

- the information included in an electronic funds transfer record, and the information included in a record for virtual currency transfers, **even if the transaction is below $ 1,000 CAD or an equivalent amount in virtual currency**:
  - if you are a bank, credit union, financial services cooperative or caisse populaire, you will find your record keeping requirements in the Record keeping requirements for financial entities guidance
  - if you are a money services business, you will find your record keeping requirements in the Record keeping requirements for money services businesses and foreign money services businesses guidance
- the source of funds or virtual currency of the transaction; and
- the purpose of the transaction

4.2 Records of receipt of cash or virtual currency – of any amount

You must keep a record of **every cash or virtual currency transaction (any amount)** that you receive that reflects a connection to Iran (such as cash received for the issuance of negotiable instruments or foreign exchange using Iranian rial). You must record:

- the information included in a large cash or virtual currency transaction record, **even if the transaction is below $10,000 CAD or an equiv-**

alent amount in virtual currency, and the information included in a foreign or virtual currency exchange transaction record, **including the information that is required when a transaction is over $3,000 CAD**:

  - if you are a bank, credit union, financial services cooperative or caisse populaire, you will find your record keeping requirements in the Record keeping requirements for financial entities guidance
  - if you are a money services business, you will find your record keeping requirements in the Record keeping requirements for money services businesses and foreign money services businesses guidance

- the source of funds or virtual currency of the transaction; and
- the purpose of the transaction

4.3 Records of redeeming other negotiable instruments and records for issuing or redeeming transactions – of any amount:

Transactions originating from or bound for Iran also include the redemption of other negotiable instruments (for example, bank drafts, money orders, traveller's cheques, etc.) in any amount. These too will have to reflect a connection with Iran, such as the use of Iranian rial in the transaction, for the Ministerial Directive to be applicable. You must record:

- the information included in a transaction record, **even if the transaction is below $3,000 CAD or an equivalent amount in virtual currency**:

  - if you are a bank, credit union, financial services cooperative or caisse populaire, and a client is redeeming any amount in one or multiple money orders, your record keeping requirements are referenced in the Record keeping requirements for financial entities guidance
  - if you are a money services business, and a client is redeeming money orders in any amount, your record keeping requirements are referenced in the Record keeping requirements for money services businesses and foreign money services businesses guidance

- the source of funds or virtual currency of the transaction; and
- the purpose of the transaction

4.4 Information on records and retention

If you are required by this Ministerial Directive to keep a record of information that is readily available in other records, you do not have to record the same information again. This means that if you keep the required information and can produce it during a FINTRAC examination, you do not need to create a new record to meet the obligations.

You must keep all records applicable to this Ministerial Directive in accordance with their associated record retention requirement, or for at least five years from the date the record was created.

5. Reporting transactions captured under this Ministerial Directive

5.1 Reporting an electronic funds transfer in any amount to FINTRAC:

- SWIFT electronic funds transfers that are under the reporting threshold of $10,000 CAD and **do not** aggregate to $10,000 CAD under the 24-hour rule and **involve** Iranian rial (IRR), **must be reported using the SWIFT Electronic Funds Transfer Report with the following addition**:
  - Insert the prefix **IR2020** before entering your reporting entity's report reference number. For example, if your reporting entity's report reference number is ABCD1234, then your reporting entity's report reference number would be IR2020ABCD1234.
- SWIFT electronic funds transfers that are under the reporting threshold of $10,000 CAD, **do not** aggregate to $10,000 CAD under the 24-hour rule, and **do not** involve Iranian rial (IRR), **must be reported using the Non-SWIFT Electronic Funds Transfer Report with the following addition:**
  - Insert the prefix **IR2020** before entering your reporting entity's report reference number. For example, if your reporting entity's report reference number is ABCD1234, then your reporting entity's report reference number would be IR2020ABCD1234.

Note: These transactions must have an Iranian address in at least one of the fields.

- Non-SWIFT electronic funds transfers that are under the reporting threshold of $10,000 CAD, and **do not** aggregate to $10,000 CAD under the 24-hour rule, must be reported using the Non-SWIFT Electronic Funds Transfer Report **with the following addition**:
  - Insert the prefix **IR2020** before entering your reporting entity's report reference number. For example, if your reporting entity's report reference number is ABCD1234, then your reporting entity's report reference number would be IR2020ABCD1234.
- SWIFT and Non-SWIFT electronic funds transfers of $10,000 CAD or more, and SWIFT and Non-SWIFT electronic funds transfers resulting from aggregated transactions of $10,000 CAD or more captured under the 24-hour rule are to be reported normally:

- No prefix is required

- Transfers of funds within Canada, of any amount, where it is deemed that the transaction is originating from or bound for Iran, must be reported using the suspicious transaction report as follows:
  - Insert the prefix **IR2020** before entering your reporting entity's report reference number. For example, if your reporting entity's report reference number is ABCD1234, then your reporting entity's report reference number would be IR2020ABCD1234.
  - As applicable Part B1, Item 5 – "other description" – transfer gov't Iran
  - As applicable Part B2, Item 12 – "other description" – transfer, gov't Iran
  - Insert the prefix **IR2020** into the G section of the Suspicious Transaction Report as well.
  - Because the report is related to the Ministerial Directive, **you must** ensure that information provided, such as currency type, or address or disposition details, reflect the connection to Iran.

5.2 Reporting the receipt of any amount of cash to FINTRAC:

- Any cash received (for example, Iranian rial deposited to an account, or Iranian rial received in exchange for virtual currency, CAD, or any other type of currency) that is under the reporting threshold of $10,000 CAD and **does not** aggregate to $10,000 CAD under the 24-hour rule must be reported using the Large Cash Transaction Report. Select 'IR2020' in the Ministerial Directive field to indicate the transaction is being reported under the Ministerial Directive.

  Note: Because the report is related to the Ministerial Directive, **you must** ensure that the information provided reflects a connection to Iran.

- Large cash transactions of $10,000 CAD or more, and large cash transactions that total $10,000 CAD or more when aggregated under the 24-hour rule are to be reported normally.

5.3 Reporting virtual currency transactions using the Large Virtual Currency Transaction Report :

- Any transaction involving the receipt of virtual currency for exchange to Iranian rial that is equivalent to an amount under the reporting threshold of $10,000 CAD must be reported using the Large Virtual Currency Transaction Report. Select 'IR2020' in the Ministerial Directive field to indicate the transaction is being reported under the Ministerial Directive.

  Note: Because the report is related to the Ministerial Directive, **you must** ensure that the information provided reflects a connection to Iran.

- Virtual currency transactions received in an amount equivalent to $10,000 CAD or more, and virtual currency transactions received that fall under the 24-hour rule are to be reported as normal.

5.4 Reporting negotiable instruments and issuing or redeeming transactions:

- Any negotiable instrument, and issuing or redeeming transaction that originates from or is bound for Iran, must be reported using the Reporting suspicious transactions to FINTRAC. In order to identify these transactions, submit the Suspicious Transaction Report with the following additions **when the transactions do not meet the reasonable grounds to suspect** the commission or attempted commission of a money laundering or a terrorist activity financing offence threshold:
  - Insert the prefix **IR2020** before entering your reporting entity's report reference number. For example, if your reporting entity's report reference number is ABCD1234, then your reporting entity's report reference number would be IR2020ABCD1234.
  - Insert the prefix **IR2020** into the G section of the suspicious transaction report as well.
  - Because the report is related to the Ministerial Directive, **you must** ensure that there is a connection to Iran, such as the Iranian rial, or the conductor address is Iranian.

5.5 Reporting suspicious transactions and terrorist property:

- All transactions that are associated with Iran must be treated as high risk and must be monitored for the purpose of determining whether a Suspicious Transaction Report or a Terrorist Property Report must be submitted to FINTRAC.
- For the purpose of this Ministerial Directive, only completed transactions must be reported if the sole reason for reporting is that the transaction is inbound from or outgoing to Iran. Attempted transactions remain reportable in instances where the reporting entity has reasonable grounds to suspect that the transaction is related to the attempted commission of a money laundering or a terrorist activity financing offence.
- See Reporting suspicious transactions to FINTRAC for more information.
- If you have property in **your possession or control** that you **know or believe** is owned or controlled by or on behalf of a listed person or a terrorist group you must submit a Terrorist Property Report to FINTRAC. This includes information about any transaction or proposed transaction relating to that property. See Reporting terrorist property to FINTRAC for more information.

5.6. Reporting timeframes:

- Where the Ministerial Directive reflects an enhancement to a current transaction reporting obligation (for example, the threshold to report has been reduced or eliminated) the timing for reporting that transaction remains that of the obligation being enhanced:
  - Electronic funds transfers must be reported no later than 5 working days after the day the reporting entity knows that the transfer must be reported;
  - Large cash transactions must be reported within 15 days after the transaction.
- Where the Ministerial Directive reflects an extension of reporting obligations to transactions that previously had no reporting obligation, such as the redemption of a negotiable instrument, transfers of funds within Canada, which are to be reported by means of the suspicious transaction reporting form, it is reasonable for the reporting entity to report this as soon as practicable.

Other

Your compliance program's policies and procedures should already include information on how your organization becomes aware of Ministerial Directives issued by the Minister of Finance and information on how your organization will respond. Once a Ministerial Directive has been issued, you must take steps to meet its requirements.

Your policies and procedures must also fully describe how you will make the determination that a transaction originates from or is bound for Iran and what specific mitigation measures you will take upon making this determination. For example, your policies and procedures could outline that you ask the purpose of a transaction. Similarly, you could research the origin or destination of a transaction to determine if the details about the sender, beneficiary or entities involved in the transaction, indicate that the transaction is originating from or bound for Iran.

Guidance on how to conduct and document your risk assessment can be found in the Risk assessment guidance. You are required to implement certain measures to mitigate the risk of transactions involving jurisdictions that are identified in Ministerial Directives. Examples of these measures can be found in General information on Part 1.1 of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act provided by the Department of Finance Canada.

During a compliance examination, FINTRAC may assess your compliance with any Ministerial Directive in order to verify that you have taken appropriate mitigating measures in relation to related transactions. FINTRAC may also review your overall risk assessment to verify that you have documented and assessed the risk related to your business activities and clients involving these jurisdictions. Failure to comply with the measures of a Ministerial Directive is

a very serious offence. The existing administrative monetary penalties regime extends to all Ministerial Directives, and failure to comply with a directive could result in a penalty. Penalties applicable to the breach of a directive can be found in the Proceeds of Crime (Money Laundering) and Terrorist Financing Administrative Monetary Penalties Regulations.

Guide on harm done assessment for compliance program violations

1. Introduction

This page presents how we assess the harm done and calculate the base penalty amount applied to compliance program violations.

1.1 Purpose of this guide

This guide presents how FINTRAC approaches the harm done criterion and the base penalty amount for violations under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (the Act) and its regulations. According to section 73.11 of the Act, FINTRAC must consider the harm done by a violation, that the purpose of an administrative monetary penalty (AMP) is to encourage compliance rather than to punish, and all other criteria prescribed in the regulations, including a reporting entity's (RE) history of compliance, when determining the amount of a penalty. Considerations for the non-punitive nature of an AMP and an RE's compliance history are assessed in another step in the penalty calculation and are outlined separately in FINTRAC's AMP policy.

1.2 Definition of harm

FINTRAC defines "harm" as the degree to which a violation interferes with achieving the objectives of the ActFootnote 1 or with FINTRAC's ability to carry out its mandateFootnote 2. Therefore, the consequences of non-compliance, when an AMP is imposed, are linked to its effects on Canada's efforts to combat money laundering and terrorist activity financing (ML/TF).

Compliance enforcement activities are undertaken to prevent and correct the harm that comes from non-compliance with the Act and regulations. REs' adherence to requirements such as record keeping and verifying client identity assists in the deterrence of ML/TF and supports police investigations and criminal prosecutions. The requirements related to reporting ensure that FINTRAC is supplied with the high-quality, timely financial transaction reports it needs to produce the financial intelligence that helps with the investigation and prosecution of ML/TF offences.

1.3 Considering harm in AMP calculations

When determining a penalty, FINTRAC considers the harm caused, that is, the degree to which the non-compliance interferes with the objectives of the Act and/or with FINTRAC's mandate. Non-compliance and harm are measured using the standards described in this guide, which outline the benchmark amounts for the corresponding levels of harm for a specific violation. FINTRAC considers the specific circumstances of each case, including the extent of the non-compliance and mitigating factors, which may further reduce the actual amounts applied.

2. Violations related to compliance program requirements

The fulfillment of the objectives of the Act and FINTRAC's ability to carry out its mandate depend upon REs successfully implementing a compliance program that allows them to identify clients, monitor business relationships, keep records and report certain financial transactions. The compliance program itself requires the appointment of a compliance officer, the development of policies and procedures, the assessment of ML/TF risks, the maintenance of a training program, and a review of the program's effectiveness every two years. These requirements not only ensure that REs have the structure in place to comply with the Act and its regulations, but they also establish a framework that helps facilitate the detection, prevention and deterrence of ML/TF offences in the normal course of business, which serves the objectives of the Act under paragraph 3(a).

Failing to establish and implement a compliance program can signify a serious deficit in anti-money laundering/anti-terrorist activity financing (AML/ATF) measures, leaving REs vulnerable to ML/TF offences, and ultimately impeding achievement of the Act's objectives under paragraph 3(a), or impacting FINTRAC's ability to carry out its mandate under section 40 of the Act. A compliance program requirement violation can signify gaps and weaknesses that result in not meeting other requirements such as reporting, record keeping or verifying client identity.

Therefore, FINTRAC assesses the potential harm that a compliance program violation may cause.

For example:

In situations where the absence of policies and procedures to report the receipt of $10,000 or more in cash also results in the failure to submit Large Cash Transactions Reports (LCTRs), FINTRAC may assess two distinct violations. The total penalty would be comprised of two amounts: the amount levied for the incomplete policies and procedures and the amount levied for the failure to submit LCTRs to FINTRAC. The penalty amount for incomplete policies and procedures represent the potential harm, while the actual failure to submit the LCTRs represents the concrete harm.

For guidance on how to calculate the penalty amount for other compliance

requirements such as reporting, verifying client identity and record keeping, please refer to the Penalties for non-compliance page which lists all the harm done guides by violation.

2.1 Harm consideration framework for violations related to the compliance program

FINTRAC assesses the potential harm caused by a violation and takes into account the relative importance of the requirement to achieving the objectives of the Act or FINTRAC's mandate when it considers the harm done by a compliance program violation. FINTRAC also considers the extent of the non-compliance and mitigating factors.

When assessing the extent of the non-compliance of compliance program violations, FINTRAC considers the degree to which the documentation and application of a requirement meet the Act and its regulations. More importance (weight) is given to the application of a requirement because it is the action of putting something into practice that is most effective to achieve the objectives of the Act and FINTRAC's mandate. For example, when compliance policies and procedures, documented in a comprehensive manner, are not put into practice, there is a big risk of non-compliance, which prevents the objectives of the Act and FINTRAC's mandate from being achieved.

2.1.1 Types of non-compliance for violations related to the compliance program There are two types of compliance program violations: complete or widespread non-compliance and partial non-compliance.

"Complete" or "widespread" non-compliance is when a requirement has not been met because an RE has not put in place measures to meet the requirement to any degree, or what is in place is too rudimentary. This poses the highest harm to the achievement of the objectives of the Act and FINTRAC's mandate. For example, an RE is in complete violation of the requirement under paragraph 71(1)(b) the Proceeds of Crime Money Laundering and Terrorist Financing Regulations (PCMLTFR) if there are no policies and procedures whatsoever documented or put into practice. This poses the highest harm because there would be no measures in place to comply with any of the requirements under the Act and its regulations.

"Partial" non-compliance is when only parts, or elements, of a requirement have not been met. For example, an RE that has incomplete policies and procedures when it comes to the detection and reporting of suspicious transactions would be in partial violation of the requirement under PCMLTFR 71(1)(b). This poses less harm than the previous example and poses varying levels of harm, depending on the issue.

Penalty amounts for complete or widespread violations and partial violations are calculated based on their associated levels of harm, as described below.

2.2 Levels of harm and penalty amounts for violations related to the compliance program

Compliance program violations are classified as a "serious" under the Proceeds of Crime (Money Laundering) and Terrorist Financing Administrative Monetary Penalties Regulations(AMP Regulations) with penalties ranging from $1—$100,000.

For these violations, FINTRAC has identified four levels of harm. Each level of harm incurs a penalty of either $100,000, $75,000, $50,000 or $25,000.

The table below lists the four levels of harm in descending order, the types of non-compliance and the descriptions of harm along with their corresponding penalty.

Level of harm	Type of non-compliance	Description of harm	Penalty (not considering mitigating factors)
Level 1	The requirement is not met, to any degree, or what is in place is not functional, causing widespread non-compliance. This is complete or widespread non-compliance.	Prevents the achievement of the objectives of the Act and of FINTRAC's mandate because a core AML/ATF measure is absent or non-functional.	$100,000
Level 2	An element that is priority for achieving the objectives of the Act or FINTRAC's mandate is not met. This is partial non-compliance with important weaknesses.	Prevents the achievement of results that are priority for meeting the objectives of the Act and FINTRAC's mandate.	$75,000

Level of harm	Type of non-compliance	Description of harm	Penalty (not considering mitigating factors)
Level 3	An element that forms the basis for achieving the objectives of the Act or FINTRAC's mandate is not met.This is partial non-compliance with moderate weaknesses.	Prevents the achievement of results that form the basis for meeting the objectives of the Act and FINTRAC's mandate.	$50,000
Level 4	An element that enables the efficient achievement of the objectives of the Act or FINTRAC's mandate is not met. This is partial non-compliance with lesser weaknesses.	Diminishes the efficient achievement of the objectives of the Act and FINTRAC's mandate.	$25,000

Table 1—Levels of harm and penalties for violations related to compliance program

The highest level of harm (Level 1) applies to situations of complete or widespread non-compliance because they have the greatest potential impact on the Act's objectives or FINTRAC's mandate. As such, they incur the prescribed maximum penalty which is $100,000.

Levels of harm 2, 3 and 4 apply to situations of partial non-compliance and incur penalty amounts decreasing in intervals from $75,000 to $50,000 and to $25,000 respectively.

FINTRAC will consider relevant mitigating factors that could reduce the penalty down to the prescribed minimum penalty amount of $1, regardless of the violation's level of harm.

The remainder of this guide describes how FINTRAC applies the levels of harm to the compliance program violations.

3. Violation related to the appointment of a compliance officer

This section outlines FINTRAC's approach for failing to appoint a compliance officer, including the harm assessment and penalty calculation.

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
9.6(1)	71(1)(a)	Failure of a person or entity to appoint a person to be responsible for the implementation of a compliance program	Serious$1-$100,000

Table 2— Violation related to the appointment of a compliance officer

3.1 Harm done in the case of a violation related to the appointment of a compliance officer

The purpose of appointing a person responsible for the implementation of a compliance program is to ensure that an RE has the necessary oversight to effectively comply with the requirements of the Act. The person in this role, typically referred to as the compliance officer, is responsible for putting into practice the compliance policies and procedures, ML/TF risk assessment, ongoing compliance training program and the prescribed review of the compliance program.

An effective compliance program begins with the appointment of a compliance officer; but simply appointing a person to this position is not sufficient to meet the objectives of the Act. In order for an RE to meet the requirement, it must ensure that the compliance officer has adequate knowledge of the Act and its regulations, possesses the authority and has access to adequate resources to implement the compliance program.

Failing to appoint a person responsible for the implementation of the compliance program may result in the RE not meeting the reporting, record keeping, verifying identity, and applying other compliance measures requirements. This could result in structural gaps that leave the RE vulnerable to ML/TF offences, which affects the achievement of the objectives of the Act and FINTRAC's ability to

carry out its mandate, which potentially exposes Canada's financial system and Canadians to ML/TF risks.

Deficiencies in other compliance requirements, such as reporting, record keeping and verifying identity, may be the result of the deficient implementation of a compliance program. FINTRAC will consider the overall effectiveness of the compliance program and the fulfillment of other compliance requirements when it assesses an RE's compliance with the requirement to appoint a compliance officer.

3.2 Penalty determination for a violation related to the appointment of a compliance officer

FINTRAC will assess the level of harm and penalty for failing to appoint a compliance officer using the criteria listed below.

Level of harm	Type of non-compliance	Description of non-compliance with the compliance officer requirement	Penalty (not considering mitigating factors)
Level 1	The requirement is not met to any degree, or what is in place is not functional, causing widespread non-compliance. This is complete or widespread non-compliance.	No one is carrying out the duties of implementing any part of the compliance program. As such, there is widespread and serious non-compliance.	$100,000

Level of harm	Type of non-compliance	Description of non-compliance with the compliance officer requirement	Penalty (not considering mitigating factors)
Level 2	An element that is priority to achieving the objectives of the Act or FINTRAC's mandate is not met. This is partial non-compliance with important weaknesses.	The RE has not ensured that the appointed person performs all the necessary duties related to the: 1. Implementation of the compliance policies and procedures;2. Implementation of the policies and procedures related to mitigating high risks3. Implementation of the risk-based approach in accordance with the risk assessment; 4. Implementation of the ongoing training program;5. Implementation of the prescribed review of the compliance program every 2 years; and6. Implementation of other applicable requirements under the Act and its regulations.	$75,000

Level of harm	Type of non-compliance	Description of non-compliance with the compliance officer requirement	Penalty (not considering mitigating factors)
Level 3	An element that forms the basis for achieving the objectives of the Act or FINTRAC's mandate is not met.This is partial non-compliance with moderate weaknesses.	The RE has not provided the appointed person with the authority to implement the compliance program, including the authority to make any necessary changes. The RE has not provided the appointed person with adequate resources to implement the compliance program.	$50,000
Level 4	An element that enables the efficient achievement of the objectives of the Act or FINTRAC's mandate is not met. This is to partial non-compliance with lesser weaknesses.	The RE has not ensured that the appointed person has adequate knowledge of the Act and its regulations, and how the requirements apply to the business.	$25,000

Table 3—Levels of harm and penalties for a violation related to the appointment of a compliance officer

3.2.1 Level 1 harm: Failure to appoint a person responsible for the implementation of the compliance program When an RE fails to assign the duties related to the implementation of the compliance program to a person, the objectives of the Act and FINTRAC's mandate suffer from the highest level of harm. This is because there would be no oversight to ensure that, for example, policies and procedures are followed, or that ongoing training is provided. This lack of oversight means that there is a high risk that the existing compliance program will become out-of-date or ineffective. Over time, this would likely have an important impact on an RE's compliance with the Act and its regulations, and would likely result in other requirements not being met, such as reporting, record keeping and verifying client identity. As a result, the associated penalty is the prescribed maximum of $100,000.

3.2.2 Level 2 harm: Failure to ensure that the appointed person performs all the necessary duties The second-highest level of risk is attributed when an RE has appointed a compliance officer with the proper authorities and resources but it has not made sure that this person performs all the duties related to the implementation of the compliance program. As a result, the associated penalty is $75,000.

3.2.3 Level 3 harm: Failure to provide the appointed person with authority and resources When the appointed person lacks the authority and resources to carry out the duties and measures that are necessary for the implementation and maintenance of the compliance program, this can result in inefficiencies in detecting and correcting non-compliance with the requirements of the Act and its regulations. As a result, the associated penalty is $50,000.

3.2.4 Level 4 harm: Failure to ensure that the appointed person has adequate knowledge At a minimum, the RE must ensure that the compliance officer has sufficient knowledge of the Act and its regulations, of ML/TF concepts and risks and of how they relate to the business. The compliance officer must have a good understanding of the risks most relevant to the RE and frequently encountered by the industry. Without this knowledge, the measures adopted may not be the most effective or efficient to addressing the RE's compliance needs, thereby affecting the implementation of the compliance program. As a result, the associated penalty is $25,000.

4. Violations related to compliance policies and procedures, including policies and procedures in respect of prescribed special measures for high risks

This section outlines FINTRAC's approach for failing to develop and apply compliance policies and procedures, including the harm assessment and penalty calculation.

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
9.6(1)	71(1)(b)	Failure of a person or entity to develop and apply written compliance policies and procedures that are kept up to date and, in the case of an entity, are approved by a senior officer	Serious$1-$100,000
9.6(3)	71.1	Failure of a person or entity to take the prescribed special measures	Serious$1-$100,000

Table 4— Violations related to compliance policies and procedures, including policies and procedures in respect of prescribed special measures for high risks

4.1 Harm done in the case of violations related to compliance policies and procedures

The development, documentation and application of compliance policies and procedures, including those for enhanced measures to mitigate high risk, ensure that a comprehensive framework and robust controls are in place to comply with the Act and its regulations.

Policies guide REs' decisions and actions with respect to AML/ATF requirements, and ensure that all activities take place within set boundaries. Procedures are the specific methods employed to put policies in action in day-to-day operations.

Policies and procedures are critical because they set out important principles and standards that staff and delegated persons with compliance responsibilities must meet in a consistent manner. Documented policies and procedures also serve to ensure clarity and consistency in business operations for instance, when there are changes in personnel. For each requirement under the Act and its regulations, the policies and procedures documents must include a description of when the requirement is triggered; the information that must be reported, recorded or considered; the step-by-step procedures to ensure that the requirement is fulfilled; and where applicable, the timelines associated to the requirement.

Failing to develop, apply, and keep written policies and procedures up to date can result in not meeting other requirements under the Act and its regulations, and undervalues sound business practices designed to minimize ML/TF.

4.2 Penalty determination for a violation related to compliance policies and procedures

FINTRAC will assess the level of harm and penalty for failing to develop, document and apply written compliance policies and procedures using the criteria listed below.

Level of harm	Type of non-compliance	Description of the non-compliance with the compliance policies and procedures requirement	Penalty (not considering mitigating factors)
Level 1	The requirement is not met to any degree, or what is in place is not functional, causing widespread non-compliance. This is complete or widespread non-compliance.	Policies and procedures for all, or most, of the requirements are not developed or applied.	$100,000

Level of harm	Type of non-compliance	Description of the non-compliance with the compliance policies and procedures requirement	Penalty (not considering mitigating factors)
Level 2	An element that is priority for achieving the objectives of the Act or FINTRAC's mandate is not met. This is partial non-compliance with important weaknesses.	Policies and procedures for priority requirements are not developed or applied, including:1. Know your client requirements: 1. verifying client identity 2. determination of politically exposed persons and heads of international organizations, and their family members and close associates 3. obtaining beneficial ownership information 4. third party determination2. Suspicious transaction and terrorist property reporting; and3. Compliance with Ministerial Directives.	$75,000

Level of harm	Type of non-compliance	Description of the non-compliance with the compliance policies and procedures requirement	Penalty (not considering mitigating factors)
Level 3	An element that forms the basis for achieving the objectives of the Act or FINTRAC's mandate is not met.This is partial non-compliance with moderate weaknesses.	Policies and procedures for basic requirements are not developed or applied, including:1. Reporting large cash transactions, and if applicable electronic funds transfers, and casino disbursements; 2. Ongoing monitoring of business relationships 3. Keeping prescribed records, **except** copies of submitted Suspicious Transaction Reports (STRs) and Casino Disbursement Reports (CDRs); and4. Performing the prescribed risk assessment and the prescribed review every 2 years.	$50,000

Level of harm	Type of non-compliance	Description of the non-compliance with the compliance policies and procedures requirement	Penalty (not considering mitigating factors)
Level 4	An element that enables the efficient achievement of the objectives of the Act or FINTRAC's mandate is not met. This is partial non-compliance with lesser weaknesses.	Policies and procedures for requirements that enable efficiency are not developed or applied, including keeping copies of submitted STRs and CDRs.	$25,000

Table 5—Levels of harm and penalties for violations related to compliance policies and procedures

4.2.1 Level 1 harm: Policies and procedures are not developed or applied When policies and procedures have not been developed or are not applied, the foundational framework and controls that are required to comply with the requirements of the Act and its regulations are absent. This creates an environment where widespread non-compliance and systemic weaknesses in detecting, preventing and deterring ML/TF is possible, and therefore poses the most harm to the objectives of the Act and FINTRAC's mandate. As a result, the associated penalty is the prescribed maximum of $100,000.

4.2.2 Level 2 harm: Policies and procedures for priority requirements are not developed or applied Reporting suspicious transactions and terrorist property, performing know your client procedures and complying with the minister's directives are priority requirements for Canada's AML/ATF efforts, because they are essential for the detection, prevention and deterrence of ML/TF offences. Non-compliance with these requirements is assessed as posing Level 2 harm because, while other measures may be in place, failing to meet priority requirements can pose high levels of harm to the objectives of the Act and FINTRAC's ability to fulfill its mandate. As a result, the associated penalty is $75,000.

The detection and reporting of transactions that are suspected of being related to ML/TF is therefore critical for FINTRAC's analysis and disclosure of financial intelligence that supports the investigation and prosecution of the crimes. Performing know your client procedures such as identifying clients and obtaining information on those controlling or benefitting from the movement of funds deter criminals from using Canada's financial system for ML/TF; they are also necessary to identify high-risk clients, business relationships and transactions for the purpose of reporting to FINTRAC. When proper client identification, and information on the individuals owning or controlling entities measures are not taken by REs, the objectives of the Act and FINTRAC's mandate are harmed significantly since it is then not possible for the RE to mitigate risks; for FINTRAC to conduct analysis on particular subjects; for law enforcement to investigate individuals for ML/TF offences.

Ministerial directives are targeted measures to protect Canada's financial system from being used as a vehicle for ML/TF. Compliance policies and procedures that do not meet the measures set out in a ministerial directive can result in the failure to comply with priority areas intended to detect, prevent and deter specific threats to Canada's financial system and the safety of Canadians. As a result, such a failure represents very significant harm to the achievement of the objectives set out in paragraph 3(d) of the Act.

4.2.3 Level 3 harm: Policies and procedures for basic requirements are not developed or applied Requirements that form the basis for the detection, prevention and deterrence of ML/TF are: reporting large cash transactions, reporting electronic funds transfers and casino disbursements (as required), monitoring business relationships, record keeping, assessing risk, and reviewing the effectiveness of the compliance program. Record keeping requirements are in place to ensure that the information necessary to meet other requirements of the Act and its regulations is kept. Ultimately, the information can serve as evidence in support of investigations and prosecutions of ML/TF offences.

The measures to implement these requirements are fundamental because they support Canada's AML/ATF regime by identifying and mitigating the risks related to transactions at risk of being used for ML/TF, and by helping to detect and deter those inclined to abuse the financial system for ML/TF purposes. Non-compliance with these requirements is assessed as Level 3 harm because it can pose moderate harm to the objectives of the Act and FINTRAC's mandate. Therefore, the associated penalty is $50,000.

4.2.4 Level 4 harm: Policies and procedures for requirements that enable efficiency are not developed or applied Efficiency in the fight against ML/TF is found in those elements that assist in achieving the objectives of the Act and FINTRAC's mandate and support Canada's AML/ATF regime by maximizing its performance. Non-compliance with these elements poses Level 4 harm because it diminishes the efficiency of Canada's AML/ATF

regime, but does not affect priority or basic elements. Therefore, the associated penalty is $25,000.

Keeping complete and accurate records, including copies of STRs, and CDRs (as required), ensures that REs, police, law enforcement and FINTRAC have quick and easy access to reports related to transactions or financial activities. The information captured in STRs and CDRs is required in other records under the Act. Since the information in these copies is likely kept elsewhere, failing to keep these records poses lower harm to the objective of the Act and FINTRAC's mandate.

4.3 Penalty determination for a violation related to compliance policies and procedures for taking enhanced measures to mitigate high risks

FINTRAC will assess the level of harm and penalty for failing to develop, document and apply compliance policies and procedures on taking enhanced measures to mitigate high risks using the criteria listed below.

Level of harm	Type of non-compliance	Description of the non-compliance with the policies and procedures for taking enhanced measures to mitigate high risks requirement	Penalty (not considering mitigating factors)
Level 1	The requirement is not met to any degree, or what is in place is not functional, causing widespread non-compliance. This is complete or widespread non-compliance.	Policies and procedures for taking enhanced measures for high risk are not developed or applied for any, or most, of the prescribed elements.	$100,000

Level of harm	Type of non-compliance	Description of the non-compliance with the policies and procedures for taking enhanced measures to mitigate high risks requirement	Penalty (not considering mitigating factors)
Level 2	An element that is priority for achieving the objectives of the Act or FINTRAC's mandate is not met. This is partial non-compliance with important weaknesses.	Policies and procedures relating to priority requirements for enhanced measures are not developed or applied for:1. Verifying client identity;2. Keeping client and beneficial ownership information up to date; and;3. Conducting ongoing monitoring of business relationships to identify suspicious transactions.	$75,000

Level of harm	Type of non-compliance	Description of the non-compliance with the policies and procedures for taking enhanced measures to mitigate high risks requirement	Penalty (not considering mitigating factors)
Level 3	An element that forms the basis for achieving the objectives of the Act or FINTRAC's mandate is not met.This is partial non-compliance with moderate weaknesses.	Policies and procedures relating to basic requirements for enhanced measures are not developed or applied, which includes any other measures needed to mitigate high risk.	$50,000

Table 6—Levels of harm and penalties for a violation related to compliance policies and procedures for taking enhanced measures to mitigate high risks violations

Note: Level 4 harm is not applicable in the case of this violation, as the measures related to addressing high-risk situations do not play a supporting role; they are either priority or basic elements to mitigate the risks of ML/TF.

4.3.1 Level 1 harm: Policies and procedures for taking enhanced measures to mitigate high risks are not developed or applied for any, or most, of the prescribed elements The development and application of policies and procedures for taking prescribed enhanced measures to mitigate high risk is critical to the AML/ATF regime in the detection, prevention and deterrence of ML/TF offences. These enhanced measures are meant to address the risks posed by those elements that have been expressly identified as being the most vulnerable to ML/TF. When policies and procedures for taking enhanced measures to mitigate high risks have not been developed for any, or most of the prescribed requirements, the controls and framework that are required to mitigate high risks are absent. There is a high likelihood that the highest-risk situations are not being mitigated and identified for reporting to FINTRAC,

leaving the RE and Canada's financial system vulnerable to ML/TF offences. This poses the highest harm and incurs a penalty of $100,000.

4.3.2 Level 2 harm: Policies and procedures related to priority enhanced measures are not developed or applied Taking enhanced measures to identify persons and entities controlling and benefitting from the movement of funds, keep their information up to date, and conduct ongoing monitoring to detect suspicious transactions are priority measures for ML/TF risk mitigation as they help make the most current information available in situations of high risk. Policies and procedures that do not address these elements are incomplete and can result in inadequate risk mitigation; and have a substantial impact on the detection and mitigation of high risks, including reporting related to high-risk transactions. This represents an important weakness in an RE's compliance program, which could have an important impact on the objectives of the Act and FINTRAC's mandate; and therefore poses Level 2 harm, which incurs a penalty of $75,000.

4.3.3 Level 3 harm: Policies and procedures relating to any other enhanced measures needed to mitigate high risks are not developed or applied In addition to the specific enhanced measures prescribed for high-risk mitigation, other mitigation measures may also be necessary to reduce ML/TF vulnerabilities. Policies and procedures that do not consider other measures specific to the RE's assessment of risks can result in ineffective or incomplete strategies to reduce ML/TF vulnerabilities. Depending on the nature of the risk and the RE's size and complexity, this type of non-compliance could have an impact on the objectives of the Act and FINTRAC's mandate. This type of non-compliance poses Level 3 harm and incurs a penalty of $50,000.

5. Violation related to assessing and documenting the risks of ML/TF

This section outlines FINTRAC's approach to failing to assess and document the risks of ML/TF, including the harm assessment and penalty calculation.

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
9.6(1)	71(1)(c)	Failure of a person or entity to assess and document the risk referred to in subsection 9.6(2) of the Act, taking into consideration prescribed factors	Serious$1-$100,000

Table 7— Violation related to assessing and documenting the risks of ML/TF

5.1 Harm done in the case of a violation related to assessing and documenting the risks of ML/TF

Assessing and documenting ML/TF risks ensures that REs are aware of their potential exposure and vulnerability to ML/TF. By identifying areas and levels of risk, REs may apply appropriate mitigation measures to reduce those risks. REs are able to turn more attention to higher-risk areas, thereby effectively contributing to the objectives of the Act and FINTRAC's ability to carry out its mandate.

Failing to assess and document the risks of ML/TF prevents REs from identifying areas of its operations that are vulnerable to being exploited for ML/TF purposes, and prevents appropriate mitigation measures from being put in place. This can also lead to failing to identify high-risk clients and business relationships for which enhanced risk mitigation measures must be applied. This can further result in the failure to detect and report suspicious transactions to FINTRAC.

5.2 Penalty determination for a violation related to assessing and documenting the risks of ML/TF

FINTRAC will assess the level of harm and penalty for failing to assess and document the risks of ML/TF offences using the criteria listed below.

Level of harm	Type of non-compliance	Description of the non-compliance for the risk assessment requirement	Penalty (not considering mitigating factors)
Level 1	The requirement is not met, to any degree, or what is in place is not functional, causing widespread non-compliance. This is complete or widespread non-compliance	An assessment of ML/TF risks has not been conducted or documented for any, or most, of the prescribed factors.	$100,000

Level of harm	Type of non-compliance	Description of the non-compliance for the risk assessment requirement	Penalty (not considering mitigating factors)
Level 2	An element that is priority for achieving the objectives of the Act or FINTRAC's mandate is not met. This is partial non-compliance with important weaknesses.	The risk assessment does not include priority elements, including those for high-risk situations, such as: 1. Politically exposed foreign persons, their family members and close associates;2. Entities for which beneficial ownership information cannot be obtained or confirmed;3. Clients who are mentioned in a submitted TPR; and4. Products, services, delivery channels, geographic locations or types of persons or entities, that are identified as posing a high risk by a ministerial directive, by FINTRAC, or by criteria established by the RE.	$75,000

Level of harm	Type of non-compliance	Description of the non-compliance for the risk assessment requirement	Penalty (not considering mitigating factors)
Level 3	An element that forms the basis for achieving the objectives of the Act or FINTRAC's mandate is not met.This is partial non-compliance with moderate weaknesses.	The risk assessment does not include basic elements such as:1. Products, services and delivery channels offered;2. Clients and business relationships;3. Geographic locations, (including foreign and domestic activities, clients, and business relationships); and4. New technologies.	$50,000
Level 4	An element that enables the efficient achievement of the objectives of the Act or FINTRAC's mandate is not met. This is to partial non-compliance with lesser weaknesses.	The risk assessment does not include other relevant factors that could impact ML/TF risks.	$25,000

Table 8—Levels of harm and penalties for a violation related to assessing and documenting the risks of ML/TF

5.2.1 Level 1 harm: An assessment of ML/TF risks has not been conducted or documented for any, or most, of the prescribed factors

When an assessment of ML/TF risks has not been conducted or documented, or the assessment does not address any of the prescribed requirements, there is complete or widespread non-compliance with the regulations. Failing to assess and identify ML/TF risks prevents REs from putting in place mitigation measures, leaving them vulnerable to being used for ML/TF, especially in those areas that pose the highest risk. This is assessed as posing the highest level of harm, as it has the highest impact on achieving objectives of the Act and FINTRAC's mandate, and incurs a penalty of $100,000.

5.2.2 Level 2 harm: The risk assessment does not include priority elements including those for high-risk situations The regulations, ministerial directives, FINTRAC and other AML/ATF authorities have identified situations that inherently present a high risk of ML/TF, which are key for the prescribed risk assessment. It is critical for REs to consider and assess them where applicable. Failing to consider high-risk situations may result in important weaknesses in the compliance program such as poor mitigation measures and high-risk situations potentially not being detected and reported to FINTRAC on suspicion of ML/TF offences. Non-compliance with this requirement poses Level 2 harm and incurs a penalty of $75,000.

5.2.3 Level 3 harm: The risk assessment does not include the basic elements ML/TF risk assessments allow REs to understand the vulnerabilities they are exposed to. Comprehensive risk assessments must include the prescribed elements as their basis in order to support risk mitigation. A risk assessment that does not include one or more of the prescribed elements may lead to weaknesses in the identification and mitigation of common risks, leaving the RE vulnerable to ML/TF offences and unable to effectively identify transactions that must be reported. Non-compliance with this requirement poses Level 3 harm and incurs a penalty of $50,000.

5.2.4 Level 4 harm: The risk assessment does not include any other relevant factors that could impact ML/TF risks Assessing other relevant factors allows REs to understand the ML/TF risks applicable to their operations and contributes to the efficiency of the risk assessment and mitigation strategies. Non-compliance with this requirement poses Level 4 harm and incurs a penalty of $25,000.

6. Violation related to the ongoing training program

This section outlines FINTRAC's approach to failing to develop and maintain a written ongoing training program, including the harm assessment and penalty calculation.

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
9.6(1)	71(1)(d)	Failure of a person or entity that has employees, agents or mandataries or other persons authorized to act on their behalf to develop and maintain a written ongoing compliance training program for those employees, agents or mandataries or persons	Serious$1-$100,000

Table 9— Violation related to the ongoing training program

6.1 Harm done in the case of a violation related to the ongoing training program

The purpose of a written ongoing compliance training program is to ensure that all employees, agents, mandataries and other persons authorized to act on an RE's behalf understand the requirements of the Act and its regulations and follow the policies and procedures that have been established for compliance. It also ensures that employees, agents, mandataries and other persons authorized to act on an RE's behalf understand ML/TF matters enough to be able to identify facts that may indicate financial transactions or activities related to ML/TF offences.

Failing to develop and maintain a written ongoing training program may result in the above listed purposes not being met over time, and consequently, an RE failing to comply with the requirements under the Act and its regulations. In turn, this non-compliance could ultimately affect the objectives of the Act and FINTRAC's ability to deliver on its mandate.

6.2 Penalty determination for a violation related to the ongoing training program

FINTRAC will assess the level of harm and penalty for failing to develop and maintain a written ongoing training program using the criteria listed below.

Level of harm	Type of non-compliance	Description of the non-compliance for the training program requirement	Penalty (not considering mitigating factors)
Level 1	The requirement is not met to any degree, or what is in place is not functional, causing widespread non-compliance. This is complete or widespread non-compliance.	A documented training program is not developed or maintained to cover all, or most, of the elements to comply with the Act and its regulations.	$100,000

Level of harm	Type of non-compliance	Description of the non-compliance for the training program requirement	Penalty (not considering mitigating factors)
Level 2	An element that is priority for achieving the objectives of the Act or FINTRAC's mandate is not met. This is partial non-compliance with important weaknesses.	The training program is missing priority elements, such as maintaining training on the:1. Compliance policies and procedures established; 2. Responsibilities of employees, agents and those acting on behalf of the RE when dealing with suspicious transactions; and3. Key ML/TF concepts including background information on how ML/TF related to the business.	$75,000

Level of harm	Type of non-compliance	Description of the non-compliance for the training program requirement	Penalty (not considering mitigating factors)
Level 3	An element that forms the basis for achieving the objectives of the Act or FINTRAC's mandate is not met.This is partial non-compliance with moderate weaknesses.	The training program is missing basic elements, such as:1. Frequency or timing of the training to be delivered; and2. Content that is relevant and specific for all employees, agents, and those acting on the RE's behalf.	$50,000
Level 4	An element that enables the efficient achievement of the objectives of the Act or FINTRAC's mandate is not met. This is to partial non-compliance with lesser weaknesses.	The training program is not maintained on an ongoing basis.	$25,000

Table 10—Levels of harm and penalties for a violation related to the ongoing training program

6.2.1 Level 1 harm: A documented training program is not developed or maintained When a training program has not been developed or maintained, or has been but only to a minimal degree, the foundational framework and controls that are required to comply with the requirements of the Act and its regulations are absent. This can potentially lead to widespread non-compliance and systemic weaknesses in the detection, prevention and de-

terrence of ML/TF, posing the highest possible harm to the Act's objectives and FINTRAC's mandate. Therefore, the penalty is $100,000, the prescribed maximum amount.

6.2.2 Level 2 harm: The training program is missing elements that are priority Priority elements for the training program include covering the established policies and procedures to comply with all the requirements of the Act and its regulations, the responsibilities of employees, agents and those acting on the RE's behalf when dealing with suspicious transactions, and key ML/TF concepts including background information on how they relate to the business. Non-compliance with these elements is assessed as Level 2 harm because a lack of training in these elements could cause failures in meeting other requirements such as reporting, record keeping and verifying client identity. As a result, the penalty is $75,000.

6.2.3 Level 3 harm: The training program is missing elements that are basic A plan that addresses the timing and frequency of delivery of the training program, that identifies who will receive the training and that includes content that is relevant and specific to different roles in the organization is forms the basis for the delivery of the training program. Not only does it help to comply with the requirement to maintain an ongoing training program, but it clearly lays out which employees, agents and those acting on an RE's behalf are to be provided with relevant training to effectively comply with all the requirements. The likelihood of exposure to ML/TF offences and associated risks varies for employees, depending on their roles. For example, tailored training for employees that detect transactions that need to be reported, that verify client identity, that keep records, and perform other customer due diligence measures will have a greater impact on compliance. Non-compliance with these requirements poses Level 3 harm, which incurs a penalty of $50,000.

6.2.4 Level 4 harm: The training program is not maintained on an ongoing basis Efficiency in the fight against ML/TF is found in those elements that assist in achieving the objectives of the Act and FINTRAC's mandate, and support Canada's AML/ATF regime by maximizing its performance. Guidelines dictating the frequency of training ensure that personnel receive information and training on new compliance requirements and are provided with reminders on existing requirements. Failing to establish clear guidelines for ongoing compliance training may result in program weaknesses over time, for example, due to changes to regulatory requirements, or changes in staff or organizational structure. This may lead to the RE not meeting its requirements to report, identify clients and keep records. Non-compliance with this requirement is assessed as posing Level 4 harm and incurs a penalty of $25,000.

7. Violations related to the prescribed review

This section outlines FINTRAC's approach to failing to institute and document the prescribed review, including the harm assessment and penalty calculation.

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
9.6(1)	71(1)(e)	Failure of a person or entity to institute and document the prescribed review	Serious$1-$100,000
9.6(1)	71(2)	Failure of a person or entity to report prescribed information within 30 days after assessment	Serious$1-$100,000

Table 11—Violations related to the prescribed review

7.1 Harm done in the case of violations related to the prescribed review

Changes to an organization's structure, personnel, policies and processes, and environment may over time, if not immediately, require revisions to the compliance program that is in place. The purpose of the prescribed review is to ensure that the RE's compliance program is continuously adapted to continue to comply with the requirements of the Act and its regulations. The prescribed review of the compliance policies and procedures, and that of the ongoing training program tests the reporting, client identity verification, record keeping and appropriate mitigation measures application. The prescribed review of the risk assessment ensures that the RE is adequately assessing, identifying and mitigating the risks of ML/TF over time.

Failing to conduct the prescribed review signals that the RE may not be fulfilling one or more of its other requirements under the Act and its regulations, by not having kept up to date with changes in the organization or external changes such as new technologies in the financial sector and regulatory updates. Additionally, any gaps or ineffective processes in the existing compliance program may go undetected, leading to uncorrected non-compliance. For example, the RE's existing risk assessment may not identify its most vulnerable areas, making it difficult to apply appropriate mitigating measures, to reduce the risks of ML/TF and contribute to safety of Canada's financial system and that of Canadians.

Ultimately, undetected non-compliance and inefficiencies could result in harming the achievement of the objectives of the Act and FINTRAC's mandate.

7.2 Penalty determination for violations related to the prescribed review

FINTRAC will assess the level of harm and penalty for failing to institute and document the prescribed review using the criteria listed below.

Level of harm	Type of non-compliance	Description of the non-compliance with the prescribed review requirement	Penalty (not considering mitigating factors)
Level 1	The requirement is not met to any degree, or what is in place is not functional, causing widespread non-compliance. This is complete or widespread non-compliance.	The RE has not conducted any part or most of the prescribed review.	$100,000
Level 2	An element that is priority for achieving the objectives of the Act or FINTRAC's mandate is not met. This is partial non-compliance with important weaknesses.	The review does not include testing for effectiveness; andThe scope of the review does not cover the compliance policies and procedures, risk assessment, and training program.	$75,000

Level of harm	Type of non-compliance	Description of the non-compliance with the prescribed review requirement	Penalty (not considering mitigating factors)
Level 3	An element that forms the basis for achieving the objectives of the Act or FINTRAC's mandate is not met.This is partial non-compliance with moderate weaknesses.	The review does not evaluate the compliance program documentation, such as policies and procedures, to ensure that they are complete and up to date.	$50,000
Level 4	An element that enables the efficient achievement of the objectives of the Act or FINTRAC's mandate is not met. This is to partial non-compliance with lesser weaknesses.	The review is conducted beyond the prescribed two-year period.The review methods are not clearly documented and do not demonstrate how the compliance program is tested for effective-ness.When required, an internal or external auditor did not conduct the review.	$25,000

Table 12—Levels of harm and penalties for violations related to the prescribed review

7.2.1 Level 1 harm: The RE has not conducted any part or most of the prescribed review When an RE does not conduct the prescribed

review, or when the review is absolutely minimal, this poses the highest harm to the objectives of the Act and FINTRAC's mandate. It is highly possible that policies, procedures, training, and risk assessments are outdated, inaccurate or ineffective, and therefore non-compliance with reporting, record keeping and client identification requirements is also more likely. This represents Level 1 harm, which incurs a penalty of $100,000 as the requirement has not been met to any degree, or in a manner that is too minimal for the requirement to be considered as being met.

7.2.2 Level 2 harm: The review does not include testing for effectiveness; and the scope of the review does not cover the compliance policies and procedures, risk assessment, and training program Effectiveness testing and a comprehensive review are key to meeting the requirement. Next to not instituting the prescribed review, the second-highest level of harm comes from reviews that do not include testing the effectiveness of the compliance program, and reviews that do not cover key elements of the compliance policies and procedures, risk assessment, and training program. This type of non-compliance poses Level 2 harm and incurs a penalty of $75,000.

A review that does not include effectiveness testing does not look at how the compliance program is applied in practice. It is essentially only a theoretical review of the documentation that has been developed. Even if the documentation were in order, there is still the potential that the policies and procedures are not being put into practice and this poses a high risk of errors and inadequacies in the compliance program that are not detected.

Additionally, when the review is incomplete, meaning that key elements are overlooked from the assessment, large gaps and weaknesses in the compliance program can go undetected. For example, if the review omitted to assess the training program, the staff may not be trained properly to carry out their duties. In turn, this could result in non-compliance with requirements of the Act and its regulations, despite having policies and procedures, and risk assessments.

7.2.3 Level 3 harm: The review does not evaluate the compliance program documentation to ensure that they are complete and up to date The documentation of the compliance program is the basis from which compliance is achieved. To this end, the prescribed review should at a minimum assess the documented policies and procedures, training program and risk assessment to ensure that the standards established by the RE is clear, complete and up to date, in accordance with the requirements of the Act and its regulations. A review that does not evaluate the compliance program documentation for completeness and accuracy could lead to processes that are not clearly understood, or are applied inconsistently. This type of non-compliance poses Level 3 harm and incurs a penalty of $50,000.

7.2.4 Level 4 harm: The review is conducted beyond the prescribed two-year frequency; the review methods are not clearly documented and do not demonstrate how the compliance program is tested for effectiveness; and when required, an internal or external auditor did not conduct the review Efficiency in the fight against ML/TF is found in those elements that assist in achieving the objectives of the Act and FINTRAC's mandate, and support Canada's AML/ATF regime by maximizing its performance. Non-compliance with these elements poses Level 4 harm and incurs a penalty of $25,000.

In order to identify and correct gaps in the compliance program in a timely manner, the prescribed frequency of the review is every two years. Failing to institute a review that respects this frequency could result in unidentified deficiencies that remain uncorrected for an undetermined period of time. If the period between reviews is extensive, undetected deficiencies could be exploited for ML/TF purposes.

Clearly documenting the methods used to conduct the review and demonstrating how program effectiveness will be tested contributes to the efficiency of the review and the RE's AML/ATF efforts. For example, the method for sampling and testing should reflect the size and complexity of the RE's operations to ensure that the review's findings are representative.

Where applicable, an internal or external auditor is to perform the review. This is to ensure an independent assessment of the compliance program's effectiveness and that the findings are neutral and objective. The expertise of an auditor also ensures that the scope and the effectiveness testing are adequate and comprehensive.

7.3 Harm done in the case of a violation related to prescribed review reporting

Reporting prescribed information following the compliance program's review provides an RE's senior officer with a timely understanding and oversight of the RE's overall compliance with the Act and its regulations, and of changes that would be required to improve or ensure compliance and risk mitigation. Failing to report the results of the prescribed review to an RE's senior officer within 30 days of the assessment impedes the senior officer's ability to oversee the effective application of policies and procedures and to manage ML/TF risks. This can undermine risk mitigation, leaving the RE vulnerable to ML/TF offences.

7.4 Penalty determination for a violation related to prescribed review reporting

FINTRAC will assess the level of harm and penalty for a failing to report prescribed information on the review using the criteria listed below.

Level of harm	Type of non-compliance	Description of the non-compliance with the reporting on the prescribed review requirement	Penalty (not considering mitigating factors)
Level 1	The requirement is not met to any degree, or what is in place is not functional, causing widespread non-compliance. This is complete or widespread non-compliance.	There is no reporting, or minimal reporting, of the results of the review to a senior officer.	$100,000
Level 2	An element that is key to achieving the objectives of the Act or FINTRAC's mandate is not met. This is partial non-compliance with important weaknesses.	Priority elements of the prescribed review are not reported to a senior officer, including:1. Results;2. Updates to policies and procedures, if applicable; and3. The implementation status of the updates to policies and procedures.	$75,000

Level of harm	Type of non-compliance	Description of the non-compliance with the reporting on the prescribed review requirement	Penalty (not considering mitigating factors)
Level 3	An element that forms the basis for achieving the objectives of the Act or FINTRAC's mandate is not met.This is partial non-compliance with moderate weaknesses.	The prescribed information was reported to an individual who is not a senior officer and does not have the authority to ensure that the changes to the compliance program are implemented.	$50,000
Level 4	An element that enables the efficient achievement of the objectives of the Act or FINTRAC's mandate is not met. This is to partial non-compliance with lesser weaknesses.	The prescribed information was reported beyond the 30-day period following the assessment, delaying the implementation of the required compliance program changes.	$25,000

Table 13—Levels of harm and penalties for a violation related to prescribed review reporting

7.4.1 Level 1 harm: There is no reporting, or minimal reporting, of the results to a senior officer Reporting to senior staff helps to ensure that those responsible for the RE's compliance are aware of the program's performance, including the weaknesses that must be addressed and oversight of the compliance officer's implementation of the compliance program. The harm is the greatest when the results of the review are not reported, or when minimal results are reported to a senior officer because there is a high likelihood that those

responsible for the business would not be aware the compliance challenges, making it impossible to adequately assess their seriousness, manage risks, and take corrective measures where needed. Non-compliance of this type poses Level 1 harm and incurs a penalty of $100,000.

7.4.2 Level 2 harm: Priority elements of the prescribed review are not reported to a senior officer The priority elements of the prescribed review that must be reported to senior management include: the findings of the review, updates to policies and procedures, and the implementation status of the updates. These elements give senior management a comprehensive picture of the RE's state of compliance; with this information, management can take the appropriate actions to mitigate risks and correct non-compliance. When the reporting does not cover one or more of these priority elements, it is incomplete and poses Level 2 harm, incurring a penalty of $75,000.

7.4.3 Level 3 harm: The prescribed information was reported to an individual who is not a senior officer and does not have the authority to ensure that the changes to the compliance program are implemented If the results are reported to someone who is not a senior officer, or if they are reported to a senior officer who is not in the position to bring about changes to improve the compliance program, there is a risk that nothing will come of the review. Without a senior officer's involvement, the proper attention and resources will not be given to the compliance program. As result, non-compliance issues and ML/TF risks could remain and increase in gravity over time. This type of non-compliance poses Level 3 harm and incurs a penalty of $50,000.

7.4.4 Level 4 harm: The prescribed information was reported beyond the 30-day period following the assessment, delaying the implementation of the required compliance program changes Timely communication allows senior management to make informed strategic decisions. When the prescribed information was reported to a senior officer beyond the 30-day period following the assessment, the delay affects the changes to the compliance program, which diminishes the efficient achievement of the objectives of the Act and FINTRAC's mandate. Those in charge of an RE's governance are unable to oversee the timely and efficient improvement of the compliance program and manage the ML/TF risks. This type of non-compliance poses Level 4 harm and incurs a penalty of $25,000.

Risk assessment guidance

Overview

FINTRAC developed this guidance to help you understand, as a reporting entity (RE):

- the types of money laundering (ML) and terrorist financing (TF) risks that you may encounter as a result of your business activities and clients; and
- what is a risk-based approach (RBA) and how you can use one to conduct a risk assessment of your business activities and clients.

This guidance also provides tools that you can use to develop and implement mitigation measures to address high-risk areas identified through your risk assessment. You can use these tools or you can develop your own risk assessment tools.This guidance is applicable to all REs subject to the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and associated Regulations. However, **some risk assessment obligations and/or examples may only apply to certain sectors**.

As part of your compliance program requirements under the PCMLTFA and associated Regulations, you must conduct a risk assessment of your ML/TF risks.Footnote 1 You are responsible for completing and documenting your own risk assessment. However, FINTRAC does not prescribe how a risk assessment should be conducted. Rather, this guidance explains an internationally recognized way of conducting a risk assessment using an RBA and provides you with other tools that may help you meet your risk assessment obligations. For more information about your risk assessment obligations see FINTRAC's Compliance program requirements guidance.

Who is this guidance for

- All reporting entities (REs)

1. What is risk?

Risk is the likelihood of a negative occurrence or event happening and its consequences. In simple terms, risk is a combination of the chance that something may happen and the degree of damage or loss that may result. In the context of ML/TF, risk means:

- **At the national level:** Threats and vulnerabilities presented by ML/TF that put the integrity of Canada's financial system at risk, as well as the safety and security of Canadians. For example, organized crime groups operating in Canada that launder the proceeds of crime.
- **At the RE level:** Internal and external threats and vulnerabilities that could open an RE up to the possibility of being used to facilitate ML/TF activities. For example, a possible ML/TF risk at the RE level could be conducting business with clients located in high-risk jurisdictions or locations of concern.

Threats: A person, group or object that could cause harm. In the ML/TF context, threats could be criminals, third parties facilitating ML/TF, terrorists or terrorist groups or their funds.

Vulnerabilities: Elements of a business or its processes that are susceptible to harm and could be exploited by a threat. In the ML/TF context, vulnerabilities could include weak business controls or high-risk products or services.

2. What are inherent and residual risks?

Inherent risk is the risk of an event or circumstance that exists before you implement controls or mitigation measures.Footnote 2 Whereas residual risk is the level of risk that remains after you have implemented controls or mitigation measures.

When assessing risk, it is important to distinguish between inherent risk and residual risk. The RBA described in this guidance focuses on the inherent risks to your business, its activities and clients.

3. What is an RBA?

An RBA is a way for you to conduct your risk assessment by considering elements of your business, clients and/or business relationships to identify the impact of possible ML/TF risks, and to apply controls and measures to mitigate these risks.

The Financial Action Task Force (FATF), has developed a series of Recommendations that are recognized as the international standard for combating money laundering, terrorism financing and other related threats to the integrity of the international financial system. Recommendation 1 on the RBA, recognizes that an RBA is an effective way to combat money laundering and terrorist financing.

Using an RBA will enable you to:

- conduct a **risk assessment** of your business activities and clients taking into consideration certain elements, including:
  - your products, services and delivery channelsFootnote 3;
  - the geographic location of your activitiesFootnote 4;
  - new developments and technologiesFootnote 5;
  - your clients and business relationshipsFootnote 6;
  - the activities of your foreign and domestic affiliatesFootnote 7 — This only applies to you if you are a financial entity, life insurance company or securities dealer, and the affiliate carries out activities similar to those of a financial entity, life insurance company or securities dealer; and
  - any other relevant factorFootnote 8.
- **mitigate the risks you identify** through the implementation of controls and measures tailored to these risks, which includes the ongoing monitoring of business relationships for the purpose of:

  - keeping **client identification** information and, if required, beneficial ownership and business relationship information up to date in accordance with the assessed level of risk;Footnote 9 reassessing the level of risk associated with transactions and activities;Footnote 10and
  - applying **enhanced or special measures** to those transactions and business relationships identified as high-risk.Footnote 11

- identify and assess potential gaps or weaknesses of your compliance program. For example, using an RBA can help you to identify and assess risks that could impact other parts of your compliance program, such as gaps in your written policies, procedures or training program.

The PCMLTFA and associated Regulations do not prohibit you from having high-risk activities or high-risk business relationships. However, it is important that if you identify high-risk activities or high-risk business relationships that you document and implement appropriate controls to mitigate these risks and apply prescribed special measures.

It is important to remember that assessing and mitigating the risk of ML/TF is not a static exercise. The risks you identify may change or evolve over time as new products, services, affiliations, or developments and technologies enter your business or its environment. You should be regularly reassessing the ML/TF-related risks to your business, and documenting that assessment to keep it up to date. For example, if you add a new product, service or technology to your business, or open a new location, you should evaluate and document the associated risks of this change to your business.

4. What is the RBA cycle?

The RBA cycle consists of six steps to follow to complete a risk assessment. The diagram below summarizes the RBA cycle. Additional information on how to conduct each step can be found further below.

There is no prescribed methodology for the assessment of risks. FINTRAC's suggested model presents business-based and relationship-based risk assessments separately. Although presented separately in this guidance, you can complete business-based and relationship-based assessments simultaneously. You will need to adapt this model to your business should you choose to use it.

RBA cycle — Step 1: Identify your inherent risks of ML/TF

To identify your inherent risks of ML/TF, you would start by assessing the following areas of your business:

- products, services and delivery channels;
- geography;
- new developments and technologies;
- clients and business relationships;
- activities of foreign and domestic affiliates, if applicable; and

- any other relevant factors.

Business-based risk assessment Begin your risk assessment by looking at your business as a whole. This will allow you to identify where risks occur across business lines, clients or particular products or services. You will need to document mitigation controls for the areas you identify as high-risk.Footnote 12 The number of risks you identify will vary based on the type of business activities you conduct and products and/or services you offer.

To conduct a business-based risk assessment, you need to identify the inherent risks of your business by assessing your vulnerabilities to ML/TF. Your overall business-based risk assessment includes the risk posed by the following:

1. The combination of your products, services and delivery channels;
2. The geographical locations in which your business operates;
3. The impact of new developments and technologies that affect your operations;
4. The risks that result from affiliates (the activities that they carry out); and
5. Other relevant factors.

1. Products, services and delivery channels You need to identify the products, services and delivery channels or ways in which they combine that may pose higher risks of ML/TF. Delivery channels are mediums through which you offer products and/or services to clients, or through which you can conduct transactions. See Annex 2 — Table 1: Business-based examples of higher risk indicators and considerations for products, services and delivery channels.

2. Geography You need to identify the extent to which the geographic locations where you operate or undertake activities could pose a high-risk for ML/TF. Depending on your business and operations, this can range from your immediate surroundings, whether rural or urban, to a province or territory, multiple jurisdictions within Canada (domestic) or other countries. See Annex 2 — Table 2: Business-based examples of higher risk indicators and considerations for geography.

3. New developments and technologies You need to identify the risks associated with new developments and the adoption of new technologies within your business. That is, if your business intends to put in place a new service/activity/location or introduce a new technology, then you must assess it in order to analyze the potential ML/TF risks it may bring to your business, before you implement it. See Annex 2 — Table 3: Business-based examples of higher risk indicators and considerations for new developments and technologies.

4. Foreign and domestic affiliates If you are a financial entity, life insurance company or securities dealer, you need to identify the risks associated with

having foreign and domestic affiliates, if the affiliate carries out activities similar to those of a financial entity, life insurance company or securities dealer. An entity is your affiliate if one of you is wholly owned by the other, you are both wholly owned by the same entity, or your financial statements are consolidated. See Annex 2 — Table 4: Business-based examples of higher risk indicators and considerations for foreign and domestic affiliates.

5. Other relevant factors (if applicable): You need to identify other factors relevant to your business and that could have an impact on the risk of ML/TF such as:

- **legal**: related to domestic laws, regulations and potential threats
- **structural**: related to specific business models and processes

Scoring your business-based risk assessment Once you have identified and documented all the inherent risks to your business, you can assign a level or score to each risk using a scale or scoring methodology tailored to the size and type of your business. For example, very small businesses engaged in occasional, straightforward transactions may only require distinguishing between low and high-risk categories. FINTRAC expects larger businesses to establish more sophisticated risk scales or scoring methodologies, which could include additional risk categories.

By law, you must apply and document special measures for the high-risk elements of your business.Footnote 13 You must also be able to demonstrate to FINTRAC that you have put controls and measures in place to address these high-risk elements (for example, in your policies and procedures or training program), and that they are effective (this could be done through your internal or independent review). See Annex 3 — Table 6: Examples of risk segregation for a business-based risk assessment.

Additionally, you can use a likelihood and impact matrix tool similar to the one provided in Annex 4, to help you evaluate your business-based risk assessment.

Business-based risk assessment worksheet Using a business-based risk assessment worksheet could be an easy way to document the inherent risks related to your business. The worksheet below is given as an example. You can also develop your own worksheet or method to document the inherent risks related to your business.

Column A: List of factorsIdentify all the risk factors that apply to your business (including, products, services and delivery channels, geography, new developments and technologies, foreign and domestic affiliates and other relevant factors)	Column B: Risk ratingAssess each risk factor (for example, low, medium or high).	Column C:RationaleExplain why you assigned a particular risk rating to each risk factor.
- High turnover within your business of employees who deal directly with clients.	High-risk	New employees may have less knowledge of certain clients and less experience with ML/TF indicators.
- Proximity to border crossings	High-risk	Your business may be the first point of entry into the local financial system.

Relationship-based risk assessment Once you complete your business-based risk assessment, you can focus on the last element of your risk assessment, which consists of your clients and the business relationships you have with them.

When you enter into a business relationship with a client, you have to keep a record of the purpose and intended nature of the business relationship.Footnote 14 You also have to review this information on a periodic basis, which will help you determine the risk of ML/TF and understand the patterns and transactional activity of your clients.Footnote 15 It is possible that your business deals with clients outside of business relationships. The interactions with these clients may be sporadic (for example, few transactions over time that are under the identification threshold requirement). As such, there will not be a lot of information available to assess these clients. The risk assessment of such clients may focus on the transactional or contextual information at your disposal, rather than on a detailed client file.

If you do not have business relationships, it is not necessary for you to complete a relationship-based risk assessment worksheet for low and medium risk clients. However, if you have high-risk clients outside of business relationships, you should include them in a relationship-based risk assessment. For example, clients that were included in a suspicious transaction report (STR) you submitted to FINTRAC.

To conduct a relationship-based risk assessment, you need to identify the in-

herent risks of ML/TF for your clients. You can assess the ML/TF risks for individual clients or for groups of clients with similar characteristics. Your overall relationship-based risk assessment includes the risk posed by the following:

1. The combination of products, services and delivery channels your client uses;
2. The geographical location of the client and their transactions;
3. The new developments and technologies you make available to your clients; and
4. Client characteristics and patterns of activity or transactions.

1. Products, services and delivery channels In the relationship-based risk assessment, you are looking at the products, services and delivery channels that your clients are using and the impact they have on your clients' overall risk.

Product risks:

Products will have a higher inherent risk when there is client anonymity or when the source of funds is unknown.

Where possible, it is advisable that you complete a review of such products with the employees who handle them to ensure the completeness of the risk assessment.

Service risks:

You should include in your risk assessment services that have been identified as potentially posing a high-risk by government authorities or other credible sources.

For example, potentially higher risk services could include: international electronic funds transfers (EFTs), international correspondent banking services, international private banking services, services involving banknote and precious metal trading and delivery, or front money accounts for casinos.

Delivery channel risks:

You should consider delivery channels as part of your risk assessment, given the potential impact of new developments and technologies.

Delivery channels that allow for non-face-to-face transactions pose a higher inherent risk. Many delivery channels do not bring the client into direct face-to-face contact with you (for example, internet, telephone or new products such as virtual currency, chat applications, online document signing, etc.) and are accessible 24 hours a day, 7 days a week, from almost anywhere. This can be used to obscure the true identity of a client or beneficial owner, and therefore poses a higher risk. Although some delivery channels may have become the norm (for example, the use of internet for banking), you should nonetheless consider them

in combination with other factors that could make a specific element, client or group of clients high-risk.

Some products, services and delivery channels inherently pose a higher risk. See Annex 5 — Table 9: Relationship-based examples of higher risk indicators and considerations for products, services and delivery channels.

2. Geography In the business-based risk assessment, you have identified high-risk elements related to the geographical location of your business. In the relationship-based risk assessment, you will look at the geography of your clients or business relationships and its impact on their overall risk.

Your business faces increased ML/TF risks when you receive funds from or destined to high-risk jurisdictions, and when a client has a material connection to a high-risk country. You should assess the risks associated with your clients and business relationships such as residency in a high-risk jurisdiction or transactions with those jurisdictions.

See Annex 5 — Table 10: Relationship-based examples of higher risk indicators and considerations for geography.

3. Impacts of new developments and technologies In the business-based risk assessment, you assessed potential high-risk elements related to the introduction of new developments and technologies in your business model, prior to implementing them. In the relationship-based risk assessment, you will examine the potential impacts that new developments (putting in place a new service/activity/location) and technologies (introducing a new technology) could have on your clients, affiliates, and anyone with whom you have a business relationship.

New developments and technologies can increase risk, as they may provide another layer of anonymity. For example, your business faces an increased risk of ML/TF when funds come from or are destined to high-risk jurisdictions, and when the origin of the funds can not be determined or is unknown, etc.

See Annex 5 — Table 11: Relationship-based examples of higher risk indicators and considerations for new developments and technologies.

4. Client characteristics and patterns of activity or transactions At the beginning of a business relationship, and periodically throughout the relationship, you should consider the purpose and intended nature of the relationship. Doing so will help you understand your clients' activities and transaction patterns, in order to determine their level of ML/TF risk. Your policies and procedures must reflect this process.

To help you with the overall risk assessment of a client or group of clients, you should also consider known risk factors that can **increase** a client's overall ML/TF risk rating, such as:

- criminal history of the client in regards to a designated offence.
- unknown source of funds;
- beneficiary of the transaction is unknown;
- individual conducting the transaction in unknown;
- absence of detail in the transaction records;
- unusual speed, volume and frequency of transactions; or
- unexplained complexity of accounts or transactions.

Similarly, you should also look at factors that can **decrease** a client's ML/TF risk, such as:

- a low volume of activity;
- a low aggregate balance;
- low dollar value transactions; or
- household expense accounts or accounts for the investments of funds that are subject to a regulatory scheme (for example, Registered Retirement Savings Plan).

Some client characteristics or patterns of activity will pose an inherently higher risk of ML/TF. For examples of:

- higher risk client characteristics and patterns of activity, see Annex 5 — Table 12: Relationship-based examples of higher risk indicators and rationale for client characteristics and patterns of activity;
- client characteristics that can be considered higher risk, see FINTRAC's ML/TF indicators; and
- additional higher risk indicators and rationale, see Annex 5 — Table 13: Relationship-based examples of additional higher risk indicators and related considerations.

Scoring your relationship-based risk assessment You can assess the ML/TF risk for individual clients or for groups of clients. This assessment could take the form clusters (or groups) of clients with similar characteristics. For example, you can group together clients with similar incomes, occupations and portfolios, or those who conduct similar types of transactions. This approach can be especially practical for financial institutions.

It is important to remember that identifying one high-risk indicator for a client does not necessarily mean that the client poses a high-risk (with the exception of the three indicators highlighted in Table 12). Your relationship-based risk assessment model ultimately **draws together** the products, services and delivery channels used by your client, your client's geographical risk and your client's characteristics and patterns of activity. It is up to you to determine how to best assess the risk each client or group of clients poses.

Every high-risk client (or group of clients) will need to be subjected to prescribed special measures (see step 3). You will have to document these measures in your policies and procedures, and document how you apply them to

your high-risk clients.Footnote 16

You can use a Likelihood and impact matrix like the one in Annex 4 to help you evaluate your relationship-based risk.

Relationship-based risk assessment worksheet Using a relationship-based risk assessment worksheet could be an easy way to document the inherent risks related to your clients and your business relationships with them. The worksheet below is given an example. You can also develop your own worksheet or method to document the inherent risks related to your clients.

Column A Business relationships and/or high-risk clientsIdentify all your business relationships and/or high-risk clients (individually or as groups).	Column B: Risk ratingRate each business relationship and/or client (or group of clients) (for example, low, medium or high risk).	Column C: RationaleExplain why you assigned that particular rating to each business relationship and/or client (or group of clients).
- Group A / Client A	Low-risk	Known group or client conducting standard transactions in line with their profile.
- Group B / Client B	High-risk	Conducts several large cash transactions that seem to be beyond their means.

RBA cycle — Step 2: Setting your risk tolerance

Risk tolerance is an important component of effective risk management. Consider your risk tolerance before deciding how you will address risks. When considering threats, the concept of risk tolerance will allow you to determine the level of risk exposure that you consider tolerable.

To do so, you may want to consider the following types of risk which can affect your organization:

- regulatory risk;
- reputational risk;
- legal risk; or
- financial risk.

The PCMLTFA and associated Regulations state that reporting entities have obligations when they identify high-risk business activities and high-risk clients. Setting a high risk tolerance does not allow reporting entities to avoid these obligations.

To set your risk tolerance, some questions that you may want to answer are:

- Are you willing to accept regulatory, reputational, legal or financial risks?
- Which risks are you willing to accept after implementing mitigation measures?
- Which risks are you not willing to accept?

This should help you determine your overall risk tolerance (notwithstanding your mandatory obligations).

RBA cycle — Step 3: Creating risk-reduction measures and key controls

Risk mitigation is the implementation of controls to manage the ML/TF risks you have identified while conducting your risk assessment. It includes:

1. **In all situations,** your business should consider implementing internal controls that will help mitigate your overall risk.
2. **For your business-based risk assessment,** you will have to document and mitigate all the high-risk elements identified by your assessment with controls or measures.Footnote 17
3. **For all your clients and business relationships**, you will be required to:Footnote 18
    1. Conduct ongoing monitoring of all your business relationships; and
    2. Keep a record of the measures and information obtained through this monitoring.
4. **For your high-risk clients and business relationships**, you will be required to adopt the prescribed special measures, including:Footnote 19
    1. Conducting **enhanced** monitoring of these clients and business relationships.
    2. Taking enhanced measures to verify their identity and/or keep client information up to date.

Implementing risk mitigation measures will allow your business to stay within your risk tolerance. It is important to note that having a higher risk tolerance may lead to your business accepting higher risk situations and/or clients. If you accept to do business in higher risk situations and/or with higher risk clients, you should have stronger mitigation measures and controls in place to adequately address the risks.

For **detailed** information on risk mitigation measures, please consult FINTRAC's Compliance program requirements guidance.

RBA cycle — Step 4: Evaluating your residual risks

Your residual risks should be in line with your risk tolerance. It is important to note that no matter how robust your risk mitigation measures and risk management program is, your business will always have exposure to some residual ML/TF risk that you must manage. If your residual risk is greater than your

risk tolerance, or your measures and controls do not sufficiently mitigate high-risk situations or high-risk posed by clients, you should go back to step 3 and review the mitigation measures that were put in place.

If your business is willing to deal with high-risk situations and/or clients, FINTRAC expects that the mitigation measures or controls put in place (see step 3) will be commensurate with the level of risk, and that the residual risks will be reasonable and acceptable.

Types of residual risk:

- **Tolerated risks:** These are risks that you accept because there is no benefit in trying to reduce them. Tolerated risks may increase over time. For example, when you introduce a new product or a new threat appears.
- **Mitigated risks:** These are risks that you have reduced but not eliminated. In practice, the controls put in place may fail from time to time (for example, you do not report a transaction within the prescribed timeframe because your transaction review process has failed).

This is an example of a business further mitigating risk because over time their risks and clients have evolved:

Business A offers international EFTs as a service to its clients. Reporting systems are in place to capture transactions of $10,000 or more, and Business A has developed policies and procedures to properly verify identity for transactions of $1,000 or more. A reporting system is also in place to identify transactions that could be related to an ML/TF offence (for suspicious transaction reporting purposes).

Since Business A considers international EFTs to be a high-risk service, it added a mitigation measure to control the risk associated with the service. The staff (through the training program) is reminded regularly of the risks associated with international EFTs and are made aware of updates and changes to high-risk jurisdictions as indicated in government advisories. These measures were put in place by Business A years ago and are well understood and followed by the staff.

In this example, the mitigation measures put in place at the time were in line with the risk tolerance of Business A in regards to international EFTs. As such, the residual risk was tolerable for Business A.

However, as risks and/or clients changed over time, Business A now feels that the mitigation measures are no longer sufficient to meet its risk tolerance. In fact, Business A's risk tolerance is now lower than it used to be (that is, it is less inclined to take on high-risks). The residual risks from the previously established mitigation measures now exceed the new risk tolerance.

Business A will add new mitigation measures to realign the residual risk with its new tolerance level. Some examples of additional mitigation measures are:

- put a limit on specific transactions (for example, international EFTs to specific jurisdictions);
- require additional internal approvals for certain transactions; and/or
- monitor some transactions more frequently to help reduce the risk of structuring (for example, a $12,000 transaction that is split into two $6,000 transactions to avoid reporting).

RBA cycle — Step 5: Implementing your RBA

You will implement your RBA as part of your day-to-day activities.

You must document your risk assessment as part of your compliance program.Footnote 20 A detailed and well-documented compliance program shows your commitment to preventing, detecting and addressing your organization's ML/TF risks.

Risk and risk mitigation requires the leadership and engagement of your senior management (should this apply to your business). Senior management or your business owner is ultimately accountable, and may be responsible for making decisions related to policies, procedures and processes that mitigate and control ML/TF risks.

For more information, please consult FINTRAC's Compliance program requirements guidance.

RBA cycle — Step 6: Reviewing your RBA

You must institute and document a periodic review (minimum of every two years) of your compliance program, to test its effectiveness, which includes reviewing:Footnote 21

- your policies and procedures;
- your risk assessment related to ML/TF; and
- your training program (for employees and senior management).

If your business model changes and you offer new products or services, you should update your risk assessment along with your policies and procedures, mitigating measures and controls, as appropriate.

When reviewing your risk assessment to test its effectiveness, you must cover all components, including your policies and procedures on risk assessment, risk mitigation strategies and special measures which include your enhanced ongoing monitoring procedures. This will help you evaluate the need to modify existing policies and procedures or to implement new ones. Consequently, the completion of this step is crucial to the implementation of an effective RBA.

For more information, please consult FINTRAC's Compliance program requirements guidance.

Annex 1 — FINTRAC's RBA expectations

Overall expectations

There is no standard risk assessment methodology. In building a new or validating an existing risk assessment, you may find this guidance useful to inform your risk assessment. However, you should not limit yourself to the information provided in this guidance when developing your own RBA.

The expectations below are at a high level. FINTRAC's risk assessment expectations for each step of the RBA cycle are described further in this annex.

- Your risk assessment must be documented and should:
  - reflect the reality of your business;
  - include all prescribed elements (products, services and delivery channels, geography, new developments and technologies, affiliates if applicable, and any other factors relevant to your business); and
  - be shared with FINTRAC during an examination upon request.
- You need to tailor your risk assessment to your business size and type. For example, FINTRAC would expect a more detailed assessment from REs that conduct large volumes of transactions across various business lines and/or products. Additionally, FINTRAC would expect the overall business-based risk rating for larger REs to have separate risk ratings for different lines of business.
- You need to document all steps of your risk assessment, the process you followed, and the rationale that supports your risk assessment.
- During an examination, FINTRAC may review:
  - your risk assessment, your controls and mitigating measures (including your policies and procedures) to assess the overall effectiveness of your risk assessment;
  - your business relationships and evaluate whether they have been assessed based on the products, services, delivery channels, geographical risk, impact of new developments and technologies and other characteristics or patterns of activities;
  - your high-risk client files to ensure that the prescribed special measures have been applied;
  - your records to assess whether monitoring and reporting are done in accordance with the PCMLTFA and associated Regulations and with your policies and procedures; and
  - whether your prescribed review (to be conducted at least once every two years) appropriately assessed the effectiveness of your business and relationship-based risk assessment.

Expectations for Step 1 — Identification of your inherent risks

FINTRAC expects that:

- You have considered and assessed your business risks (including, prod-

ucts, services and delivery channels, geography, new developments and technologies, affiliates if applicable, and any other factors relevant to your business) and you are able to provide a rationale for your assessment. For every element that you assess as posing a high-risk, you will need to document the controls and mitigation measures you are taking. You need to be able to show that these controls and measures have been implemented.

- You have considered and assessed your clients and business relationships based on the products, services and delivery channels they use, on their geography, and on their characteristics and patterns of activity. You can do this by:
  - Demonstrating that you have assessed the risks posed by each client you have a business relationship with; or
  - Assessing groups of clients or of business relationships that share similar characteristics, as long as you can demonstrate that the groupings are logical and specific enough to reflect the reality of your business.
- You can provide documented information that demonstrates that you have considered high-risk indicators in your assessment (such as those included in this guidance where applicable).
- In situations where high-risk indicators are not considered (for example, FINTRAC considers a specific element to pose a high-risk but you decide that the element poses a lower level of risk), you must be able to provide a reasonable rationale.
- For every high-risk relationship, you have put in place the prescribed special measures and document these measures in your policies and procedures.
- If you use a checklist for your risk assessment, you must be able to provide a documented analysis of the risk that draws conclusions on your business's vulnerabilities to ML/TF and the threats it faces, including the required elements (referred to above).
- If your business is using a service provider to perform the risk assessment, you are nonetheless ultimately responsible to ensure that the for the risk assessment obligation is met correctly.

Expectations for Step 2 — Set your risk tolerance

FINTRAC expects that:

- You take time to establish your risk tolerance, as it is an important component of effectively assessing and managing your risks.
- Your risk tolerance will have a direct impact on creating risk-reduction measures and controls, on your policies and procedures, and on training (step 3).

Setting your risk tolerance includes obtaining approval from senior management (should that be a part of your business structure).

Expectations for Step 3 — Create risk-reduction measures and key controls

FINTRAC expects that:

- You keep the client identification and beneficial ownership information of your business relationships up to date.Footnote 22
- You establish and conduct the appropriate level of ongoing monitoring for your business relationships (taking enhanced measures for high-risk clients).Footnote 23
- You implement mitigation measures for situations where the risk of ML/TF is high (for your business-based risks and relationship-based risks). These written mitigation strategies must be included in your policies and procedures.

Apply your controls and procedures consistently. FINTRAC may assess them through transaction testing.

Expectations for Step 4 — Evaluate your residual risks

FINTRAC expects that:

- You take the time to evaluate your level of residual risk.
- You confirm that the level of residual risk is aligned with your risk tolerance (as described in step 2).

Expectations for Step 5 — Implement your RBA

FINTRAC expects that:

- Your RBA process is documented, and includes your ongoing monitoring procedures (including their frequency) and the measures and controls put in place to mitigate the high-risks identified in step 1.
- You apply your RBA as described in your documentation.
- You keep the client and beneficial ownership information of your business relationships up to date.Footnote 24
- You conduct ongoing monitoring of all your business relationships.Footnote 25
- You apply the appropriate prescribed special measures to your high-risk clients and business relationships.Footnote 26
- You involve the persons responsible for compliance when dealing with high-risk situations (for example, when dealing with foreign politically exposed persons (PEPs), obtain senior management approval to keep accounts open after a determination has been made).

Expectations for Step 6 — Review your RBA

FINTRAC expects that:

- You conduct a review at least every two years, or when there are changes to your business model, when you acquire a new portfolio, etc.Footnote 27
- This prescribed review will test the effectiveness of your entire compliance program, including your compliance policies and procedures, your risk assessment of ML/TF risks and your ongoing training program.Footnote 28
- You document the review and report it to senior management within 30 days.Footnote 29
- You document the results of the review, along with corrective measures and follow-up actions.Footnote 30

Annex 2 — Examples of higher risk indicators and considerations for your business-based risk assessment

Examples of higher risk indicators	Considerations
Higher risk products and services, such as:- EFTs, - electronic cash (for example, stored value cards and payroll cards) - letters of credit- bank drafts- front money accounts- products offered through the use of intermediaries or agents- private banking - mobile applications	Legitimate products and services can be used to mask the illegitimate origins of funds, to move funds to finance terrorist acts or to hide the true identity of the owner or beneficiary of the product or service. You should assess the market for your products and services (for example, corporations, individuals, working professionals, wholesale or retail etc.), as this may have an impact on the risk.Do the products or services you provide allow your clients to conduct business or transactions with higher risk business segments? Could your clients use the products or services on behalf of third parties? Products and services offered that are based on new developments and technologies such as electronic wallets, mobile payments, or virtual currencies, may be considered higher risk as they can transmit funds quickly and anonymously.

Examples of higher risk indicators	Considerations
Delivery channels, such as transactions for which an individual is **not physically present**, including- agent network - online trading	Your delivery channels may have a higher inherent risk if you offer non face-to-face transactions, use agents, or if clients can initiate a business relationship online. This is especially true if you rely on an agent (that may or may not be covered by the PCMLTFA) to verify the identity of your clients.For the purpose of the PCMLTFA, REs are accountable for the activities conducted by their agents.In addition, new delivery channels (for example, products or services such as virtual currency) may pose inherently higher ML/TF risks due to the anonymous nature of transactions when conducted remotely.

Table 1: Business-based examples of higher risk indicators and considerations for products, services and delivery channels

Examples of higher risk indicators	Considerations
Border-crossings:- air (for example, airports)- water (for example, ports, marinas)- land (for example, land border-crossings)- rail (for example, passenger and cargo)	If your business is near a border-crossing, you may have a higher inherent risk because your business may be the first point of entry into the Canadian financial system.This does not mean that you should assess all activities and clients as posing a high-risk if your business is located near a border-crossing or major airport. FINTRAC is simply highlighting that such businesses may want to pay closer attention to the fact that their geographical location may impact their business. For example, this could be done through training so that staff better understand the placement stage of ML and its potential impacts.

Examples of higher risk indicators	Considerations
Geographical location and demographics:- large city- rural area	Your geographical location may also affect your overall business risks. For example, a rural area where you know your clients could present a lesser risk compared to a large city where new clients and anonymity are more likely. However, the known presence of organized crime would obviously have the reverse effect. Some provincial governments have interactive maps on crime by regions, which may inform your risk assessment. Other websites provide good information on crime in Canada, including statistics and trends by province. For example, crimes, by type of violation, and by province and territory:http://www.statcan.gc.ca/tables-tableaux/sum-som/l01/cst01/legal50b-eng.htm.

Examples of higher risk indicators	Considerations
Your business is located in an area known for having a high crime rate	High crime rate areas should be indicated in the overall assessment of your business as they may present higher ML/TF risks.You do not need to consider every client from a higher crime area as posing a high-risk. However, you should be aware of how these areas can affect client activities. Searching online for crime related statistics in your city or area should result insources you can consult (such as municipal police departments or other databases). For example, the following websites provide information on crime in cities or neighborhoods: - Vancouver: http://vancouver.ca/police/organization/planning-research-audit/neighbourhood-statistics.html- Edmonton: http://crimemapping.edmontonpolice.ca/- Calgary: http://www.calgary.ca/cps/Pages/Statistics/Calgary-Police-statistical-reports.aspx#- Winnipeg: https://winnipeg.ca/police/crimestat/viewMap.aspx- Toronto: http://www.torontopolice.on.ca/statistics/stats.php- Ottawa: https://www.ottawapolice.ca/en/crime/crime-stats.aspx- Montreal: https://ville.montreal.qc.ca/vuesurlasecuritepublique/ (in French only) - Halifax: https://www.halifax.ca/fire-police/police/crime-mappingPlease note that statistics such as those found under the links above are not necessarily linked to ML/TF offences. They provide a general idea of where crime occurs in a given city.

Examples of higher risk indicators	Considerations
Events and patterns	Depending on your clientele, are there events or patterns (either domestic or international) that could affect your business? For example, you may be dealing with clients that have a connection to high-risk jurisdictions or with jurisdictions that are dealing with a specific event (such as terrorism, war, etc.). You do not need to classify all activities and clients as posing a high-risk in relation to an event, conflict or high-risk jurisdiction. However, you should be aware of these circumstances in order to determine whether a transaction becomes unusual or suspicious.

Examples of higher risk indicators	Considerations
Connection to high-risk countries:- Special Economic Measures Act (SEMA)- FATF list of High-Risk Countries and Non-Cooperative Jurisdictions- UN Security Council Resolutions- Freezing Assets of Corrupt Foreign Officials Act (FACFOA) sanctions	International conventions and standards may affect mitigation measures aimed at the detection and deterrence of ML/TF. You should identify certain countries as posing a high-risk for ML/TF based on (among other things) their level of corruption, the prevalence of crime in their region, the weaknesses of their ML/TF control regime, or the fact that they are listed in the advisories of competent authorities such as the FATF or FINTRAC. If you and/or your clients have no connection to these countries, the risk will likely be low or non-existent.If you transfer funds to or receive funds from a country subject to economic sanctions, embargoes or other measures, you should consider that country as high-risk. For example, you should be aware of: - Canadian Economic Sanctions: https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/index.aspx?lang=eng- High-Risk and Non-Cooperative Jurisdictions: http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/- FINTRAC Advisories: https://fintrac-canafe.canada.ca/new-neuf/1-eng- Security Council Resolutions: https://www.un.org/securitycouncil/content/resolutions- Freezing Assets of Corrupt Foreign Officials Act sanctions: https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/current-actuelles.aspx?lang=eng

Table 2: Business-based examples of higher risk indicators and considerations

for geography

Examples of higher risk indicators	Considerations
Use of technology, such as:- Payment methods: - E-wallets in fiat currencies (CAD, USD, etc.) - E-wallets in virtual currencies - pre-paid cards - internet payment services - mobile payments - money transfers between individuals over mobile devices and the Internet- Methods of communication or identification: - phone - email - chat applications - electronic information exchange - document signing on a cloud server such as DocuSign	Your overall inherent risks may be higher if your business adopts new technologies or operates in an environment subject to frequent technological change. New technologies may include systems or software used in your organizations ML/TF mitigation strategy such as a transaction monitoring system or a client onboarding or identification tool.The implementation of new technologies such as mobile payment services could subject your business to a wide range of vulnerabilities that can be exploited for ML. For example, the use of new technologies can result in less face-to-face interaction with customers, allowing more anonymity and possibly increasing ML/TF risks. Therefore, when you implement new technology in your business, it is important that you assess the associated ML/TF risks and document and implement appropriate controls to mitigate those risks. **Payment methods**The payment method examples listed in the Indicators column can be used to transfer funds faster and anonymously, which can increase ML/TF risks.If your business offers such products, services and delivery channels, you must assess them for ML/TF risks to your business.**Methods of communication or identification**Your business may communicate with clients through means other than the telephone and email or your clients may use new ways to communicate with you or identify themselves to you. Communications means are evolving continually and can affect your overall inherent risks.

Examples of higher risk indicators	Considerations
New developments	Consider acquisitions, changes to your business model, or business restructuring.

Table 3: Business-based examples of higher risk indicators and considerations for new developments and technologies

Examples of higher risk indicators	Considerations
Business model of foreign affiliate: - operational structure- reputational risk	Review the business model, size, number of employees and the products and services of your affiliates to determine whether they represent a risk that can affect your business. For example: - If a business has hundreds of branches and thousands of employees, it poses different risks than a business with a single location and two employees.- If the media negatively mentions one of your affiliates, your reputation could also be affected given the connection between you and that affiliate.

Table 4: Business-based examples of higher risk indicators and considerations for foreign and domestic affiliates

Examples of higher risk indicators	Considerations
- Special Economic Measures Act (SEMA)- ministerial directives- regulators- national risk assessment	Restrictions such as economic sanctions can impact your business by:- prohibiting trade and other economic activity with a foreign market;- restricting financial transactions such as foreign investments or acquisitions; or- leading to the seizure of property situated in Canada. These restrictions may apply to dealings with entire countries, regions, non-state actors (such as terrorist organizations), or designated persons from a target country.As part of your risk assessment, you must also take into consideration ministerial directives.Your sector's regulator may also impose additional measures (for example, provincial, prudential, etc.).The national risk assessment assesses the ML/TF risks in Canada, which may help you identify potential links to your own business activities.
Trends, typologies and potential threats of ML/TF:- ML/TF methods used in specific sectors- ML/TF actors including organized crime groups, terrorist organizations, facilitators, etc.- corruption and other crimes	Trends and typologies for your respective activity sector may include specific elements of risks that your business should consider. For example:- FATF Methods and Trends (not available for all activity sectors): http://www.fatf-gafi.org/topics/methodsandtrends/. - Public Safety Canada — Organized Crime: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cmbtng-rgnzd-crm/index-en.aspx- Transparency International (rank by country): https://www.transparency.org/en/countries/canadaNot all elements listed in these trends and typologies will affect you, but you should be aware of the high-risk indicators that may have an impact on your business.

Examples of higher risk indicators	Considerations
Business model: - operational structure- third party and/or service providers	To determine if risks exist in relation to this element, you need to consider your business model, the size of your business, and the number of branches and employees. For example: - A business with hundreds of branches and thousands of employees will present different risks than a business that has one location and two employees.- A business with a high employee turnover. These examples highlight the fact that your risk assessment should be related to other compliance program elements, such as training. Training should give employees an understanding of the reporting, client identification, and record keeping requirements, and an understanding of the penalties for not meeting those requirements. If you have numerous branches or a high employee turnover, your training program should address these risks.It is also important to remember that although the use of a third party or service provider can be a good business practice, your business is ultimately responsible for complying with your obligations under the PCMLTFA and associated Regulations. You will want to ensure that you fully understand how your third party or service provider is functioning.

Table 5: Business-based examples of higher risk indicators and considerations for other relevant factors

Annex 3 — Examples of risk segregation for your business-based risk assessment

The table below lists examples of risk factors you could encounter **as part of your business-based risk assessment**. It also provides a rationale on how you could differentiate between risk ratings.

Please note that:

1. The PCMLTFA and associated Regulations do not require you to use a low, medium and high scale. You could use low and high-risk categories only. You must establish a risk scale and you must tailor the risk scale to your business's size and type.
2. Utilizing a table similar to this one **is not** in itself a risk assessment, as it does not meet the requirement as stated in the Regulations. However, the table below is an example of a business-based risk assessment. It does not consider your clients or business relationships.

This list includes **inherent risks** that have not been mitigated yet. By law, controls or mitigation measures are required for all high-risk factors.

Factors	Low	Medium	High
Products & services — Electronic transactions	No electronic transaction services	You have some electronic transaction services and offer limited products and services	You offer a wide array of electronic transactions services
Products & services — Currency transactions	Few or no large transactions	Medium volume of large transactions	Significant volume of large or structured transactions
Products & services — EFTs	Limited number of funds and transfers of low value for clients and non-clientsLimited third party transactions and no foreign funds transfers	Regular funds transfers and transfers of medium valueFew international funds transfers from personal or business accounts with typically low-risk countries	Frequent funds transfers and transfers of high value from personal or business accounts, to or from high-risk jurisdictions and financial secrecy jurisdictions

Factors	Low	Medium	High
Products & services (business model) — International exposure	Few international accounts or very low volume of transactions in international accounts	Some international accounts with unexplained transactions	High number of international accounts with unexplained transactions
Geography (location) — Prevalence of crime	All locations are in an area known to have a low crime rate	One or a few locations are in an area known to have an average crime rate	One or a few locations are in an area known to have a high crime rate and/or criminal organization(s)
Technology	No new technologies are used to conduct the business in terms of products and services to clientsNo new technologies are used to contact clients	Certain areas of the business use new technologies to contact clients but products, services and payment methods do not use new technologies	The majority of products, services, delivery channels, payment methods and client contact methods use new technologies.

Table 6: Examples of risk segregation for a business-based risk assessment

Note: Some of the descriptors in the above table are vague (such as "some", "significant", etc.). A table such as this one needs to be customized to the reality of your business. For example, if FINTRAC states that it considers a "significant volume of transactions with high-risk countries" as posing a high-risk, this could mean that a business could compare the transactions to high-risk countries to the overall quantity of transactions conducted by their business. If a business conducting 600 transactions with high-risk-countries out of 1,000 monthly transactions it has a "significant" inherent risk. Qualifiers depend on the specifics of your own business.

Annex 4 — Likelihood and impact matrix

You can use the likelihood and impact matrix described below for your business and client risks. It can help you determine the level of effort or monitoring required for inherent risks. You use the matrix or develop your own to better reflect the realities of your business.

Likelihood is the chance of an ML/TF risk is present. What is the likelihood that the identified risks are actually present? The "likelihood" is the level of risk you have identified as part of your business-based risk assessment and/or your relationship-based risk assessment (for example, a client assessed as posing a medium risk). You can use a scale similar to this one:

Rating	Likelihood of ML/TF risk
High	High probability that the risk is present
Medium	Reasonable probability that the risk is present
Low	Unlikely that the risk is present

Table 7: Rating and likelihood of the ML/TF risk

Impact isthe damage incurred if ML/TF occurs. Depending on business circumstances, the impact could be a financial loss, or a regulatory, legal, reputational or other impact. To help you determine the impact of your ML/TF risks, you can use a scale similar to this one:

Rating	Likelihood of ML/TF risk
High	The risk has severe consequences
Medium	The risk has moderate consequences
Low	The risk has minor or no consequences

Table 8: Rating and impact of the ML/TF risk

You can use the matrix to help you decide which actions to take considering the overall risk. Each box in the matrix shows the level of resources required for:

- action (the need to respond to the risk)
- effort (level of effort required to mitigate the risk)
- monitoring (level of monitoring required)

Diagram 4: Likelihood and impact matrix

!Likelihood and impact matrix.jpg)

View Text Equivelant

The following graphic is called the likelihood and impact matrix. It is made up of 2 axes. The vertical axis is the likelihood of ML/TF risk while the horizontal axis is the impact of ML/TF. Each axis contains 3 levels of risk – low, medium and high - for a total of 9 boxes within the matrix.

On the impact axis, the left side represents the low risk category, the middle being medium risk and the right side representing high risk. On the vertical

axis, the bottom represents the low risk category, the middle being medium risk and the top representing high risk.

The 9 boxes within the matrix represent various combinations of risk. In addition, each box contains a level of resource required for: action (i.e. the need to respond to risk), effort (i.e. level of effort required to mitigate the risk) and monitoring (i.e. level of monitoring required). The level of resource is being represented by level 0, being the lowest, up to level 3 being the highest.

1. The box on the lower left corner (low impact and low likelihood) represents the lowest overall risk. Action is at level 0 while effort and monitoring are at level 1.
2. The box immediately to its right (medium impact and low likelihood) is also considered to be in the lower overall risk. Action is at level 0 while effort and monitoring are at level 1.
3. The box on the bottom right corner (high impact and low likelihood) represents a medium / low overall risk. Action and effort are at level 1 while monitoring is at level 2.
4. The box located at low impact and medium likelihood is considered to be in the lower overall risk. Action is at level 0 while effort and monitoring are at level 1.
5. The box immediately to its right, at the centre of the matrix (medium impact and medium likelihood), is considered to be medium overall risk. Action, effort and monitoring are at level 2.
6. The box located at high impact and medium likelihood is considered to be in the higher overall risk. Action, effort and monitoring are at level 3.
7. The box on the top left corner (low impact and high likelihood) represents a medium / low overall risk. Action and effort are at level 1 while monitoring is at level 2.
8. The box immediately to its right (medium impact and high likelihood), is considered to be in the higher overall risk. Action, effort and monitoring are at level 3.
9. The box on the top right corner (high impact and high likelihood) represents the highest overall risk. Action, effort and monitoring are at level 3.

How to read the matrix

Box 6 may not require any response, effort or monitoring because you consider both the likelihood and impact to be low.

Box 3 will require you to allocate resources for action, effort and monitoring. You will want to monitor all business risks and business relationships that are in box 3 to ensure that the risks identified do not move into the red categories (boxes 1 and 2).

In Box 1, you have identified the risks to be highly likely to occur and to have a severe impact on your business. Anything in this box (for example, business

risks, business relationship, etc.) would require the most resources for action, effort, and monitoring.

Examples

For the example below, you should consider all risk factors or clients as:

- low-risk if situated in boxes 5–6;
- medium-risk if situated in boxes 3–4; and
- high-risk if situated in boxes 1–2.

Example 1 You complete the risk assessment of clients A and B and determine that they both have the same likelihood of ML/TF risk: medium.

Taking a closer look at their accounts, you realize that both have EFTs on file (product/service with a high inherent risk). However, client A has not conducted an EFT in months and you know that the EFTs were to family members abroad. However, client B regularly conducts EFTs but you do not know a lot about the recipients or the reasons for the EFTs.

As such, you could assess the impact of the ML/TF risk to be greater with client B than with client A. You could decide to leave client A in the medium impact category (placing the client in box 3) and to move client B to the high-impact category (placing the client in box 2). You should document your decision and rationale.

In this example, you would need to implement mitigation measures for client B, who is now a high-risk client.

Example 2 After completing the risk assessment of clients A and B, you determine that they have the same likelihood of ML/TF risk: high.

Taking a closer look at the volume of transactions both clients conduct, you see that client A conducts 1 transaction per week on average; whereas client B conducts several transactions every day. In this example, the impact not submitting suspicious transaction reports would be greater with client B because of the volume of transactions.

You could decide to place client A in a lower category (placing the client in box 4) while client B could remain in a higher category (placing the client in box 1 or 2). You should document your decision and rationale

In this example, you would implement mitigation measures for client B, who is now a high-risk client.

Example 3 In this scenario, an RE applies the risk matrix to risk elements identified in their risk assessment:

Risk factor	Likelihood	Impact	Overall	Mitigation measures
Clients always use cash as method of payment	High	Medium	**High (box 2)**	- Perform enhanced ongoing monitoring of transactions or business relationships.- Obtain additional information beyond the minimum requirements about the intended nature and purpose of the business relationship, including the type of business activity.

Risk factor	Likelihood	Impact	Overall	Mitigation measures
Clients frequently use EFTs for no apparent reason	Medium	High	**High (box 2)**	- Set transaction limits for high-risk products such as EFTs to high-risk jurisdictions.- Obtain additional information beyond the minimum requirements for the intended nature and purpose of the business relationship, including type of business activity.- Implement a process to end existing high-risk relationships that exceed your risk tolerance level.

Diagram 5 — Example of a risk matrix

Annex 5 — Examples of higher risk indicators and considerations for your relationship-based risk assessment

Examples of higher risk indicators	Considerations
Your clients use electronic funds payment services such as: - EFTs - electronic cash	EFTs can be done in a non-face-to-face environment. Additionally, transmitting large amounts of funds outside of Canada or into Canada can disguise the origin of the funds.**Electronic cash** is a higher risk service because it can allow unidentified parties to conduct transactions.
Your clients use products such as bank drafts and letters of credit.	**Bank drafts** can move large amounts of funds in bearer form without the bulkiness of cash. They are much like cash in the sense that the holder of the draft is the owner of the money. For example, a 100,000 dollar bank draft (showing a financial institution as the payee) and can be passed from one person to another, effectively blurring the money trail.You can mitigate the inherent risk of this product when it is issued as payable only to specific payees and when the information about the draft's originator are included (name, account number, etc.). **Letters of credit** are essentially a guarantee from a bank that a seller will receive payment for goods. While guaranteed by a bank, letters of credit have a higher inherent ML/TF risk as they can be used in trade-based transactions to increase the appearance of legitimacy and reduce the risk of detection. Money launderers using trade-based transactions (for example, seller or importer) may also use under or over valuation schemes, which will allow them to move money under the veil of legitimacy.There is also higher risk when letters of credit are not used in a way consistent with the usual pattern of activity of the client.

Examples of higher risk indicators	Considerations
Your clients use some products and services that you offer through non-face-to-face channels or use intermediaries, agents or introducers (refer clients or businesses to you for specific products or services).	Non-face-to-face transactions can make it more difficult to verify the identity of your clients.Using intermediaries or agents may increase your inherent risks, because intermediaries or agents may lack adequate supervision if they are not subject to anti-money laundering and anti-terrorist financing (AML/ATF) laws or measures. It is important to note that under the PCMLTFA, you are accountable for the activities conducted by all your agents. As a result, you need to ensure that they meet all compliance obligations on an ongoing basis. Furthermore, you should have due diligence processes in place (such as background checks and ongoing monitoring) to lessen the risk of your agent network being used for ML/TF purposes.

Table 9: Relationship-based examples of higher risk indicators and considerations for products, service and delivery channels

Examples of higher risk indicators	Considerations
Your client's proximity to a branch or location	A client that conducts business or transactions away from their home branch or address without reasonable explanation. For example, one of your clients conducts transactions at different branches across a broad geographical area over one day and this does not appear to be practical.
Your client is a non-resident	Identifying non-resident clients may prove to be more difficult if they are not present and as such, could raise the inherent level of risk.

Examples of higher risk indicators	Considerations
Your client has offshore business activities or interests	Is there a legitimate reason for your client to have offshore interests? Offshore activities may be used by a person to add a layer of complexity to transactions, thus raising the overall risk of ML/TF.
Your client's connection to high-risk countries	Take your client's connection to high-risk countries into account as some countries have weaker or inadequate AML/ATF standards, insufficient regulatory supervision or present a greater risk for crime, corruption or TF.

Table 10: Relationship-based examples of higher risk indicators and considerations for geography

Examples of higher risk indicators	Considerations
Changing payment methods	The variety of payment methods made possible by advancements in technology is a potential risk for ML/TF. Many countries and companies have moved to a "cashless world" approach. As a result, clients are using alternative payment methods such as e-wallets. It is important to analyze the risk associated with these payment methods (for example, anonymity, borderless transactions, speed of the transactions, vulnerabilities in terms of know your client requirements) to determine how the technology used by your clients may increase their risk level.
A new service or activity that offers transaction anonymity	It is important to assess the impact that a new service or activity can have on the behaviour of your clients who may use it to distance themselves from a transaction.

Table 11: Relationship-based examples of higher risk indicators and considera-

tions for new developments and technologies

Examples of higher risk indicators	Rationale
Your client is in possession or control of property that you **know/believe** is owned or controlled by or on behalf of a terrorist or a terrorist group	You are required to send a terrorist property report to FINTRAC if you have property in your possession or control that you **know/believe** is owned or controlled by or on behalf of a terrorist or a terrorist group. This includes information about transactions or proposed transactions relating to that property. Once you file a terrorist property report, the client automatically becomes high-risk.
Your client is a foreign PEP	A foreign PEP is an individual who is or has been entrusted with a prominent function. Because of their position and the influence they may hold, a foreign PEP, their family members and their close associates are vulnerable to ML/TF and other offences such as corruption. As a business, you **must** consider a foreign PEP, their family members and their close associates as a high-risk client.

Examples of higher risk indicators	Rationale
The entity has a complex structure that conceals the identity of beneficial owners	When you cannot obtain or confirm the ownership and control information of a corporation or an entity, you are required to verify the identity of the most senior managing officer of the entity and treat the entity as high-risk, and apply the prescribed special measures as stated in the Proceeds of Crime Money Laundering and Terrorist Financing Regulations.For more information, please consult FINTRAC's Beneficial ownership requirements guidance.It is important to note that when you do have the information on beneficial ownership, there may be other information or indicators that would make this relationship pose a higher risk.

Table 12: Relationship-based examples of higher risk indicators and rationale for client characteristics and patterns of activity

Examples of higher risk indicators	Considerations
STR was previously filed or considered	Suspicious transactions (or attempted transactions) are financial transactions for which you have reasonable grounds to suspect they are related to the commission or attempted commission of an **ML/TF offence**. For more information about STRs and ML/TF indicators, see FINTRAC's STR guidance.Clients that are the conductors of suspicious transactions that have been reported should be assessed as posing a higher risk.
Transactions involving third parties	Transactions involving third parties may indicate high-risk when the link between the third party and the client is not obvious.

Examples of higher risk indicators	Considerations
The account activity does not match the client profile	Account activity that does not match the client profile may indicate a higher risk of ML/TF.You may face situations where you have submitted several large cash transaction reports to FINTRAC about a client with an occupation that does not match this type of activity (for example, student, unemployed, etc.).
Your client's business generates cash for transactions not normally cash intensive	The fact that there is no legitimate reason for the business to generate cash represents a higher risk of ML/TF.
Your client's business is a cash-intensive business (such as a bar, a club, etc.)	Certain types of business, especially those that are cash-intensive may have a higher inherent risk for ML/TF because legitimate money can be co-mingled with illegitimate money. For example, clients that own white label ATMs.
Your client offers online gambling	Industry intelligence, including reports from the Royal Canadian Mounted Police, indicates that due to the nature of the business, the gambling sector is susceptible to ML activity. Additionally, the FATF has indicated that internet payment systems are an emerging risk in the gambling industry. Internet payment systems are used to conduct transactions related to online gambling, these two factors make the online gambling industry inherently higher risk.As well, higher inherent risk may exist if the online gambling activities are not managed by provincial lottery and gaming corporations.

Examples of higher risk indicators	Considerations
Your client's business structure (or transactions) seems unusually or unnecessarily complex	An unnecessarily complex business structure or complex client transactions (compared to what you normally see in a similar circumstance) may indicate that the client is trying to hide transactions or suspicious activities.
Your client is a financial institution with which you have a correspondent banking relationship; **or**Your client is a correspondent bank that has been subject to sanctions.	Some countries have weaker or inadequate AML/ATF standards, insufficient regulatory supervision or simply present a greater risk for crime, corruption or TF. Additionally, the nature of the businesses that your correspondent bank client engages in and the type of markets it serves may present greater risks. The fact that your client has been subject to sanctions should raise the risk level and you should put appropriate measures in place to monitor the account.
Your client is an RE under the PCMLTFA that is not otherwise regulated	Some reporting entities that are not federally or provincially regulated (other than under the PCMLTFA) may present higher risks of ML/TF. In addition, some may have cash intensive businesses that can also increase the overall risks of ML/TF.
Your client is an intermediary or a gatekeeper (such as a lawyer or accountant) holding accounts for others unknown to you	Accountants, lawyers and other professionals sometimes hold co-mingled funds accounts for which beneficial ownership may be difficult to verify. This does not mean that all clients with these occupations are high-risk. You need to be aware of the risks that exist for these occupations and determine if the activities of the clients are in line with what you would expect and with the intended purpose of the account (for example a personal, business or trust account).

Examples of higher risk indicators	Considerations
Your client is an unregistered charity	Individuals and organizations can misuse charities in ML schemes or to finance or support terrorist activity. It is important to be aware of the risks in relation to charities and to apply due diligence by confirming if a charity is registered with the Canada Revenue Agency
Domestic PEPs and heads of international organizations (HIOs)	Corruption is the misuse of public power for private benefit. Internationally, as well as in Canada, it is important to understand that the possibility for corruption exists and that domestic PEPs or HIOs can be vulnerable to carrying out or being used for ML/TF offences.Once you have determined that a person is a domestic PEP, a HIO or a family member or close associate of them, you must determine if the person poses a higher risk for committing an ML/TF offence. If you assess the risk to be high, then you must treat the person as a high-risk client.For more information, please consult the PEP and HIO guidance for your sector (if applicable).

Table 13: Relationship-based examples of additional higher risk indicators and related considerations

Compliance program requirements : FINTRAC's compliance guidance

From: Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)

This guidance explains the compliance program requirements under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (the Act) and associated Regulations that **apply to all reporting entities**.

1. What is a compliance program and what are its requirements

A compliance program is established and implemented by a reporting entity that is intended to ensure its compliance with the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (the Act) and associated Regulations. A compliance program forms the basis for meeting all of your reporting, record keeping, client identification and other know-your-client requirements under the Act and associated Regulations. All reporting entities must establish and implement a compliance program.

Specifically, all reporting entities must implement the following elements of a compliance program:

- appoint a compliance officer who is responsible for implementing the program
- develop and apply written compliance policies and procedures that are kept up to date and, in the case of an entity, are approved by a senior officer
- conduct a risk assessment of your business to assess and document the risk of a money laundering or terrorist activity financing offence occurring in the course of your activities
- develop and maintain a written, ongoing compliance training program for your employees, agents or mandataries, or other authorized persons
- institute and document a plan for the ongoing compliance training program and deliver the training (training plan)
- institute and document a plan for a review of the compliance program for the purpose of testing its effectiveness, and carry out this review every two years at a minimum (two-year effectiveness review)

2. Who can be a compliance officer and what are their responsibilities

Depending on the size of your business, you could be the appointed compliance officer, or it could be another individual, such as:

- a senior manager, the owner or the operator of your small business, or
- someone from a senior level who has direct access to senior management and the board of directors of your large business

If you are a person rather than an entity, such as a sole proprietor, you can appoint yourself as the compliance officer, or you may choose to appoint someone else to help you implement the compliance program.

As a best practice, the appointed compliance officer of a larger business should not be directly involved in the receipt, transfer or payment of funds. The appointed compliance officer should also have independent oversight and be able to communicate directly with those parties who make decisions about the business

such as senior management or the board of directors.

Appointing someone to be your compliance officer alone does not fulfil your compliance program requirements. The appointed compliance officer is responsible for implementing all elements of a compliance program. Therefore, a compliance officer needs to:

- have the necessary authority and access to resources in order to implement an effective compliance program and make any desired changes
- have knowledge of your business's functions and structure
- have knowledge of your business sector's money laundering, terrorist activity financing and sanctions evasion risks and vulnerabilities as well as money laundering, terrorist activity financing and sanctions evasion trends and typologies
- understand your business sector's requirements under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (the Act) and associated Regulations

A compliance officer may delegate certain duties to other employees. For example, the compliance officer of a large business may delegate responsibility to an individual in another office or branch. However, the compliance officer remains responsible for the implementation of the compliance program.

While the compliance officer is appointed, it is the reporting entity's responsibility to meet its compliance program requirements under the Act and associated Regulations.

3. Compliance policies and procedures requirements

Your compliance policies and procedures must be:

- written and should be in a form or format that is accessible to its intended audience
- kept up to date (including changes to legislation or your internal processes, as well as any other changes that would require an update)
- approved by a senior officer, if you are an entity

Your policies and procedures should be made available to all those authorized to act on your behalf, including employees, agents and any others that deal with clients, transactions, or other activities.

Your compliance policies and procedures should cover at minimum the following requirements as applicable to you as a reporting entity:

- **compliance program**: this includes your requirements to have an appointed compliance officer, a risk assessment, an ongoing compliance training program and plan, and a two-year effectiveness review and plan, which consists of a review of your policies and procedures, risk assessment, and ongoing training program and plan

- **know your client**: this includes your requirements for verifying client identity, politically exposed persons, heads of international organizations, their family members and close associates, beneficial ownership, and third party determination
- **business relationship and ongoing monitoring**
- **record keeping**
- **Transaction reporting**
- **travel rule** requirements: this includes your requirement to develop and apply written risk-based policies and procedures to help determine whether you should suspend or reject an electronic funds transfer or virtual currency transfer that you receive, and any other follow-up measures, if the transfer does not include the required travel rule information and you are unable to obtain this information through your reasonable measures
- **Ministerial directive** requirements

Your compliance policies and procedures should also include the processes and controls you have put in place to meet your requirements, including:

- when the obligation is triggered
- the information that must be reported, recorded, or considered
- the procedures you created to ensure that you fulfill a requirement
- the timelines associated with your requirements and methods of reporting (if applicable)

Your policies and procedures must also describe the steps you will take for all the obligations that require you to take reasonable measures. For example, when you are required to take reasonable measures to obtain information to include in a report, your policies and procedures must describe the steps you will take, which could include asking the client.

If your reporting entity sector has an industry association or governing body that has provided you with a generic set of policies and procedures, you must tailor them to your business.

The level of detail in your compliance policies and procedures will depend on your business's size, structure, and complexity, and degree of exposure to money laundering, terrorist activity financing and sanctions evasion risks.

4. Risk assessment requirements

Your compliance program must include policies and procedures that you develop and apply to assess your money laundering, terrorist activity financing and sanctions evasion risks in the course of your activities. When assessing and documenting your money laundering, terrorist activity financing and sanctions evasion risks, you must consider the following:

- your clients, business relationships, and correspondent banking relationships including their activity patterns and geographic locations
- the products, services and delivery channels you offer

- the geographic location(s) where you conduct your activities
- if you are a **financial entity**, **life insurance company**, or **securities dealer**, the risks resulting from the activities of an **affiliate,** if it is also subject to the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and associated Regulations under these reporting entity sectors, or if it is a foreign affiliate that carries out activities outside Canada that are similar to these sectors
- the risks resulting from new developments or new technologies you intend to carry out or introduce, before doing so, that may have an impact on your clients, business relationships, products, services or delivery channels, or the geographic location of your activities
- the applicable risks for your reporting entity sector, detailed in the latest National Risk Assessment of Money Laundering and Terrorist Financing in Canada
- any other relevant factors affecting your business (for example, employee turnover, industry rules and regulations)

If, at any time, you consider the risk of a money laundering or terrorist activity financing offence to be high, you must take enhanced measures.

5. Enhanced measures

Enhanced measures are the additional controls and processes that you have put in place to manage and reduce the risks associated with your high-risk clients and business areas. As part of your compliance program, you must develop and apply written policies and procedures for the enhanced measures that you will take for any money laundering, terrorist activity financing or sanctions evasion risks you identify as high.

Your policies and procedures for enhanced measures must include:

- the additional steps, based on assessment of the risk, that you will take to verify the identity of a person or entity
- any other additional steps that you will take to mitigate the risks, including, but not limited to, the additional steps to:
  - ensure client identification information and beneficial ownership information is updated at a frequency that is appropriate to the level of risk
  - conduct ongoing monitoring of business relationships at a frequency that is appropriate to the level of risk

Enhanced measures to mitigate risk can include:

- obtaining additional information on a client (for example, information from public databases and the internet)
- obtaining information on the client's source of funds or source of wealth
- obtaining information on the reasons for attempted or conducted transactions, or

- any other measures you deem appropriate

6. Training program and plan requirements

If you have employees, agents or mandataries, or other persons authorized to act on your behalf, you must develop and maintain a written, ongoing compliance training program. Your training program should explain what your employees, agents or mandataries, or other persons authorized to act on your behalf, need to know and understand, including:

- your requirements under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (the Act) and associated Regulations
- background information on money laundering and terrorist activity financing, such as the definition of money laundering and terrorist activity financing, and methods of money laundering and terrorist activity financing
- how your business or profession could be vulnerable to money laundering and terrorist activity financing activities (provide indicators and examples)
- the compliance policies and procedures you have developed to help meet your requirements under the Act and associated Regulations for preventing and detecting money laundering and terrorist activity financing, including your reporting, record keeping and know your client requirements
- their roles and responsibilities in detecting and deterring money laundering and terrorist activity financing activities, and when dealing with potentially suspicious activities or transactions

You must institute and document a plan for your ongoing compliance training program and for delivering the training. Your training plan should cover how you will implement your ongoing compliance training program and its delivery.

This includes documenting the steps you will take to ensure your employees, agents or mandataries, or other persons authorized to act on your behalf receive an appropriate level of training relevant to their duties and position, on an ongoing basis.

Your training plan should include information on:

- training recipients
- training topics and materials
- training methods for delivery
- training frequency

Training recipients

Your training plan should explain who will receive training. Training recipients should include those who:

- have contact with clients, such as front-line staff or agents
- are involved in client transaction activities

- handle cash, funds, or virtual currency for you, in any way, and
- are responsible for implementing or overseeing the compliance program, such as the compliance officer, senior management, information technology staff or internal auditors

Training topics and material

Your training plan should outline the topics that will be covered in your training program. It should also include the sources of the training materials that will cover these topics.

Training methods for delivery

Your training plan should describe the training method(s) that you will use to deliver your ongoing compliance training program.

Training methods could include:

- self-directed learning (where recipients read materials on their own, register for on-line courses or use e-learning materials)
- information sessions
- face-to-face meetings
- classroom
- conferences, and
- on-the-job training where instruction is provided

Instructors can be in-house personnel or an external service provider, but they should have knowledge of the Act and associated Regulations. If you decide to use in-house personnel, you may need to hire or allocate staff to provide training.

If you decide to use an external service provider, you may need to determine whether their services and training content are suitable for your business. You can use 1 or more training methods. The method(s) that you choose may depend on the size of your business and the number of people that need to be trained.

Training frequency

Your training plan should describe the frequency of your training program. Training can be delivered at regular intervals (for example, monthly, semi-annually, annually), when certain events occur (for example, before a new employee deals with clients, after a procedure is changed), or by using a combination of both.

Your training program and plan should be tailored to your business's size, structure and complexity, and its degree of exposure to money laundering, terrorist activity financing and sanctions evasion risk. For example, if you are a large business, you may decide to provide different types of training to your employees, agents or mandataries, or other persons authorized to act on your behalf based

on their specific roles and duties (for example, general or specialized training). This should be explained in your training plan.

Your training program should also include a record of the training that has been delivered (for example, the date the training took place, a list of the attendees who received the training, the topics that were covered). Training records will help you keep track of the training and assist you in scheduling the next training dates. They will also demonstrate that you are carrying out your training program on an ongoing basis.

Note: If you are a sole proprietor with no employees, agents or other individuals authorized to act on your behalf, you are not required to have a training program nor are you required to have a training plan in place for yourself.

7. Two-year effectiveness review and plan requirements

A two-year effectiveness review is an evaluation that must be conducted every 2 years (at a minimum) to test the effectiveness of the elements of your compliance program (policies and procedures, risk assessment, and ongoing training program and plan). You must start your effectiveness review no later than 2 years (24 months) from the start of your previous review. You must also ensure that you have completed your previous review before you start the next review.

The purpose of an effectiveness review is to determine whether your compliance program has gaps or weaknesses that may prevent your business from effectively detecting and preventing money laundering, terrorist activity financing and sanctions evasion.

Your effectiveness review will help you determine if:

- your business practices reflect what is written in your compliance program documentation and if you are meeting your requirements under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (the Act) and associated Regulations
- your risk assessment is effective at identifying and mitigating the money laundering, terrorist activity financing and sanctions evasion risks related to your clients, affiliates (if any), products, services, delivery channels, new developments or technology, and geographic locations where you do business

The review must be carried out and the results documented by an internal or external auditor, or by yourself if you do not have an auditor. Your review should be conducted by someone who is knowledgeable of your requirements under the Act and associated Regulations. Also, as a best practice, to ensure that your review is impartial, it should not be conducted by someone who is directly involved in your compliance program activities. Regardless of who carries out the review, as a reporting entity it is your responsibility to ensure that the review is conducted (at a minimum) every 2 years and that the review tests the effectiveness of your compliance program.

You must also institute and document a plan for the two-year effectiveness review of your compliance program. This plan should describe the scope of the review and must include all the elements of your compliance program. The breadth and depth of review for each element may vary depending on factors such as:

- the complexity of your business
- transaction volumes
- findings from previous reviews
- current money laundering, terrorist activity financing and sanctions evasion risks.

Your plan should not only describe the scope of the review, but it should include the rationale that supports the areas of focus, the time period that will be reviewed, the anticipated evaluation methods and sample sizes.

The evaluation methods can include, but are not limited to, interviewing staff, sampling records and reviewing documentation. The following are examples of what can be included in your review:

- interviews with those handling transactions to evaluate their knowledge of your policies and procedures and related record keeping, client identification and reporting requirements
- a review of a sample of your records to assess whether your client identification policies and procedures are being followed
- a review of your agreements with agents or mandataries, as applicable, as well as a review of a sample of the information that your agents or mandataries referred to in order to verify the identity of persons, to assess whether client identification policies and procedures are being followed
- a review of transactions to assess whether suspicious transactions were reported to FINTRAC
- a review of large cash transactions to assess whether they were reported to FINTRAC with accurate information and within the prescribed timelines
- a review of electronic funds transfers to assess whether reportable transfers were reported to FINTRAC with accurate information and within the prescribed timelines (applicable to reporting entity sectors that have electronic funds transfer obligations)
- a review of a sample of your client records to see whether the risk assessment was applied in accordance with your risk assessment process
- a review of a sample of your client records to see whether the frequency of your ongoing monitoring is adequate and carried out in accordance with the client's risk level assessment
- a review of a sample of high-risk client records to confirm that enhanced mitigation measures were taken
- a review of a sample of your records to confirm that proper record keeping procedures are being followed
- a review of your risk assessment to confirm that it reflects your current operations

- a review of your policies and procedures to ensure that they are up to date and reflect the current legislative requirements and that they reflect your current business practices

You should also document the following in your two-year effectiveness review:

- the date the review was conducted, the period that was covered by the review and the person or entity who performed the review
- the results of the tests that were performed
- the conclusions, including deficiencies, recommendations and action plans, if any

If you are an entity, you must report, in writing, the following to a senior officer no later than 30 days after the completion of the effectiveness review:

- the findings of the review (for example, deficiencies, recommendations, action plans)
- any updates made to the policies and procedures during the reporting period (the period covered by the two-year review) that were not made as a result of the review itself
- the status of the implementation of the updates made to your policies and procedures

FINTRAC assessment manual: The approach and methods used during examinations

From: Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)

Introduction

Why is the manual important and what does it cover?

The Financial Transactions and Reports Analysis Centre of Canada, known as FINTRAC, is committed to helping you meet the legal requirements set out in the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and associated Regulations.

Our objective is to support businesses as we work together to protect Canadians and the integrity of Canada's financial system from money laundering and terrorist activity financing vulnerabilities.

To this end, in the spirit of openness and transparency, we have published this assessment manual detailing how we conduct examinations.

Examinations are one of the main activities we use to assess whether businesses are adequately implementing and maintaining a compliance program, which is important to detecting and mitigating the money laundering and terrorist

activity financing risks your business may face. In turn, it can also reduce financial, reputational and legal risks should criminals try to exploit your business's vulnerabilities.

The manual does not replace the PCMLTFA and associated Regulations, establish new legal requirements or expectations, serve as regulatory guidance, or tell you how to carry out your day-to-day business operations.

The manual, which is for all Canadian businesses covered by the PCMLTFA, describes how FINTRAC conducts its compliance examinations. It is meant to help you understand how we assess whether you have implemented and maintained a compliance program that adequately meets all of the legal requirements, and to help you prepare for a FINTRAC examination.

The manual is divided into three parts:

1. Part 1—the framework we apply to ensure that we conduct our examinations in a consistent manner;
2. Part 2—the phases of an examination; and
3. Part 3—the methods we use in examinations to assess whether you are adequately meeting the legal requirements.

Canadian businesses covered under the Act:

- Accountants
- British Columbia notaries
- Casinos
- Dealers in precious metals and stones
- Financial entities
- Life insurance
- Money services businesses
- Real estate
- Securities dealers

While our examinations take into account the differences across business sectors, our overall examination approach and methods remain the same for all.

The assessment methods we may use in an examination are not limited to those described in the manual. The manual is an evergreen document that we will update through consultations with businesses as our assessment methods evolve, or as legislative and regulatory changes are introduced.

The manual represents FINTRAC's examination approach and methods. It does not address how other federal or provincial regulators or supervisors carry out their oversight activities relating to compliance with anti-money laundering and anti-terrorist activity financing requirements.

Note: FINTRAC typically refers to the businesses covered by the PCMLTFA as reporting entities, while the PCMLTFA refers to "persons" and "entities". In this manual, the term "businesses" will be used.

Part 1—Examination framework

The examination framework we use ensures that we conduct our examinations in a consistent manner, while taking into account the type, nature, size, and complexity of different businesses.

The framework is comprised of three main components outlined below.

Risk-based examinations

We focus our examinations on areas where your business may be vulnerable to money laundering or terrorist activity financing risks and where there is a greater risk of not meeting the legal requirements (risk of non-compliance). Using this approach reduces the burden on businesses by minimizing disruptions and ensuring the effective and efficient use of resources.

When determining the risks your business may be exposed to, we rely on our experience, knowledge, training, and professional judgment. We take into account relevant information from FINTRAC publications and guidance. We may also take into consideration relevant information taken from publicly available reports and publications issued by well-known credible sources on money laundering and terrorist activity financing.

We recognize that businesses will adopt different approaches to implementing and maintaining their compliance programs, based on their type, nature, size, complexity and risk profile. In light of this, we will include in our examination plans the areas you have identified as posing a higher risk to your business as well as gaps you have identified in your compliance program, where appropriate.

Part 2 of the manual describes in more detail how risk informs our examinations.

Assessment methods

Once we have evaluated your business's risks, we select assessment methods described in Part 3 that we will use as part of our examination.

We use the methods to assess how you comply with the legal requirements set out in the PCMLTFA and associated Regulations. We also consider FINTRAC guidance, which sets out how we interpret the legal requirements.

For example, the PCMLTFA requires that Suspicious Transaction Reports be submitted to FINTRAC under certain circumstances. FINTRAC guidance presents money laundering and terrorist activity financing indicators to help businesses better understand typical risks they may be exposed to, and should watch for, in their day-to-day activities. When we assess the requirement to report suspicious transactions using the methods described in the manual, we may refer to the indicators we provide in the guidance, in addition to the obligation in the PCMLTFA, to support the rationale for suspicion.

When applying our assessment methods, we may review your documents, client records, records of transactions, and financial transaction reports, as well as conduct interviews.

Assessment approach to evaluating findings

We take an assessment approach when evaluating examination findings. This means that we take a holistic approach when evaluating findings rather than evaluating them in isolation. We focus less on technical non-compliance and more on the overall soundness of the areas of your compliance program we are assessing.

We look at all the information gathered to ensure that your compliance program is complete and put into practice. When we identify technical non-compliance within an otherwise adequate system of policies, procedures, processes, and controls, we will notify you of the non-compliance, but the overall result of our assessment may not be negatively affected by it.

With our findings, we aim to make decisions that are reasonable, fair, and balanced. We base our decisions on what we believe a reasonable, experienced and knowledgeable person in your business sector would have done if they were assessing the same set of facts and circumstances.

We expect you to provide us with, or make available, all relevant facts and information so that we can make decisions based on complete information.

Finally, in the spirit of transparency, openness, and fairness in our examinations, we will share our findings with you during the examination, explain them, and offer you the opportunity to provide us with additional information for our consideration.

Part 2—Examination phases

Examinations are conducted on weekdays, during FINTRAC's regular business hours (8 a.m. to 5 p.m.). If these hours do not suit your business, please notify us, as we may be able to offer some flexibility.

The number of days we will spend on your premises will depend on the type, nature, size, and complexity of your business. For example, the examination of a small or medium-sized business may take less than a week, while the examination of a bank may take several weeks.

In order to ensure the examination runs efficiently, and to reduce unnecessary business disruptions, it is important that you provide us with the requested information, documents, client records, records of transactions, and access to your staff, for interview purposes, in a timely manner.

Our examinations are broken down into three phases: planning and scoping; examination and assessment; and developing the findings and finalizing the exami-

nation. Below, we present each phase and describe the roles and responsibilities of each party to an examination.

Roles and responsibilities

You can expect us to be professional, provide clear information, respect your privacy and the confidentiality of your clients' personal and financial information, and offer services in either official language. You can also expect us to observe the highest standard of ethical conduct.

The PCMLTFA requires FINTRAC to protect the personal information under its control. We take this mandate very seriously and safeguard all personal information when we carry out an examination.

The PCMLTFA also requires that you provide FINTRAC with assistance during an examination. This assistance includes providing us with the information we ask for within the agreed upon timelines, giving us access to your place of business, providing us with the documents and records we request, answering our questions about your business and making employees available for interviews. We may also ask you to assist us in accessing information stored on your computers and systems, to help us better understand your operations.

Phase 1—Planning and scoping

Once we select a business for examination, we begin planning the examination, which includes selecting the areas and requirements we will examine (examination scope), as well as the assessment methods we will use.

Planning the examination We develop the overall plan to determine the staffing needs and level of expertise required to conduct the examination based on the type, nature, size, and complexity of the business to be examined.

Setting the scope of the examination When we set the scope of the examination, we choose the business areas and the specific requirements that we will examine.

To do this, we first gain a general understanding of your business model, environment, activities and operations. We then look at the risks your business may be exposed to, as well as the risks associated with your business sector. This includes determining:

1. your business areas at risk of being used for money laundering and terrorist activity financing; and
2. your business areas at risk of not meeting the legal requirements of the PCMLTFA and associated Regulations (the risk of non-compliance).

In order to gather this information and assess your risk, we may consult the files we have on your business and search the internet. For example, we may look at, as applicable:

- Your history of compliance with the PCMLTFA and associated Regulations;
- Findings from previous FINTRAC examinations or examinations conducted by a regulator or supervisor with whom FINTRAC has established a Memorandum of Understanding (MOU) to share information related to compliance with the PCMLTFA;
- Letters and emails you may have sent us describing how you will address previously found non-compliance;
- Voluntary self-declarations of non-compliance (VSDONC) in which you informed us that you have not met certain requirements;
- Previous questions you asked about the requirements or requests for policy interpretations to ensure that potential non-compliance has been addressed in a reasonable period following the enquiries (if applicable);
- Financial transaction reports you sent to FINTRAC;
- Actions taken when you received feedback from us about the quality, timing or volume of your financial transaction reports;
- Policies and procedures, risk assessments and two-year reviews and other documents and information that we may have on file from a previous examination;
- Information about your business or your clients available on the internet; and
- History of enforcement actions (administrative or criminal), in respect of your business, taken by FINTRAC, other regulatory/supervisory bodies, and law enforcement.

We use this information to assess risk and determine the scope of the examination, including the requirements we will assess and the appropriate assessment methods we will use. We also use a risk-based approach to establish the number of sample documents, client records, records of transactions, and financial transaction reports we plan to examine, the period covered by the examination, and who will be interviewed from your business.

When we have limited information on file regarding a business, we rely on the characteristics of similar businesses, and on the information obtained in our examination notification call to define the scope of the examination.

Desk versus on-site examinations We conduct examinations either remotely (a desk examination), or at your place of business (an on-site examination). You will be informed of the examination's location during our notification call and in the notification letter.

In either case, you must send all the requested information, documents and records to FINTRAC for a preliminary review.

When we conduct an examination remotely, we hold interviews with your compliance officer, employees, and agents (if applicable). When we conduct our examination at your place of business, we typically hold in-person interviews at

your main location and may visit or call your other locations, if applicable, to conduct our interviews.

If you have multiple business locations, we typically ask that the information, documents, and records from all your locations be made available for our review at the location that has been selected for the examination.

Examination notification We will call the person responsible for the implementation of your compliance program (commonly referred to as the compliance officer) to discuss an upcoming examination's scope and date.

After our notification call, we will confirm the examination details in writing with a notification letter addressed to your compliance officer. The letter will indicate where and when we will conduct the examination. We will usually send you the letter 30 to 45 days before the examination date. Given the amount of information and data involved, we may provide larger businesses with more than 45 days' notice to grant them sufficient time to gather the required information.

The letter is our formal request for information, documents and records, and for your assistance during the examination. We will ask you to send the requested material to FINTRAC, including, for example, your compliance program documents and when applicable, lists of transactions and records of transactions.

While we always encourage businesses to address non-compliance whenever they detect it, we will not generally accept certain documents, records, or financial transaction reports once an examination has started.

If you identify non-compliance after a FINTRAC examination has started, you should inform the FINTRAC officer immediately and send us a voluntary self-declaration of non-compliance. We consider the date on which we notify you of the examination to be the start of the examination (that is, the date of the notification call).

When we receive a voluntary self-declaration of non-compliance on an issue that was not previously voluntarily disclosed before a FINTRAC examination has started, we will not consider enforcement actions, such as an administrative monetary penalty. However, if we receive a self-declaration during an examination, we will assess the non-compliance as part of the examination, work with the business to correct it, and determine if the non-compliance warrants an enforcement action.

For example, if you did not submit a financial transaction report to FINTRAC when required and then submit it after the notification date, we will consider that you did not meet your requirement to submit the report. In addition, there may be situations where compliance program documents (for example, compliance policies and procedures) are created or adjusted after the notification date. In such cases, we may determine that you did not meet the compliance program requirements.

When we ask you to send us documents, client records and transaction records in advance of the examination, we do so to conduct the examination more efficiently and to minimize any disruption to your business during the on-site examination.

While we request most of the documents that we will need during the planning phase, we may request additional information or documents at a later stage of the examination process.

Given the sensitive nature of the documentation, and in the interest of limiting the risk of loss during transit, we encourage you to provide the material electronically through a secure digital mailbox service. This type of service uses advanced encryption that allows for the transmission of sensitive information securely. If you agree to use this option, please contact FINTRAC for further information on the process.

Reviewing the material you send us We will review the material we requested in our notification letter, including your compliance program documents. This material is used to help us prepare interview questions. It may also further inform the scope of our examination. If the scope of the examination changes, we will notify you.

Phase 2—Examination and assessment

In this phase, we apply the assessment methods described in Part 3.

We start by conducting a preliminary assessment of the requirements that were part of the initial examination scope. We review your documents, conduct preliminarily interviews with your compliance officer, employees, or agents and review a sample of your transaction records and financial transaction reports. The objective of this preliminary assessment is to determine areas where we need to focus our attention.

If we identify areas or issues that require further attention, we will sample more client records, transaction records and reports, and if required, conduct follow-up interviews with your compliance officer, employees or agents. This may lead us to broaden the scope of the examination. If we need to adjust the scope of the examination, you will be notified.

This phase of the examination may extend beyond our last day on your premises or beyond the date of our videoconference or telephone interviews for desk examinations. This may be necessary if we need to further review and analyze certain documents, client records, transaction records, and reports before we consolidate our findings.

Conducting interviews We may interview different members of your staff and your agents. These one-on-one interviews may be in person, by telephone, or by videoconference.

We do our best to minimize undue business disruptions, particularly as they relate to front-line business functions. We also make every effort to make employees feel at ease.

We do not expect interviewees to memorize your business's policies and procedures or other documents. Rather, our goal is to confirm that your employees and agents are aware of the requirements applicable to their duties and know how to seek clarification when needed.

Exit meeting Even if we need to continue our review, once we are ready to leave your premises or have concluded the desk examination, we will hold an exit meeting in person, by telephone, or videoconference to discuss our preliminary findings with you. The findings are presented as "deficiencies". Each deficiency is a violation of a provision in the PCMLTFA or associated Regulations.

At this time, you may offer additional information to help clarify a deficiency. We will agree on a timeline for you to provide this material. After our review of this material, we may maintain our original deficiency, modify it, or withdraw it.

Phase 3—Developing conclusions and finalizing the examination

Deciding on our findings When we consolidate our findings, we use the assessment approach described in Part 1. Using this approach, we focus less on technical non-compliance and more on the overall soundness of the areas of your compliance program we are assessing. We evaluate findings holistically, rather than in isolation, to determine if you are adequately meeting the requirements.

As part of our evaluation, we consider the harm done by not meeting a requirement. In doing so, we assess the nature, relative importance, extent, the root cause of the non-compliance, and any mitigating or aggravating factors.

The nature of the non-compliance means which requirement (such as a compliance program or financial transaction reporting requirement) was not met.

We consider the relative importance of the requirement with which you were not compliant. While all requirements are important, and we expect businesses to fulfill them, certain requirements have a greater impact on FINTRAC's ability to carry out its mandate and on Canada's anti-money laundering and anti-terrorist financing regime. For example, the requirement to submit financial transaction reports could have a greater impact on FINTRAC's intelligence mandate and the regime as a whole than the requirement to submit reports that are free of minor data-quality issues.

We also assess the extent (degree) of the non-compliance; that is, how much information is missing from a required document, record or financial transaction report; how many times the non-compliance is repeated; and if the non-compliance points to gaps in the compliance program. We also try to identify the root cause of the non-compliance.

We look at all of the information we have gathered to ensure that your compliance program is complete and put into practice. When we identify technical non-compliance within an otherwise adequate system of policies, procedures, processes, and controls, we will make note of the non-compliance, but the overall results of our assessment may not be negatively affected by it.

Finally, we take into account other mitigating or aggravating factors that may influence how we view the non-compliance. Mitigating factors may decrease the seriousness of the non-compliance, while aggravating factors may increase it. For example, a business may have submitted a Suspicious Transaction Report (STR), but omitted to send a Large Cash Transaction Report (LCTR) that was also required. If most of the LCTR's information is included in the STR, we may consider this a mitigating factor.

Examination findings letter We will send our examination findings letter to your compliance officer. This letter describes the findings that we discussed during the exit interview.

The letter will indicate the documents, client records, transaction records and financial transaction reports we have examined, as well as the consolidated results of our interviews with your employees and agent. When applicable, we will provide additional information, such as the number of documents we sampled and the number of instances of non-compliance that were found in the sample. The individual records and reports that we have found to be deficient will be listed in an annex to the letter.

In some cases, the letter may also include "observations". They are included to help you improve your business processes and practices in order to strengthen your compliance program.

The letter will also state which of the following three actions we may take following an examination based on the results of our assessment:

- no further compliance or enforcement action;
- possible follow-up compliance action; or
- a recommendation for an enforcement action, such as an administrative monetary penalty (AMP).

When you receive a findings letter, we expect you to address the causes of the identified deficiencies within a reasonable amount of time. In certain cases, we may ask you to send us an action plan that describes how and when the cause of the deficiencies will be addressed. When requested, an action plan must be sent within 30 calendar days of the receipt of the findings letter, unless otherwise specified. When an action plan is not requested, we still expect that you will take the time to address the cause of the deficiencies. Whether an action plan has been requested or not, you do not need to send us documents that demonstrate that the deficiencies have been addressed. We will evaluate these documents should we conduct a follow-up compliance activity.

If, on the basis of the examination findings, FINTRAC is considering issuing an administrative monetary penalty, this will be stated in the findings letter. The findings letter will also inform you how many days you have to send us any additional information, which is generally 30 calendar days, that you believe could influence our findings or our decision to issue an administrative monetary penalty. We will take into consideration additional relevant information you provide us within the established timeline and send you a written response of our decision. In cases where any adjustment to the findings is required, our response will include a revised findings letter.

Follow-up activities After an examination, we may follow up to make sure that you have addressed the deficiencies we identified in our findings letter. We may:

- Conduct a follow-up on-site or desk examination;
- Monitor the reports you send to FINTRAC, if the examination revealed that the quality of your reports was inadequate or that the reports were late; and
- Monitor the progress of your action plan, if we asked you to provide one.

Penalties for non-compliance Our focus is on supporting businesses—administrative monetary penalties are not meant as an automatic response to non-compliance. If we decide to impose a penalty, our aim is to encourage a change in compliance behaviour. When deciding whether a penalty should be considered, FINTRAC compliance officers assess the harm done by looking at various factors. They will assess the nature, relative importance, extent, and root cause of the non-compliance, mitigating or aggravating factors, and a business's history of compliance. Generally speaking, penalties may be issued in cases of serious or repeated non-compliance. We will consider the unique factors in each case to determine if the examination should result in a penalty.

Should you receive a penalty, you have the right to make representations to FINTRAC's Director and Chief Executive Officer (CEO) for the review of your file. You also have the right to appeal the Director and CEO's decision to the Federal Court. Please visit our administrative monetary penalties page for more information.

We may disclose cases of non-compliance to law enforcement when there is extensive non-compliance or little expectation of immediate or future compliance, and where there are reasonable grounds to suspect that the information would be relevant to investigating or prosecuting an offence arising out of a contravention of Part 1 or Part 1.1 of the PCMLTFA (related to non-compliance). It is then up to law enforcement to conduct an investigation and decide whether further action is warranted. Please visit our penalties for non-compliance page for more information.

Part 3—Assessment methods

In Part 3, we describe the assessment methods that we use to ensure that you are adequately meeting the requirements.

We use the methods to assess how you comply with the legal requirements set out in the PCMLTFA and associated Regulations. We also consider FINTRAC guidance, which sets out how we interpret the legal requirements.

We assess the following requirements, unless exemptions apply:

- compliance program requirements;
- client identification and other know your client requirements;
- financial transactions reporting requirements;
- record keeping requirements;
- correspondent banking relationship requirements;
- foreign branches, foreign subsidiaries and affiliates requirements;
- registration of money services business and foreign money services business requirements; and
- ministerial directives' requirements.

We may not assess all of the requirements listed above during an examination, nor will we use every assessment method described in this section. Instead we will choose the requirements and the assessment methods that best fit our risk assessment of your business and the scope of the examination.

In the interest of efficiency, we may apply some of our assessment methods simultaneously, or use variations of the methods described in this section.

3.1. Compliance program requirements

This section describes the methods we use to assess whether you have adequately implemented and maintained a compliance program.

The five required elements of a compliance program are to:

- appoint a compliance officer;
- develop policies and procedures;
- conduct a risk assessment;
- develop and provide an ongoing compliance training program; and a plan for the delivery of the program; and
- develop a plan to conduct an effectiveness review of the compliance program, and carry it out every two years.

We will verify that you have a well-documented and complete compliance program in place, and assess whether your compliance program is put into practice.

To do so, we assess your compliance with other requirements, such as client identification and other know your client requirements, reporting requirements, and record keeping requirements. We may consider deficiencies identified through

the assessment of these other requirements to be an indication that one or more of the five elements of your compliance program is not being applied.

3.1.1. Compliance officer—the person responsible for the implementation of the compliance program (Applicable to all business sectors)

We use the methods described in this section to assess your compliance with the requirement to appoint a compliance officer who is responsible for implementing your compliance program.

We verify that the following criteria have been adequately met:appointment (selection), authority, knowledge, and duties.

To conduct this assessment, we may:

- Review documents that show you have formally appointed a compliance officer. We may also review your compliance officer's job description, documents that describe their authority, and an organizational chart. We may also review your policies and procedures to confirm that they give your compliance officer enough guidance to meet the legal requirements.
  - Confirm that the compliance officer has direct access to senior management or the board of directors, to those who make important decisions about compliance issues or who control the company (where applicable).
  - Confirm that the compliance officer has timely access to information from all business lines to ensure they have knowledge of and are aware of potential compliance related risks or concerns (where applicable).
- Look at the compliance officer's background and experience, as well as the training you have given them to verify that you have made sure that the officer has enough knowledge of:
  - your business's functions and structure;
  - your sector's money laundering and terrorist activity financing risks and vulnerabilities, as well as related trends and typologies; and
  - your sector's requirements under the PCMLTFA and associated Regulations.

Our focus While we assess the appointment, authority, knowledge and duties of the compliance officer, our focus is on verifying that the compliance officer is fulfilling their duties to implement a sound compliance program. To make this determination, we assess whether the areas of your compliance program that we examined are adequately put into practice.

3.1.2. Policies and procedures (Applicable to all business sectors)

We use the methods described in this section to assess your compliance with the requirement to develop, document and apply policies and procedures.

We verify that your policies and procedures cover requirements such as (if applicable, and not meant to be exhaustive):

- compliance program, including special measures you take for high risk;
- client identification and other know your client requirements;
- financial transactions reporting;
- record keeping;
- correspondent banking relationships;
- foreign branches, foreign subsidiaries and affiliates;
- registration of money services businesses and foreign money services businesses;
- travel rule;
- reasonable measures; and
- ministerial directives.

We also verify that your policies and procedures include the processes and controls you have in place to implement your policies and meet your requirements. For example:

- The process you have in place and the source you use to convert foreign currency and virtual currency into Canadian dollars to meet your reporting, verifying identity and record keeping obligations when an exchange rate is not published by the Bank of Canada.
- The processes you have in place to take reasonable measures to obtain and report information.
- The process you have in place to establish reasonable grounds to suspect that transactions or attempted transactions may be related to money laundering or terrorist activity financing, and your process for submitting Suspicious Transaction Reports " as soon as practicable" and as a priority over other tasks.
- The process you have in place for electronic funds transfer and virtual currency transfers to meet your travel rule obligations. We will also review the process you follow when, after taking reasonable measures, you are unable to obtain the required information and the steps that you take to decide whether you allow, suspend or reject a transaction, and any follow-up measures you take.

We also verify that your policies and procedures are adequate, tailored to your business (that is, they take into account the type, nature, size, and complexity of your business) and are designed to control the risks you may face.

To conduct this assessment, we may:

- Review your policies and procedures to confirm that they are written, up to date and, if your business is an entity, approved by a senior officer.
- Review your policies and procedures to confirm that they provide enough guidance for your employees or agents.
- Interview your employees and agents to assess their knowledge of your policies and procedures.

Our focus While we assess your policies and procedures, we will focus on ensuring that you are adequately putting them into practice with respect to your obligations, including reporting, client identification, beneficial ownership, third party determination, politically exposed persons and heads of international organizations, ministerial directives, and special measures for high-risk client requirements, when required.

3.1.3. Risk assessment (Applicable to all business sectors)

We use the methods described in this section to assess your compliance with the requirement to assess and document your business risks and vulnerabilities related to money laundering and terrorist activity financing.

We verify that you have a documented risk assessment and that it includes the following elements, as applicable: products, services and delivery channels; clients and business relationships; geographic locations; new developments and new technologies; foreign and domestic affiliated entities (if applicable), and other prescribed high-risk elements such as persons or entities listed in ministerial directives.

We also verify that your risk assessment takes into account the type, nature, size, and complexity of your business, and we consider the rationale for each element of your business risk assessment.

To conduct this assessment, we may:

- Verify that you have assessed and documented the risks to your business related to money laundering and terrorist activity financing and that you have identified measures to mitigate these risks, and applied special measures for any high risks.
- Verify that you have assessed and documented risk using a risk-based approach before you implement a new development or introduce a new technology that may affect your clients, business relationships, products, services or delivery channels, or the geographic location of your activities. We may also review the process you follow before introducing new developments or new technologies.
- Verify that you have assessed risks adequately by looking at the areas you have identified as posing a high-risk and the assessment's written rationale. We may review a sample of client records and transaction records in order to determine whether your risk assessment is reasonable and consistent with your business's risk profile, and policies and procedures.
- Verify that you document and apply special measures to elements you have determined pose a high risk. Special measures include taking enhanced measures to identify clients and to mitigate risks such as keeping client identification information up to date and conducting ongoing monitoring for the purpose of detecting suspicious transactions, as well as any other enhanced measures you identify.

- Verify that the controls you have in place are consistent with your identified risk levels (ratings or rankings) and adequately mitigate your business risks.
- Verify that your compliance program is in line with and informed by the results of your risk assessment. For example, we will confirm that your policies and procedures, ongoing training documentation and two-year review documentation adequately address the areas you have assessed as posing a higher risk and that they provide adequate guidance to your employees or agents.
- Verify how you use publicly available information to inform your compliance program.
- Interview the employees and agents responsible for your risk assessment to assess their knowledge of the requirements associated with conducting a risk assessment.

Our focus While we review the elements of your risk assessment, we will focus on verifying that you have considered and rated the risk of all aspects of your business, that you have provided rationales for your decisions, and that you have applied special measures to areas identified as posing a high risk.

3.1.4. Ongoing compliance training program and plan (Applicable to all business sectors)

We use the methods described in this section to assess your compliance with the requirement to develop and maintain a written, ongoing compliance training program for employees, agents, and those acting on your behalf. We will also assess your compliance with the requirement to have a documented plan to deliver your training program on an ongoing basis.

We look at who receives training, what topics are covered, when and how often training takes place, how you have implemented your training program, and how training is delivered.

We also verify that your training program is adequate, takes into account the size, type, nature and complexity of your business, and is put into practice.

To conduct this assessment, we may:

- Review your policies and procedures to confirm that they provide enough guidance to your employees, agents, and those acting on your behalf to develop, implement and maintain an ongoing training program.
- Review your training plan to confirm that it considers and documents the steps you take to develop, maintain, and deliver your training program.
- Review your training material to confirm that the training content is suitable. For example, we verify that it is tailored to your business and adequate for your employees, agents and their respective responsibilities.
- Interview your employees and agents to confirm that they understand the requirements as they relate to their positions, understand and follow the

policies and procedures, understand how your business could be vulnerable to ML/TF activities, and have received adequate ongoing training.

Our focus While we assess your ongoing training program, we will focus on whether it helps your employees and agents understand the requirements, your policies and procedures, and indicators and trends of money laundering and terrorist activity financing. We will also pay close attention to the training you provide regarding the detection of suspicious transactions.

3.1.5. Two-year effectiveness review (Applicable to all business sectors)

We use the methods described in this section to assess your compliance with the requirement to institute and document a review of the compliance program to test its effectiveness.

We will verify that you have a documented plan to conduct a review of your policies and procedures, risk assessment, and training program for the purpose of testing their effectiveness, and that you carry out this plan to conduct a review every two years.

We will verify that your two-year effectiveness review is adequate, tailored to your business by taking into account the type, nature, size, and complexity of your business, and consistent with your risk assessment.

To conduct this assessment, we may:

- Review your documented plan to verify that it considers all the elements of your compliance program for the purpose of testing its effectiveness.
- Review your policies and procedures to determine whether they give enough guidance to your employees or agents to conduct a two-year effectiveness review.
- Look at the scope of the review (what the review covered) and methodology (how the review was conducted):
  - Interview the person who conducted the review to learn about its scope and methodology, and to ensure that they understand all the requirements that apply to your business;
  - When looking at the scope, for example, we assess whether your policies and procedures, risk assessment and ongoing compliance training program have been reviewed and cover the current legal requirements and your current operations. We also confirm that the review covers and tests all the requirements applicable to your sector; and
  - When looking at the methodology, for example, we verify whether the review was carried out by an internal or external auditor, or by you if you do not have an auditor; whether it was conducted

within the required timelines; and whether the testing methods and methodology used were adequate and reasonable.

- Verify that a written report has been provided to a senior officer within 30 days after the completion of the review, and that the report includes the findings of the review, updates made to the policies and procedures within the reporting period of the review, and the status of the implementation of these updates.
- Verify that the findings of the review are being actioned.

Our focus We verify that your review assesses whether you have a well-documented compliance program and that your program is adequately put into practice. We will also focus on whether your review adequately identifies areas where you did not meet your requirements, whether you updated your policies and procedures, and the status of these updates.

3.2. Client identification and other know your client requirements

We use the methods described in this section to assess your compliance with client identification and other know your client requirements.

3.2.1. Client identification requirements (Applicable to all business sectors)

To conduct our assessment of your compliance with the verifying client identity requirements we may:

- Review your policies and procedures to confirm that they give enough guidance to your employees or agents to verify the identity of your clients.
- Review client records and transaction records to confirm that you apply these policies and procedures.
- Confirm, through a review of client records and transaction records, that you verify the identity of persons and entities in all situations where you are required to do so. These situations include, but are not limited to, when you:
  - open an account for a client, if applicable;
  - receive cash or virtual currency in the amount of $10,000 or more from, or on behalf of, the same person or entity within a 24-hour period;
  - must submit a Suspicious Transaction Report;
  - must create an information record; and
  - are unable to obtain or confirm beneficial ownership information and must therefore take reasonable measures to identify the most senior managing officer of the entity.
- Verify that you use the methods prescribed by law to verify the identity of a person or an entity and that you rely on valid and current information, or authentic, valid and current documents to do so.

- Confirm that you verify the identity of your clients within the prescribed timeframe.
- Interview your employees and agents to assess their knowledge of verifying client identity requirements.

If you use an agent, another reporting entity, or a foreign affiliated entity to help you verify the identity of clients, we may:

- Verify that you have a written agreement with the agent, reporting entity, or the foreign affiliate.
- Verify that you obtain all the required information from the agent, reporting entity, or the foreign affiliate as soon as feasible.
- Verify how you ensure that your agent, reporting entity, or foreign affiliate is using the identity verification methods required by law.

In addition, we verify that you document the required information when you verify the identity of a person or an entity. Refer to our record keeping guidance for more information on the requirement to keep records and to the section of this manual that describes the methods we use to assess record keeping.

When you have verified the identity of a client as required by the PCMLTFA and associated Regulations, you may have additional responsibilities related to know your client requirements. Refer to our know your client guidance and to the section of this manual that describes the methods we use to assess these requirements for more information.

Our focus We will focus on the steps you take to ensure that you verify the identity of a person or an entity.

3.2.2. Know your client requirements We use the methods described in this section to assess your compliance with the know your client requirements, including:

- Business relationships and ongoing monitoring requirements;
- Beneficial ownership requirements;
- Third party determination requirements; and **(based on specific activity)**
- Politically exposed persons and heads of international organizations requirements. **(Based on specific activity)**

To assess the requirements listed above, we may:

- Review your policies and procedures to confirm that they provide enough guidance for your employees or agents.
- Review your client records and transaction records to confirm that you put the policies and procedures into practice.
- Review records of transactions to confirm that you take the necessary steps for all the know your client requirements (as applicable) including:
  - taking all the measures as described in the know your client guidance;

  - obtaining the required approvals;
  - identifying your clients;
  - obtaining and keeping records of required information;
  - performing a risk assessment and ongoing monitoring;
  - taking special measures when required; and
  - meeting the requirements within the prescribed timeframes.
- Interview your employees and agents to assess their knowledge of the know your client requirements.

We use the methods listed below to evaluate your risk assessment practices relating to knowing your client.

Business relationships and ongoing monitoring To conduct this assessment, we may:

- Verify that you used the results of your risk assessment to determine how often you monitor your clients, or which transactions you will monitor more often or more closely. We focus on situations where you may not be adequately monitoring a client or transactions that you consider to pose a high-risk or to be suspicious.
- Verify that you monitor your high-risk business relationships more frequently to identify suspicious transactions, and apply special measures to mitigate risks.
- Review business relationships that you have ranked as posing a low or medium risk to determine whether this ranking is appropriate. We will compare your low-risk and medium-risk clients to your high-risk clients in light of the criteria you have established to identify high-risk situations.
- Review your ongoing monitoring of low and medium risk business relationships to ensure they are adequately monitored.
- Verify that you identify and address inconsistencies between a client's actual and expected transactional activity. Transactional activity inconsistency is a common indicator of money laundering and terrorist activity financing.

Beneficial ownership To conduct this assessment, we may:

- Verify that you have a process in place to obtain beneficial ownership information.
- Verify your records and the process you have in place to confirm the accuracy of the information obtained.
- Verify whether you take reasonable measures to identify the chief executive officer of an entity, or the person who performs that function, for which you are unable to obtain or confirm the beneficial ownership information, and treat the entity as posing a high risk and apply special measures.
- Verify whether you monitor the entities you consider to pose a high risk more frequently than other entities, and apply special measures to mitigate the risks.

Third party transactions To conduct this assessment, we may:

- Review your procedures, processes and controls for situations where you are not able to determine whether an account is to be used by, or on behalf of, a third party when there are reasonable grounds to suspect that it would be.

Politically exposed persons and heads of international organizations To conduct this assessment, we may:

- Verify your records to confirm that you rate all your foreign politically exposed person clients as posing a high risk, as well as their family members and close associates.
- Review your records of domestic politically exposed persons and heads of international organizations, as well as those of their family members and close associates, to ensure that you have adequately assessed the level of risk posed by these clients. To do so, we look at a sample of these clients to see if they meet the criteria you have established to rate a client as posing a high-risk.
- Verify whether you monitor your high-risk clients more frequently than your lower risk clients and apply special measures.
- Review transaction records involving politically exposed persons and heads of international organizations, as well as their family members and close associates, to confirm that you are reporting suspicious transactions when required.

Our focus We will focus on the following:

- **Business relationships and ongoing monitoring:** we will focus on ensuring you have an adequate ongoing monitoring process in place.
- **Beneficial ownership:** we will focus on ensuring that you have a process in place to obtain, and take reasonable steps to confirm the accuracy of beneficial ownership information.
- **Third party determination:** we will focus on ensuring that you are taking reasonable steps to determine whether there is a third party to a transaction or giving instructions on an account.
- **Politically exposed persons and heads of international organizations:** we will focus on ensuring that you are taking reasonable steps to find out if your clients are politically exposed persons or heads of international organizations (including family members and close associates), and for those who pose a high risk, we will focus on the special measures you have in place.

3.3. Financial transactions reporting requirements

We use the methods described in this section to assess your compliance with financial transaction reporting requirements.

To conduct this assessment, we may:

- Review your policies and procedures to confirm that they provide enough guidance for your employees or agents to meet the reporting requirements.
- Review your client records, transaction records and submitted reports to confirm that you adequately apply your policies and procedures.
- Interview your employees and agents to assess their knowledge of the reporting requirements.

Our focus We will focus on confirming that you have sound policies, procedures, processes and controls in place to adequately meet the following requirements: to submit financial transaction reports to FINTRAC (when required); to submit the reports on time; and to submit complete and accurate reports.

3.3.1. Requirements related to all reports types (all report types) (Applicable to all business sectors)

We use the methods described in this section to assess your compliance with reporting requirements. The methods apply to all report types (Large Cash Transaction Reports, Large Virtual Currency Transaction Reports, Electronic Funds Transfer Reports, Casino Disbursement Reports, and Suspicious Transaction Reports), with the exception of Terrorist Property Reports, for which only the assessment method titled "All report types 5" applies.

We use comparison testing, follow-up testing, quality testing, and timing testing.

Comparison testing (All report types 1) Reviewing changes in your reporting behaviour

We review your reporting history to identify important variations, such as a noticeable increase or decrease in reporting, and confirm that you send reportable transactions when required. If we observe changes, we check to see if we have an explanation for them on file. If not, we follow up with you. We may review your transaction records to see if there are reports that should have been sent to us.

Follow-up testing (All report types 2): Ensuring that you resubmit the reports FINTRAC rejected for technical errors

FINTRAC can reject a report if it contains technical errors, such as the way the report is formatted, or when quality issues are identified by our validation process. At the assessment, we provide you with a list of rejected reports which you did not correct and resubmit.

If you think this list is incorrect, we may ask you to provide us with the FINTRAC generated External Report Reference Number or the Reporting Entity's

Report Reference Number to allow us to further enquire. Refer to our guidance on Batch Reporting Instructions and Specifications and FINTRAC Web Reporting system (FWR, formerly F2R).

For the reports that were not resubmitted, we may ask you why that was the case. We may also look at the records of transactions to confirm whether they were reportable.

(All report types 3) Ensuring past reporting issues have been fixed

We review your records and transaction records to confirm that you have fixed previous compliance issues related to reporting, such as those identified by way of a voluntary self-declaration of non-compliance, and those identified through previous compliance assessment activities that FINTRAC has conducted.

Quality testing (All report types 4) Ensuring you report on transactions handled by your agents

We verify that you are reporting the transactions conducted by your agents on your behalf. You, not your agents, are ultimately responsible for submitting these reports. We may ask you to give us a list of your agents, including agency agreements, and a list of the transactions conducted by each agent to ensure that reportable transactions were submitted to FINTRAC.

(All report types 5) Ensuring your reports are complete and accurate

We review the information in your reports to verify that they are complete and accurate.

When we assess the quality of your reports, we verify whether any information is missing, inadequate or incomplete. For example, if the address field in a report was blank, we would consider this to be missing information. If the field included a post office box rather than a civic address, we would consider this to be inadequate information. If the field showed a civic address without the city, we would consider this to be incomplete. All of the fields in your reports must be complete and accurate.

We review the quality of your reports by considering all of the fields, including those that are mandatory, mandatory if applicable, and reasonable measures fields.

When reasonable measure fields are left blank, we will examine your records to see if you had the information at the time of the transaction. If you did have the information but did not include it in the report, as required, we will ask you to explain why.

We assess the information reported in Part G, "Description of Suspicious Activity" of Suspicious Transaction Reports to verify that there is an adequate description of the reasonable grounds to suspect that the reported transaction(s),

or attempted transaction(s), were related to the commission, or attempted commission, of a money laundering offence or a terrorist activity financing offence.

In Terrorist Property Reports, we verify that information about the property and the persons or groups that own or control it, and information about transactions or attempted transactions related to the property, has been provided.

(All report types 6) Ensuring that your third party service provider reports correctly

When you use a third-party service provider to submit reports on your behalf, we verify that the reports list the correct identification information, such as your business name, phone number and location, not the identification information of the service provider.

We examine your records of transactions to identify the ones that should have been reported, and then verify that the service provider sent us the reports with the correct identification information. If we cannot find the reports in our database under the name of your business, we will seek to determine if your service provider used the wrong identification information when it sent the reports to FINTRAC or if the reports were not submitted.

Timing testing (All report types 7) Ensuring that you are sending reports on time

We assess whether you are submitting reports within the timelines set out in the PCMLTFA and associated Regulations, and as described in FINTRAC guidance. We may review the reports you submitted and compare them to your transaction records to confirm that the reports were sent on time.

3.3.2. Large Cash Transaction Reports (LCTRs) We use methods described in this section to assess your compliance with requirements relating to Large Cash Transaction Reports.

(LCTR 1) Confirming you are submitting LCTRs (Applicable to all business sectors)

We ask you to provide us with a list of your cash transactions or records of transactions of $10,000 or more, or both, including transaction and client identification information, so that we can compare the transactions with your reporting. If we cannot find a report for a given transaction, we will enquire into the reasons behind this discrepancy.

To be clear, we do not require a list of the Large Cash Transaction Reports you or your third-party service provider have submitted; we already have these reports in our database. What we require is a list that includes the information about your large cash transactions, one that comes directly from your business records or the systems that you or your third-party service provider may have used to gather the information to submit Large Cash Transaction Reports. We

may ask you to send us a sample of this list before requesting the complete list in order to verify that it is in the format that we need.

If you do not have an automated system that can extract the information and produce a list, you will need to provide the records of the transactions. These could be deposit slips, invoices, sales receipts, receipt books, foreign currency exchange transaction tickets, pit logs (casino sector), records of player buy-ins (casino sector), etc.

(LCTR 2) Confirming you are correctly applying the 24-hour rule to LCTRs (Applicable to all business sectors)

We review your policies and procedures, records of transactions, internal records and reports and other documents to identify how you treat cash transactions of less than $10,000 conducted by, or on behalf of, the same person or entity, that, when combined, total $10,000 or more within a 24-hour period. We confirm that you combine these transactions and send us the required Large Cash Transaction Reports when the transactions were made within 24 consecutive hours.

We also verify that you send us separate Large Cash Transaction Reports for lump-sum cash transactions of $10,000 or more, and that you do not combine these with cash transactions of less than $10,000 conducted within a 24-hour period.

(LCTR 3) Confirming that you are submitting all the required reports for a given transaction (Applicable to financial entities, casinos and money services businesses)

We review your records to verify that you have submitted a Large Cash Transaction Report **and** an Electronic Funds Transfer Report when you have received $10,000 or more in cash from, or on behalf of, the same person or entity, in a lump sum or over a 24-hour period, for the purpose of initiating an outgoing international electronic funds transfer of $10,000 or more. We look at your transaction records or the Large Cash Transaction Reports in which you indicated that the disposition of funds was through an "outgoing electronic funds transfer". We may ask you to provide the report numbers for the Electronic Funds Transfer Reports and the Large Cash Transaction Reports to confirm that both types of reports were submitted to FINTRAC.

(LCTR 4) Reviewing exceptions to submitting LCTRs Exception—Alternative to large cash transactions

(Applicable to financial entities)

If a financial entity has used the alternative to submitting Large Cash Transaction Reports, as permitted under the PCMLTFA and associated Regulations and as described in our guidance, we verify that all of the conditions associated with this exception were respected. We confirm that you submitted, within the

prescribed timeframe, a complete and accurate Financial Entity Business Client Report that includes a list of all the clients to which the exception has been applied. If you continue to apply the alternative to a client who no longer meets the prescribed conditions, we will review the client's cash transactions to determine whether Large Cash Transaction Reports should have been submitted to FINTRAC.

Exception—Cash received from financial entities or public bodies or from a person who is acting on behalf of a client that is a financial entity or public body

(Applicable to all business sectors)

If you did not send us Large Cash Transaction Reports for clients who are financial entities, public bodies, or a person who is acting on behalf of a client that is financial entity or public body as the law permits, we will verify that the clients are financial entities or public bodies as defined in the PCMLTFA and associated Regulations. If they do not meet the definition, we may review the client's cash transaction history to determine if there are Large Cash Transaction Reports that should have been submitted to FINTRAC.

3.3.3. Large Virtual Currency Transaction Reports (LVCTRs) We use the methods described in this section to assess your compliance with the requirements relating to Large Virtual Currency Transaction Reports.

(LVCTR 1) Confirming you are submitting LVCTRs (Applicable to all business sectors)

We ask you to provide us with a list of your virtual currency transactions or records of virtual currency transactions of $10,000 or more, or both, including transaction and client identification information, so that we can compare the transactions with your reporting. If we cannot find a report for a given transaction, we will enquire into the reasons behind this discrepancy.

To be clear, we do not require a list of the Large Virtual Currency Transaction Reports you or your third-party service provider have submitted; we already have these reports in our database. What we require is a list that includes the information about your large virtual currency transactions, one that comes directly from your business records or the systems that you or your third-party service provider may have used to gather the information to submit Large Virtual Currency Transaction Reports. We may ask you to send us a sample of this list before requesting the complete list in order to verify that it is in the format that we need.

If you do not have an automated system that can extract the information and produce a list, you will need to provide the records of the transactions. These could be virtual currency exchange transaction tickets, deposit slips, invoices,

sales receipts, receipt books, foreign currency exchange transaction tickets, pit logs (casino sector), records of player buy-ins (casino sector), etc.

(LVCTR 2) Confirming you are correctly applying the 24-hour rule to LVCTRs (Applicable to all business sectors)

We review your policies and procedures, records of transactions, internal records and reports, and other documents to identify how you treat virtual currency transactions that total $10,000 or more within 24 consecutive hours, and that are conducted by, or on behalf of, the same person or entity, or when the amounts are for the same beneficiary. We confirm that you combine these virtual currency transactions and send us the required Large Virtual Currency Transaction Reports when the transactions were made within 24 consecutive hours.

(LVCTR 3) Confirming that you are submitting all the required reports for a given transaction (Applicable to financial entities, casinos, money services businesses and foreign money services businesses)

We review your records to verify that you have submitted a Large Virtual Currency Transaction Report **and** an Electronic Funds Transfer Report when you have received $10,000 or more in virtual currency, in a deemed single transaction, for the purpose of initiating an outgoing international electronic funds transfer of $10,000 or more. We look at your transaction records or the Large Virtual Currency Transaction Reports in which you indicated that the disposition of funds was an "outgoing international electronic funds transfer". We may ask you to provide the relevant report numbers to confirm that both types of reports were submitted to FINTRAC.

3.3.4. International Electronic Funds Transfer Reports (EFTRs) (Applicable to financial entities, casinos, money services businesses and foreign money services businesses)

We use methods described in this section to assess your compliance with the requirements relating to Electronic Funds Transfer Reports.

(EFTR 1) Confirming that you are submitting EFTRs We ask you to provide us with a list of your international electronic funds transfers of $10,000 or more, including transaction and client information, when you are the initiator or final receiver of the international electronic funds transfer, so that we can compare the transactions with your reporting. If we cannot find a report for a given transaction, we will enquire into the reasons behind this discrepancy.

To be clear, we do not require a list of the Electronic Funds Transfer Reports that you or your third-party service provider have submitted; we already have these reports in our database. What we require is a list that includes the information about your international electronic funds transfer transactions, one that comes

directly from your business records or the systems you or your third-party service provider may have used to submit Electronic Fund Transfer Reports. We may ask you to send us a sample of this list before requesting the complete list in order to verify that it is in the format that we need.

If you do not have an automated system that can extract the information and produce a list, you will need to provide the records of the transactions. These could be transfer slips, wire logs, foreign currency exchange transaction tickets, invoices, etc.

(EFTR 2) Confirming that you are applying the 24-hour rule to EFTRs We review your policies and procedures, records of transactions, internal records and reports and other documents to identify how you treat international electronic funds transfers of less than $10,000 conducted by, or on behalf of, the same person or entity, that, when combined, total $10,000 or more within a 24-hour period. We then confirm that you combine these transactions and send us the required Electronic Funds Transfer Reports.

We verify that you send us separate Electronic Funds Transfer Reports for lump-sum international transfers of $10,000 or more, and that you do not combine these with international electronic funds transfers of less than $10,000 conducted within a 24-hour period.

We also verify that you do not combine incoming international electronic funds transfers with outgoing international electronic funds transfers. In addition, for outgoing international electronic funds transfers, we verify that you combine transactions correctly when applying the 24-hour rule for transactions conducted by, or on behalf of, the same client. We also ensure you correctly combine incoming international electronic funds transfers.

(EFTR 3) Confirming that you are submitting all the required reports for a given transaction (Applicable to financial entities, casinos, money services businesses and foreign money services businesses)

We review your records to verify that you have submitted a Large Cash Transaction Report **and** an Electronic Funds Transfer Report when you have received $10,000 or more in cash, in a deemed single transaction, for the purpose of initiating an outgoing international electronic funds transfers of $10,000 or more. We look at your transaction records or the Large Cash Transaction Reports in which you have indicated that the disposition of funds was an "outgoing electronic funds transfer". We may ask you to provide the relevant report numbers to confirm that both types of reports were submitted to FINTRAC.

Assessment methods LCTR 3, LVCTR 3 and EFTR 3 are identical and are repeated for ease of reference.

3.3.5. Casino Disbursement Reports (CDRs) (Applicable to casinos)

We use the methods described in this section to assess your compliance with the requirements related to Casino Disbursement Reports.

(CDR 1) Confirming that you are submitting CDRs For this test, we ask you to provide us with a list of your casino disbursement records of $10,000 or more, including transaction and client information, so we can compare the transactions with your reporting. If we cannot find a report for a given transaction, we will enquire into the reason behind this discrepancy.

To be clear, we do not require a list of the Casino Disbursement Reports that you or your third-party service provider have submitted; we already have these reports in our database. What we require is a list that includes the information about your cash disbursements, one that comes directly from your business records or systems. We may ask you to send us a sample of this list before requesting the complete list, in order to verify that it is in the format we need.

If you do not have an automated system that can extract the information and produce a list, you will need to provide records of the disbursements. These could be cheque registers, player tracking sheets, transaction logs, etc.

(CDR 2) Confirming that you are applying the 24-hour rule to CDRs We review your policies and procedures, records of transactions, internal records and reports and other documents to identify how you treat disbursements of less than $10,000 received by, or on behalf of, the same client, that, when combined total $10,000 or more, within a 24-hour period. We confirm that you combine these transactions and send us the required Casino Disbursement Reports.

We also confirm that you send us separate Casino Disbursement Reports for lump-sum disbursements of $10,000 or more and that you do not combine these with disbursements of less than $10,000 conducted within a 24-hour period.

3.3.6. Suspicious Transaction Reports (STR) (Applicable to all business sectors, with the exception of STR 13, STR 14 and STR 15)

We use the methods described in this section to assess your compliance with Suspicious Transaction Report requirements.

Suspicious Transaction Reports are of significant intelligence value to FINTRAC as they are the cornerstone of the Centre's mandate to detect, deter and prevent money laundering and terrorist activity financing. Suspicious Transaction Reports, and other reports, enable the Centre to conduct analysis and produce actionable financial intelligence, which it discloses to police, law enforcement and national security agencies when prescribed thresholds are met.

Most of the assessment methods described in this section are based on money laundering and terrorist activity financing indicators published in FINTRAC guidance and other well-known reliable sources, such as the Financial Action Task Force (FATF).

The assessment methods for Suspicious Transaction Reports serve to evaluate how you address suspicious transactions, as well as other requirements. We use them to:

- Assess your compliance with other requirements, such as the risk assessment, special measures, and ongoing monitoring requirements;
- Verify that you identify money laundering and terrorist activity financing indicators, as well as transactions that may give rise to reasonable grounds to suspect that the transactions, or attempted transactions, are related to the commission or attempted commission of a money laundering offence or terrorist activity financing offence;
- Verify that you have a sound escalation and decision-making process for suspicious transactions;
- Verify that all relevant business areas receive key information regarding suspicious transaction activity; and
- Verify that you are sending us Suspicious Transaction Reports when required.

When assessing the information we gather through the application of these methods, we will use the approach described in Part 1 to arrive at our conclusions. We will evaluate the body of information and the totality of the circumstances and take a holistic and reasonable approach when arriving at our conclusions.

We use monitoring and unusual transactions testing, testing of high-risk areas, money laundering and terrorist activity financing indicator testing, external information testing, comparison testing, transaction reversal and relationship termination testing, and business sector specific testing.

The methods described in this section apply to both completed and attempted suspicious transactions. Assessment methods relating to the quality and timing of reports can be found in section 3.3.1 (all reports types).

Monitoring and unusual transaction testing (STRs) In this section, the words "alerts" and "unusual transactions" refer to completed or attempted transactions that have been identified or flagged as part of your internal monitoring process because they may be related to money laundering or terrorist activity financing. Alerts and unusual transactions should be further assessed in keeping with your policies and procedures and could eventually lead to a Suspicious Transaction Report.

(STR 1) Reviewing your policies and procedures on how you monitor activities and transactions

We review your policies and procedures to confirm that you have a monitoring process that enables you to detect, assess and, when required, report suspicious transactions related to money laundering and terrorist activity financing. If you use generic policies and procedures developed by an industry group or consultant, we verify that you have adapted these policies and procedures to your

business, including monitoring procedures.

We may ask questions such as:

- Is your monitoring process automated, manual or both?
- How are you alerted to, or informed of, unusual transactions, and how do you prioritize and action these?
- When you receive an alert, what process do you follow to identify, assess, and make a decision about the unusual transaction and, when required, report the transaction to FINTRAC?
- How often do you review your transaction monitoring process to make sure it remains in line with your risk assessment, and policies and procedures?

(STR 2) Reviewing your monitoring rules

We review the automated and manual monitoring rules that you have put in place to confirm that they help you detect unusual transactions and provide alerts on potentially suspicious transactions. When we review your rules, we confirm that they are reasonable, put into practice, and that they monitor transactions in keeping with your risk assessment. We may also ask you how often you adjust the rules, what would cause you to adjust them, what steps you take to do so, and how you document these adjustments. We may verify whether you periodically review your rules, to confirm that you are not overlooking potentially suspicious transactions.

(STR 3) Reviewing unusual transactions

We review the unusual transactions identified by your monitoring system that you did not report to confirm that your decisions were sound.

We look into whether you use a risk-based approach to identify unusual transactions and generate alerts, so that you can direct more of your time and effort to areas of higher risks of money laundering and terrorist activity financing. For example, you may place more importance on transactions that present two or more money laundering or terrorist activity financing indicators.

If you do use a risk-based approach to manage unusual transactions, we will determine if your approach is reasonable. To do this, we will assess:

- If you have sufficient resources to monitor and review transactions based on the size of your business and its transaction volume.
- If you have a reasonable rationale to support the thresholds placed on the monitoring rules and unusual transactions.
- How often you monitor and action unusual transactions that pose a lower risk.

Testing high-risk areas (STR) (STR 4) Reviewing your high-risk areas

We review client records and transaction records related to the high-risk areas identified in your risk assessment, such as high-risk clients, high-risk delivery

channels, or high-risk jurisdictions. We may also review a sample of client records and transaction records for areas you did not determine to pose a high risk to ensure no gaps exist in your risk assessment or reporting procedures.

Money laundering and terrorist activity financing indicator testing (STR) (STR 5) Identifying indicators consistently

We ensure that you are applying your money laundering or terrorist activity financing indicators in a consistent manner when submitting Suspicious Transaction Reports. We first review Part G of the reports you have submitted to identify the most common indicators listed. We then verify your records to assess whether you continue to submit suspicious transaction reports when these common indicators are present in other transactions, and there are reasonable grounds to suspect that the transactions are potentially related to money laundering or terrorist activity financing. If we identify suspicious transactions that were not reported, we will prioritize transactions that would have given FINTRAC new information for analysis.

(STR 6) Reviewing transactions for money laundering and terrorist activity financing indicators

As part of our risk assessment of your business, we identify money laundering and terrorist activity financing indicators that you may come across in the course of your business. We verify that these indicators inform your compliance program and support your efforts to detect, assess, and report suspicious transactions. Should we detect transactions that reflect these indicators in our review of your client records and transaction records, we will look into the actions you took to determine whether they were reasonable.

In addition, while we recognize that you may prioritize certain indicators over others, we verify that your processes and systems do not overlook suspicious behaviour.

External information testing (STR) (STR 7) Reviewing how you use publicly available information

We look at how you use publicly available information as part of your risk assessment, monitoring and Suspicious Transaction Report processes. Publicly available information includes news releases issued by industry regulators, police and other law enforcement agencies, mainstream news media, and other credible sources. We assess whether you take reasonable steps when you discover something of interest about a client. We will enquire about your reasons for not acting upon publicly available information.

(STR 8) Reviewing how you process information from credible sources

We verify how you use information received from police, law enforcement and national security agencies, and regulatory or supervisory bodies, related to money laundering and terrorist activity financing, to inform your compliance program.

This information could include production orders, comfort letters, alerts and internal referrals. Specifically, we look at how you use this information to identify potential high-risk clients, take measures to reduce the risk related to these clients, and submit Suspicious Transaction Reports when required. We verify that the information is forwarded to your compliance officer or your compliance department when it is addressed to a different person or department.

FINTRAC will not ask to see sealed production orders nor those that include an order of non-disclosure.

Comparison testing (STR) (STR 9) Verifying variances in actual versus expected transactional behaviour

We verify whether you detect when a client's transactions differ noticeably from what is expected and that you take action. We may review the client records and transaction records of clients whose transactions noticeably differ from those of similar clients. For example, a client may conduct more transactions or transactions of higher value than what is expected when compared to a group of similar clients.

(STR 10) Detecting unusual patterns

We review your client records of transactions for unusual patterns or connections that we determine meet the reasonable grounds to suspect threshold and should be reported. For example, we may look for:

- Clients who appear unrelated but have the same address or phone numbers.
- Clients who are in school or unemployed and conducting high-value transactions.
- People without any apparent relation making deposits into the same account.

When we search for patterns or connections, we look through your electronic or paper records, as well as through the reports you sent us. We also ask if you look for such patterns or connections and how you do so.

Transaction reversal and relationship termination testing (STR) (STR 11) Reviewing your refunds, cancellations and overpayments

We review records of transactions where a refund cheque was issued because a customer returned an item, cancelled a life insurance policy, terminated a service, cancelled a real estate transaction, or overpaid for transactions. These situations may represent common money laundering and terrorist activity financing indicators, and as such, we review your procedures to ensure that you are adequately assessing these situations and taking the necessary measures, as applicable.

(STR 12) Reviewing how you end relationships with clients and agents

The PCMLTFA and associated Regulations do not require you to end business relationships. That decision remains yours to make. However, if you decide to end a relationship with a client or an agent because of concerns related to money laundering or terrorist activity financing, we verify that you continue to monitor their transactions for possible suspicious transactions, and take steps to mitigate risks, until the relationship is officially ended.

Business-sector-specific testing (STR) The Suspicious Transaction Report assessment methods described above are applicable to most business sectors. However, some sectors have characteristics that require specific testing.

(STR 13) Real estate: Reviewing how you use market values and local market conditions

(Applicable to real estate)

We verify that you detect purchase or sale transactions that are noticeably below or above the expected market value, based on local market conditions, to determine whether the transaction is suspicious. Real estate values and market conditions vary across Canada based on location, the economic cycle and other factors. We assess whether you are aware of these market conditions and that you identify transactions that are well outside their expected or average market value.

(STR 14) Real estate: Reviewing deals with last-minute changes in ownership

(Applicable to real estate)

We review transaction records, including client records, receipt of funds records, bank drafts and third party determination records where there are unexplained or last-minute substitutions of the buyer. We assess whether you have identified these cases as needing further review and assessment for possible layering or hiding of the true ownership, or that the original purchaser may be instructed by a third party until the property is assigned.

(STR 15) Casino: Reviewing your issued cheques for unusual buy-ins or disbursements

(Applicable to casinos)

We review the cheques you issued to clients to identify unusual buy-ins or disbursements that may indicate an attempt to layer proceeds of crime. We first ask you to explain how you identify unusual buy-ins or disbursements, reduce potential risks, monitor the transactions, and decide whether to submit a Suspicious Transaction Report.

Then, we may ask you for a list of the clients you have issued cheques to, so that we can identify irregularities, such as clients who may have received more cheques than what would usually be seen. If we do identify irregularities,

we ask for the client history information and look for suspicious buy-ins or disbursements that should have been reported.

3.3.7 Terrorist Property Report (TPRs) We use the methods described in this section to assess your compliance with Terrorist Property Report requirements.

(TPR 1) Reviewing your correspondence with authorities (Applicable as indicated below)

We review:

- For all business sectors, correspondence with the Royal Canadian Mounted Police (RCMP) or the Canadian Security Intelligence Service (CSIS) in which you indicated that you are in possession or in control of property owned or controlled by, or on behalf of, a terrorist, terrorist group, or listed person.
- The reports that financial entities, life insurance companies, and securities dealers are required to submit under the Criminal Code or the Regulations Implementing the United Nations Resolution on the Suppression of Terrorism. These reports are sent to provincial or federal regulators, in which the business indicated being in possession or control of property owned or controlled by, or on behalf of, a listed entity or listed person.

If you have disclosed that you are in possession of such property, we confirm that you sent us a Terrorist Property Report. We also verify that the information in the Terrorist Property Report is consistent with the information you sent the RCMP, CSIS, and your regulator (if applicable).

(TPR 2) Verifying lists for terrorist or terrorist groups and listed persons (Applicable to all business sectors)

We confirm the steps you take to determine whether your business possesses or controls the property of a terrorist, terrorist group or listed person, and submit a Terrorist Property Report. If you are, or were, in possession or control of such property, we verify that you sent us a Terrorist Property Report.

We may assess how you handle situations where you cannot determine, based on the information you have, if you are dealing with a terrorist, terrorist group or listed person.

Whether you cannot file a Terrorist Property Report because you cannot make the necessary determination, or whether you are able to file a Terrorist Property Report, we verify that you send us Suspicious Transaction Reports when required. The added information in the Suspicious Transaction Report may prove valuable to FINTRAC in its intelligence work.

We may compare your clients' names against the list published in the Regulations Establishing a List of Entities issued under the Criminal Code and the list

published in the Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism. If one of your clients is on either list, we verify that you submitted a Terrorist Property Report.

3.4. Record keeping requirements

(Applicable to all business sectors)

We use the methods described in this section to assess your compliance with record keeping requirements.

To conduct this assessment, we may

- Review your policies and procedures to confirm that they give enough guidance to your employees or agents to meet the record keeping requirements.
- Review your client records and records of transactions to confirm that you put these policies and procedures into practice.
- Verify that you keep records as required by the PCMLTFA and associated Regulations when reviewing your client records and transaction records.
- Records may include the following, as applicable:
  - account opening records;
  - credit card account and transaction records;
  - prepaid payment product account and transaction records;
  - records of large cash transactions or large virtual currency transactions
  - records of electronic funds transfer or virtual currency transfer transactions;
  - records of casino disbursements;
  - foreign currency exchange or virtual currency exchange transaction tickets;
  - information records;
  - records that you are required to keep under client identification and know your client requirements; and
  - copies of reports submitted to FINTRAC
- Verify that you keep the information that is required (for example, name, address, date of transaction, etc.) for each type of record. The information that you are required to keep is determined by the type of record that needs to be kept.
- Verify that your records are kept in a format that can be produced within 30 calendar days of a request, and confirm that you keep the records for five years, or as long as required by the PCMLTFA and associated Regulations.
- Interview your employees and agents to assess their knowledge of record keeping requirements.

Our focus While we assess record keeping, we will focus on ensuring that you accurately record information that identifies persons and entities that open or control accounts, and conduct or direct transactions.

3.5. Correspondent banking relationship requirements

(Applicable to financial entities)

We use the methods described in this section to assess your compliance with correspondent banking relationships requirements.

To conduct this assessment, we may:

- Review your policies and procedures to confirm that they provide enough guidance for your employees or agents.
- Review your records, including records of transactions to confirm that your policies and procedures are put into practice.
- Review your records of transactions to confirm that you, as applicable:
  - take all required measures as per the PCMLTFA and associated Regulations—described in FINTRAC guidance;
  - do not deal with a shell bank;
  - obtain the required approvals;
  - identify your clients, when required;
  - obtain and keep records of required information;
  - risk assess the relationship;
  - take special measures, when required; and
  - meet the requirements within the prescribed timeframes.
- Interview your employees and agents to assess their knowledge of correspondent banking requirements.

When we evaluate your risk assessment, we may:

- Verify whether you have considered correspondent banking relationship risks such as the correspondent bank's location, corporate structure, profile and reputation, clientele, products and services, type and volume of activity, openness to sharing information as needed, and regulatory history.
- Review your record of the correspondent bank's anticipated account activity, including products or services. We may ask if, and how, you use this information to review the transactions conducted through your correspondent banking accounts in order to determine whether there are transactions or attempted transactions that deviate from the terms of your agreement. We may also review the records of transactions to this end.

If your policies and procedures allow for:

- Payable-through accounts: we verify that you take reasonable measures to confirm that the correspondent bank identifies its clients who have direct access to your correspondent banking services in a manner that is

consistent with Canadian client identification requirements and that it has agreed to provide you with relevant client identification data upon request;
- Nested accounts: as a best practice, we may review the information that you have about the downstream bank and the controls you have implemented to mitigate risk and monitor the transactions conducted by the downstream banks and their clients.

If your policies and procedures prohibit payable-through accounts and nested accounts, we will ensure you have the appropriate controls in place to detect transactions involving these types of accounts and, if detected, that you have taken remedial action in keeping with your policies and procedures.

As part of our assessment, we may also:

- Verify that you update information regarding your correspondent banking relationship, the type of information that you update, and how often you update it.
- Verify that you have disclosed all your correspondent relationships to us, which may include a review of your records of transactions to confirm.
- Review your process to end a correspondent banking relationship because of money laundering or terrorist activity financing concerns.

Our focus We will focus on the steps you take to ensure that senior management has approved your correspondent banking relationships and is aware of the risks involved.

We will also focus on the steps you take to ensure that you are not dealing with a shell bank. Shell banks operate outside the country where they are incorporated and licensed; they are not affiliated to a financial services group that is supervised in that country. Shell banks pose a serious risk to the Canadian anti-money laundering and anti-terrorism financing regime because of the difficulty that exists in ensuring regulatory oversight for requirements such as customer due diligence and risk mitigation measures.

3.6. Foreign branches, foreign subsidiaries and affiliates requirements

(Applicable to financial entities, securities dealers, and life insurance)

We use the methods described in this section to assess your compliance with requirements relating to foreign branches, foreign subsidiaries and affiliates.

Foreign branches and foreign subsidiaries Information on requirements relating to foreign branches and foreign subsidiaries is available in our guidance.

To conduct this assessment, we may:

- Review the policies and procedures that you developed for your foreign branches and foreign subsidiaries to ensure that they are adequate, and reflect Canadian obligations when it comes to:

  - the establishment and implementation of a compliance program, including policies and procedures to evaluate the risk of money laundering and terrorist activity financing and risk mitigation measures when risk is considered high;
  - record keeping and retention; and
  - client identification.
- Confirm that the Board of Directors (if you have one) has approved these policies and procedures before they are put into practice.
- Review your client records and transaction records to confirm that your foreign branches and foreign subsidiaries apply these policies and procedures to the extent permitted by the laws of the country where the branch or subsidiary is located. If the policies and procedures conflict with local laws, we may ask you for the reason of the conflict and whether you have informed FINTRAC and your primary regulator of this issue, and have considered how you plan to mitigate any associated risks.
- Confirm how you ensure that your foreign branches and foreign subsidiaries are implementing the policies and procedures.

Domestic and foreign affiliates Information on requirements relating to affiliates is available in our guidance.

To conduct this assessment, we may confirm that you have adequate policies and procedures in place to share information with your affiliates for the purpose of assessing the risk of money laundering and terrorist activity financing, and detecting and deterring such offences.

As part of our evaluation of your risk assessment, we may:

- Verify that you have assessed the risk of money laundering and terrorist activity financing for all of your foreign and domestic affiliates. This includes verifying that you have implemented measures to reduce risks should foreign affiliates be located in higher-risk countries.
- Ask you how you use information from affiliates about suspicious activities or transactions in your compliance program.

Our focus We will focus on whether, as described, your foreign branches and foreign subsidiaries have policies and procedures in place and whether you have policies and procedures in place to share information with your affiliates.

3.7. Money services business (MSB), and Foreign money services business (FMSB) registration requirements

(Applicable to money services businesses and foreign money services businesses)

We use the methods described in this section to assess your compliance with money services business and foreign money services business registration requirements.

We verify that you keep registration information up to date, respond to clarification requests, renew your registration, and cancel your registration (if applicable).

To conduct this assessment, we may:

- Review your policies and procedures to confirm that they give enough guidance to your employees or agents to meet the requirements relating to money services business and foreign money services business registration.
- Review your client records and transaction records to confirm that the information provided to FINTRAC is accurate and that your policies and procedures are put into practice.
- Interview your employees and agents to assess their knowledge of the registration requirements.

Our focus We will focus on ensuring that your registration information is accurate and up to date.

3.8. Ministerial directives' requirements

(Applicable to all business sectors)

We use the methods described in this section to assess your compliance with requirements relating to ministerial directives.

The instructions provided in each ministerial directive will vary and, as such, our assessment will focus on the essence of the directive.

To conduct this assessment, we may:

- Review your policies and procedures to confirm that they give enough guidance to your employees or agents to meet the ministerial directive requirements.
- Verify that your policies and procedures clarify what ministerial directives are and where they can be found. We may also look to see whether your policies and procedures indicate how often you should check for new, updated or amended directives; who should be informed when a directive is applicable to your business; and what steps to take to make sure the directive is being followed.
- Review your client records and transaction records to confirm that you put the policies and procedures into practice.
- Verify that you have taken action when directives are applicable through our review of your client records and transaction records. These records may include:
  - the verification of the identity of a person or an entity;
  - the exercise of customer due diligence, including ascertaining the source of funds of a financial transaction, the purpose of a financial transaction or the beneficial ownership or control of an entity;
  - monitoring financial transaction for an account;

  - keeping records;
  - reporting financial transactions to FINTRAC; and
  - complying with other requirements of the PCMLTFA and associated Regulations.
- Interview your employees and agents to assess their knowledge of the requirements relating to ministerial directives.
- Verify that your business, including foreign branches and subsidiaries (if applicable), follows the directives.

When a foreign branch or foreign subsidiary cannot comply with a directive because it conflicts with local laws, we may:

- Review your records to verify that you obtained documents to confirm the conflict.
- Verify that you informed FINTRAC of the reasons for the conflict and, as applicable, the principal agency or body that supervises or regulates your business under federal or provincial law within a reasonable period.
- Ask about the measures you put in place to reduce the risks.

When you conduct business in a foreign jurisdiction or with a foreign entity named in a ministerial directive, we may:

- Verify that your risk assessment considers the parameters of the ministerial directive.
- Verify that you apply the processes that you have in place to manage high-risk transactions associated with ministerial directives, including monitoring the transactions more frequently, applying special measures, and submitting Suspicious Transaction Reports when required.

Our focus We will focus on determining whether you are adequately implementing ministerial directives.

Guide on harm done assessment for violations of other compliance measures

1. Introduction

This page presents how we assess the harm done and calculate the base penalty amount applied to violations of requirements related to correspondent banking, foreign branches and subsidiaries, complying with the Minister's Directive, prescribed information in prescribed electronic funds transfers (travel rule), and providing assistance or information reasonably required to FINTRAC.

1.1 Purpose of the guide

This guide presents how FINTRAC approaches the harm done criterion and the base penalty amount for violations under the *Proceeds of Crime (Money*

Laundering) and Terrorist Financing Act (the Act) and its regulations. According to section 73.11 of the Act, FINTRAC must consider the harm done by a violation, that the purpose of an administrative monetary penalty (AMP) is to encourage compliance rather than to punish, and all other criteria prescribed in the regulations, including a reporting entity's (RE) history of compliance, when determining the amount of a penalty. Considerations for the non-punitive nature of an AMP and an REs' compliance history are assessed in another step in the penalty calculation and are outlined separately in FINTRAC's AMP policy.

1.2 Definition of harm

FINTRAC defines "harm" as the degree to which a violation interferes with achieving the objectives of the ActFootnote 1 or with FINTRAC's ability to carry out its mandateFootnote 2. Therefore, the consequences of non-compliance, when an AMP is imposed, are linked to its effects on Canada's efforts to combat money laundering and terrorist activity financing (ML/TF).

Compliance enforcement activities are undertaken to prevent and correct the harm that comes from non-compliance with the Act and regulations. REs' adherence to requirements such as record keeping and verifying client identity assists in the deterrence of ML/TF and supports investigations and criminal prosecutions. The requirements related to reporting ensure that FINTRAC is supplied with the high-quality, timely financial transaction reports it needs to produce the financial intelligence that helps with the investigation and prosecution of ML/TF offences.

1.3 Considering harm in AMP calculations

When determining a penalty, FINTRAC considers the harm caused, that is, the degree to which the non-compliance interferes with the purpose of the Act and/or with FINTRAC's mandate. Non-compliance and harm are measured using the standards described in this guide, which outline the benchmark amounts for the corresponding levels of harm for a specific violation. FINTRAC considers the specific circumstances of each case, including the extent of the non-compliance and mitigating factors, which may further reduce the actual amounts applied.

2. Violations related to other compliance measures

Compliance measures related to correspondent banking, foreign branches and subsidiaries, minister's directives, prescribed information in electronic funds transfers (EFTs) and assistance to the Centre have been put in place to strengthen Canada's Anti-Money Laundering and Anti-Terrorism Financing (AML/ATF) regime. In particular, measures related to correspondent banking, foreign branches and subsidiaries, and minister's directives help to achieve the objectives set out in subsections 3(c) and 3(d) of the Act concerning Canada's international commitment to fight transnational crime, especially ML/TF.

These measures also strengthen Canada's ability to take targeted steps to protect Canada's financial system. Measures concerning prescribed information in EFTs help eliminate anonymous transactions and ensure that transaction information is made available for compliance, risk assessment, analysis, investigations and prosecutions. Finally, measures concerning assistance to FINTRAC are in place so that we can ensure REs comply with the requirements of the Act and its regulations. If an RE fails to meet these requirements, it interferes with the regime's ability to achieve the objectives of the Act and FINTRAC's mandate, which is to detect, prevent and deter ML/TF.

3. Violations related to complying with a Minister's directive

In order to safeguard the integrity of Canada's financial system, the Minister of Finance has the authority to issue directives to REs and their foreign branches and subsidiaries, in respect of a designated foreign jurisdiction or entity. A directive allows the Minister to require that specific measures be carried out beyond those of the Act and its regulations when a foreign jurisdiction or entity is at a heightened risk of facilitating ML/TF. These additional, targeted measures are designed to enhance existing requirements to mitigate the specific ML/TF risks of financial transactions originating from or destined to foreign jurisdictions or entities with ineffective or insufficient AML/ATF measures. These additional, targeted measures may help avoid an adverse impact on the integrity of Canada's financial system or on its reputation.

Provision of the Act	Description	Classification of violation
11.43	Failure to comply with a ministerial directive	Very serious$1-$500,000
11.44(1)	Failure to ensure that a foreign branch or foreign subsidiary complies with a ministerial directive	Very serious$1-$500,000

Table 1—Violations related to complying with a Minister's directive

3.1 Harm done in the case violations related to complying with a Minister's directive

Failing to comply with a Minister's directive could interfere with the achievement of the objectives described under paragraphs 3(c) and (d) of the Act with respect to fulfilling Canada's international commitments to fight transnational crime, particularly ML/TF, and enhancing Canada's targeted measures to protect its financial system from ML/TF. Non-compliance with a minister's direc-

tive poses a very high risk to the integrity of Canada's financial system and the safety of Canadians. This is because detection and mitigation measures would not be applied to transactions originating from or destined to a foreign state or a foreign entity that has an ineffective or insufficient AML/ATF regime. In a worst case scenario, suspicious transactions related to ML or TF offences could remain undetected, posing a risk to the financial system and the safety of Canadians.

3.2 Penalty determination for violations related to complying with a Minister's directive

When an RE or its foreign branches or subsidiaries fail to comply with a minister's directive, Canada's financial system is at risk to be used for international ML/TF transactions. The prescribed maximum penalty of $500,000 is applied when a directive is not implemented because ministerial directive violations pose the greatest harm to the achievement of the objectives of the Act and FINTRAC's mandate.

The measures required by a Minister's directive vary, therefore, the penalty determination criteria for partial violations is dependent on the contraventions and the extent of the non-compliance. FINTRAC will consider the circumstances of each case to determine if there are mitigating factors that may reduce the penalty amount.

4. Violations related to correspondent banking

This section outlines FINTRAC's approach to the violations related to correspondent banking requirements, including harm assessments and penalty calculations.

4.1 Violation for having a correspondent banking relationship with a shell bank

Removing anonymity in transactions is one of the most important safeguards against the exploitation of Canada's financial system for ML/TF. Financial entities in Canada are specifically prohibited from having correspondent banking relationships with shell banks because this could facilitate anonymity in transactions and give little or no AML/ATF oversight.

Provision of the Act	Description	Classification of violation
9.4(2)	Having a correspondent banking relationship with a shell bank	Serious$1-$100,000

Table 2—Violation for having a correspondent banking relationship with a shell bank

4.1.1 Harm done in the case of a violation related to having a correspondent banking relationship with a shell bank Shell banks operate outside the country where they are incorporated and licensed, and are not affiliated with a financial services group that is subject to supervision in that country. The control and management of a shell bank happens from a different jurisdiction, sometimes from a private residence, and poses a serious risk to Canada's AML/ATF regime as it is difficult to ensure regulatory oversight for requirements such as customer due diligence and risk mitigation. The banking supervisor in the country where the shell bank operates is generally unaware of its existence. Shell banks pose a higher risk of ML/TF and they are known for being used to launder the proceeds of crime. If a financial entity in Canada were to allow a shell bank to access to Canada's financial system, this could interfere with the detection, prevention and deterrence of ML/TF activities here, and could also interfere with the achievement of one of the objectives set out in paragraph 3(c), of the Act which is to assist in fulfilling Canada's international commitments to participate in the fight against transnational crime, particularly money laundering, and the fight against terrorist activity.

4.1.2 Penalty determination for a violation related to having a correspondent banking relationship with a shell bank When an RE provides financial services to a shell bank, the RE provides the shell bank with broad access to the Canadian financial system, putting it at risk for ML/TF because of the anonymity the shell bank entails. An RE that has a correspondent banking relationship with a shell bank, that has conducted a transaction with that shell bank, poses the highest risk to Canada's AML/ATF regime and directly contravenes the prohibition under subsection 9.4(2) of the Act. Therefore, the penalty is determined at the prescribed maximum, $100,000. FINTRAC will consider mitigating factors in its calculation of the penalty.

4.2 Violation related to obtaining approval of senior management for correspondent banking relationship

A correspondent banking relationship requires the financial entity's senior management oversight to ensure that it is not a conduit for anonymous, illicit financial transactions. Approval from senior management is required to enter into such a relationship, to ensure accountability at the highest level, and that the organization fully understands the associated ML/TF risks, and has the proper controls in place to mitigate risks.

Provision of the Act	Provision of the PCMLTFRFootnote 3	Description	Classification of violation
9.4(1)(c)	15.1(1)	Failure of a specified entity entering into a correspondent banking relationship with a prescribed foreign entity to obtain the approval of senior management	Minor$1-$1,000

Table 3—Violation related to obtaining approval of senior management for correspondent banking relationship

4.2.1 Harm done in the case of a violation related to obtaining approval of senior management for a correspondent banking relationship When approval to enter into a correspondent banking relationship is not obtained, there is high potential for harm related to the detection, prevention and deterrence of ML/TF in Canada, because there is no oversight and accountability from a financial entity's senior management which would ensure proper assessment and risk mitigation. Transactions posing high ML/TF risk could be conducted through a correspondent banking relationship that has not been scrutinized and risk-assessed by senior management. This makes the financial entity's operations more vulnerable to ML/TF offences and introduces vulnerabilities into Canada's financial system that may go undetected.

4.2.2 Penalty determination for a violation related to obtaining approval of senior management for a correspondent banking relationship When approval to enter into a correspondent banking relationship is not obtained, there is high potential for harm as the financial entity's operations are more vulnerable to ML/TF offences and introduces vulnerabilities into Canada's financial system that may go undetected. Therefore, the prescribed maximum penalty of $1,000 is determined for each correspondent banking relationship that senior management did not approve.

FINTRAC will consider relevant mitigating factors in its determination of the penalty. For example, if there have been no financial transactions or activities conducted with that foreign financial institution at the time that the non-compliance was discovered.

4.3 Violation related to ascertaining the name and address of a foreign financial institution

Financial entities that enter into a correspondent banking relationship are required to ascertain the name and address of the foreign financial institution by examining specific records from recognized authorities. This verification confirms the existence of the foreign financial institution and mitigates the possibility that the foreign financial institution is a shell bank. This information can be used for risk assessment, preparation of reports to FINTRAC, and as evidence when investigating and prosecuting ML/TF offences.

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
9.4(1)(a)	55.1(a)	Failure of a financial entity that enters into a correspondent banking relationship with a foreign financial institution to ascertain, in the prescribed manner, prescribed information in respect of the foreign financial institution	Minor$1-$1,000

Table 4—Violation related to ascertaining the name and address of a foreign financial institution

4.3.1 Harm done in the case of a violation related to ascertaining the name and address of a foreign financial institution Financial entities that enter into a correspondent banking relationship are required to ascertain the name and address of the foreign financial institution by examining specific records from recognized authorities. This verification confirms the existence of the foreign financial institution and mitigates the possibility that the foreign financial institution is a shell bank. This information can be used as evidence when police investigate ML/TF offences and for the preparation of reports to FINTRAC, as well as risk assessments.

Failing to ascertain the name and address of the foreign financial institution

makes the Canadian RE's operations more vulnerable to ML/TF offences and introduces vulnerabilities into Canada's financial system that may go undetected.

4.3.2 Penalty determination for a violation related to ascertaining the name and address of a foreign financial institution The PCMLTFR set out the manner in which the foreign financial institution's name and address must be verified. The requirements were developed to ensure that records from a recognized authority are used to ascertain the information.

Because of the risk that dealing with shell banks poses, when an RE has taken no measures to verify a foreign financial institution's name and address this constitutes a complete violation of the requirement, therefore the maximum penalty of $1,000 per instance will apply.

When the methods used to verify the information are not in line with the methods set out in the PCMLTFR, or when an RE fails to completely adhere to them, the requirement has not been met. As a result, the harm to achieving the objectives of the Act and FINTRAC's mandate is the same as that of a complete violation, therefore the same penalty ($1,000 per instance) will apply. FINTRAC will consider mitigating factors in its determination of the penalty. For example, there have been no financial transactions or activities conducted with that foreign financial institution at the time that the non-compliance was discovered, or corrective measures were taken before any financial transactions or activities were conducted.

4.4 Violations related to ascertaining prescribed information in respect of a foreign financial institution

Correspondent banking relationships with foreign financial institutions that have AML/ATF policies and procedures in place help safeguard Canada's financial system from ML and TF. When foreign financial institutions do not have AML/ATF policies and procedures in place, the risk of exposure to ML/TF offences is heightened for REs transacting with them under correspondent banking relationships. This risk can be further heightened when foreign financial institutions have received civil or criminal penalties related to violations of AML/ATF requirements.

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
9.4(1)(e)	15.1(1) and (3)	Failure of a specified entity to take reasonable measures to ascertain whether a prescribed foreign entity with whom it has entered into a correspondent banking relationship has in place prescribed policies and procedures and, if they are not in place, to take prescribed measures	Minor$1-$1,000

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
9.4(1)(a)	55.1(b)	Failure of a financial entity that enters into a correspondent banking relationship with a foreign financial institution to take reasonable measures to ascertain, in the prescribed manner, prescribed information in respect of the foreign financial institution and to conduct prescribed monitoring	Minor$1-$1,000

Table 5—Violations related to ascertaining prescribed information in respect of a foreign financial institution

4.4.1 Harm done in the case of violations related to ascertaining prescribed information in respect of a foreign financial institution Financial entities entering into a correspondent banking relationship with foreign financial institutions must take reasonable measures to ascertain whether the foreign financial institutions have AML/ATF policies and procedures, including those for approval of new account openings, and whether there are any civil or criminal penalties that have been imposed. If the foreign financial institution does not have the required policies and procedures, or if there has been a civil or criminal penalty imposed, then the Canadian financial entity must take reasonable measures to conduct ongoing monitoring of all transactions under the correspondent banking relationship, for the purpose of detecting transactions that must be submitted as a Suspicious Transaction Report (STR). Not meeting these requirements could signify that the ML/TF risks posed by the correspondent banking relationship are not managed effectively, which can result in unreported suspicious transactions, a loss of financial intelligence and other non-compliance issues. This impedes the achievement of the objectives

set out in subparagraph 3(a)(ii) and paragraph 40(b) of the Act.

4.4.2 Penalty determination for violations related to ascertaining prescribed information in respect of a foreign financial institution The potential harm is highest when an RE fails to take reasonable measures to determine whether the above circumstances apply to a correspondent banking relationship. If ongoing monitoring is not conducted on a foreign financial institution that has no AML/ATF procedures in place, or the foreign financial institution has received civil or criminal penalties for non-compliance with AML/ATF requirements, the prescribed maximum penalty of $1,000 per instance applies.

FINTRAC will consider mitigating factors in its determination of the penalty. For example, FINTRAC will consider whether very limited financial services (or none) have been provided to the foreign financial institution; or whether ongoing monitoring is in place for all transactions, including those conducted under the correspondent banking relationship. In these cases, FINTRAC may consider a penalty amount that is lower than the maximum prescribed.

4.5 Violations related to ascertaining that a foreign financial institution meets client identification requirements

Regulatory requirements are designed to identify individuals and entities that conduct, control, direct, or are involved in financial transactions in order to remove anonymity. The requirements extend to the clients of foreign financial institutions who can access Canada's financial system through a correspondent banking relationship. REs that allow clients of foreign financial institutions direct access to their accounts must take reasonable measures to find out if the foreign financial institutions apply the requirement to verify client identity and confirm the existence of entities in a manner that is consistent with the Act and its regulations. The REs must also take reasonable measures to find out if the foreign financial institutions agree to provide client identification data upon request.

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
9.4(1)(a)	55.2(a)	Failure of a financial entity that enters into a correspondent banking relationship with a foreign financial institution to take reasonable measures to ascertain whether the institution has met the prescribed requirements	Minor$1-$1,000
9.4(1)(a)	55.2(b)	Failure of a financial entity that enters into a correspondent banking relationship with a foreign financial institution to take reasonable measures to ascertain whether the institution has agreed to provide customer identification data	Minor$1-$1,000

Table 6—Violations related to ascertaining that a foreign financial institution meets client identification requirements

4.5.1 Harm done in the case of violations related to ascertaining that a foreign financial institution meets client identification requirements
Failing to comply with the requirements described above potentially allows the

clients of foreign financial institutions to conduct financial transactions directly through the RE, allowing them to move funds through Canada anonymously. This increases the Canadian financial system's exposure to ML/TF risk, because REs would not be able to identify the true beneficiaries of transactions. This violation contravenes the objectives set out in subparagraph 3(a)(i), paragraphs 3(c) and 40(e) of the Act and its regulations.

4.5.2 Penalty determination for violations related to ascertaining that a foreign financial institution meets client identification requirements

If an RE fails to take reasonable measures to find out if a foreign financial institution has met client identification requirements in keeping with sections 54 and 64 of the PCMLTFR, or if client identification data will be provided upon request, there is a high likelihood that individuals and entities that conduct, control, direct, or are involved in financial transactions in Canada through a correspondent banking relationship would not be identified. Therefore, the prescribed maximum penalty of $1,000 per instance applies.

FINTRAC will consider mitigating factors in its determination of the penalty. This could include when an RE has not transacted with the foreign financial institution or the clients did not have direct access to the accounts under the correspondent banking relationship. Another example of a mitigating factor would be if the foreign financial institution ultimately meets the client identification standards set out in the PCMLTFR through other means or processes.

4.6 Violations related to correspondent banking relationships records

See the guide on harm done assessment for record keeping violations for the harm rationale and penalty calculation for the violations below.

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
9.1(4)(a)	15.1(1) and (2)	Failure of a specified entity entering into a correspondent banking relationship with a prescribed foreign entity to keep a prescribed record.	Minor$1-$1,000

Provision of the Act	Provision of the PCMLTFR	Description	Classification of violation
9.4(1)(d)	15.1(1)	Failure of a specified entity entering into a correspondent banking relationship with a prescribed foreign entity to set out in writing their obligations and those of the foreign entity in respect of the correspondent banking services	Minor$1-$1,000

Table 7—Violations related to correspondent banking relationships records

5. Violations related to requirements for foreign branches and subsidiaries

This section outlines FINTRAC's approach to the violations related to requirements for foreign branches and subsidiaries, including the harm assessments and penalty calculations.

5.1 Violations related to compliance policies for foreign branches and subsidiaries

The requirement for certain RE sectors to hold their foreign operations to the same compliance standards as those in Canada supports the objective under paragraph 3(a) of the Act to detect, prevent and deter ML/TF. It also fulfills Canada's international commitments to fight transnational crimes as per paragraph 3(c) of the Act.

Provision of the Act	Description	Classification of violation
9.7(1)	Failure to develop policies that establish requirements similar to those of sections 6, 6.1 and 9.6 of the Act and to ensure that foreign branches and foreign subsidiaries apply those policies	Serious$1-100,000
9.7(2)	Applying policies that establish requirements similar to those of sections 6, 6.1 and 9.6 of the Act before they are approved by a board of directors	Serious$1-100,000

Table 8—Violations related to compliance policies for foreign branches and subsidiaries

5.1.1 Harm done in the case of violations related to compliance policies for foreign branches and subsidiaries Failing to develop policies that meet the requirements similar to those of sections 6, 6.1 and 9.6 of the Act leaves foreign branches and foreign subsidiaries vulnerable to ML/TF, ultimately posing a risk to the RE in Canada as well, given the possibility of overlapping services and accounts. This results in the possibility of anonymous transactions being conducted across borders without the accountability and structure to ensure group-wide compliance. Also, the necessary information and records to support client identification, risk assessments, ongoing monitoring, and transaction reporting would be missing. This could ultimately result in suspicious transactions not being detected and reported to FINTRAC to support investigations and prosecutions of ML/TF offences.

5.1.2 Penalty determination for violations related to compliance policies for foreign branches and subsidiaries We use the penalty calculation for compliance program violations to address the failure to develop and apply compliance policies for foreign branches and subsidiaries. Refer to the guide on harm done assessment for compliance program violations for harm standards and penalty determinations.

5.2 Violation related to policies and procedures for the exchange of information between affiliated entities

The Act requires the development and application of policies and procedures on the exchange of information between REs and affiliated domestic or foreign entities for the purpose of detecting and deterring ML/TF offences, and assessing the risk of ML/TF offences. This coordinated approach makes for effective customer due diligence (CDD) and ML/TF risk management.

Provision of the Act	Description	Classification of Violation
9.8(1)	Failure of an entity to develop and apply policies and procedures related to the exchange of information between it and affiliated entities	Serious$1-100,000

Table 9—Violation related to policies and procedures for the exchange of information between affiliated entities

5.2.1 Harm done in the case of a violation related to policies and procedures for the exchange of information between affiliated entities Failing to develop and apply policies and procedures for the exchange of information between affiliated entities could leave Canada's financial system vulnerable to abuse. The objectives set out in the Act are not being met when measures are not taken to detect ML/TF activities (paragraph 3(a)), to assist in fulfilling Canada's international commitments to fight transnational crime (paragraph 3(c)), and to enhance Canada's capacity to take targeted measures to protect its financial system and mitigate the risk of being used for ML/TF activities (paragraph 3(d)).

5.2.2 Penalty determination for a violation related to policies and procedures for the exchange of information between affiliated entities If there are no policies and procedures in place for the exchange of information between affiliated entities, the RE could be vulnerable to ML/TF risks through the affiliated entities' compliance gaps. When the required policies and procedures are non-existent, the maximum prescribed penalty amount of $100,000 applies because this poses the highest level of risk.

FINTRAC will consider mitigating factors when determining the penalty. For example, after considering the completeness of policies and procedures on the exchange of information, the roles and responsibilities for the exchange of information, and the timeliness and frequency of exchanges, it may consider a penalty that is lower than the maximum prescribed.

5.3 Violations related to record keeping and notification for foreign branches and subsidiaries

In order to mitigate the potential ML/TF risks to Canada's financial system stemming from financial interactions with foreign entities, REs must ensure that their overseas operations hold AML/ATF compliance standards similar to those of Canada. However, it is possible that the laws in a foreign jurisdiction may prohibit or conflict with the record keeping, identity verification or other compliance requirements of the Act and its regulations. When this is the case, an exception to applying similar AML/ATF compliance standards is justifiable. REs must keep a record of the facts and reasons why the foreign branch or subsidiary cannot apply a compliance policy. They are also required to notify FINTRAC and their principal supervisory/regulatory body under federal or provincial law of these facts and reasons within a reasonable time. The record of the facts and reasons demonstrates the RE's compliance with the requirement and allows the RE the opportunity to thoroughly assess the types of ML/TF risks associated with its foreign branches/subsidiaries, the reasons why a compliance policy cannot be applied, and the mitigation measures needed. Notifying FINTRAC and other government supervisory/regulatory bodies of the facts and reasons also fulfills the international commitment to support the fight against ML/TF crimes.

Provision of the Act	Description	Classification of Violation
9.7(4)	Failure to keep and retain a record of the fact that a foreign branch or foreign subsidiary cannot apply a policy and of the reasons why it cannot do so or to notify the Centre and the principal supervisory or regulating agency or body within a reasonable time	Minor$1-$1,000

Provision of the Act	Description	Classification of Violation
11.44(2)	Failure to keep and retain a record of the fact that a foreign branch or foreign subsidiary cannot comply with a ministerial directive and of the reasons why it cannot do so or to notify the Centre and the principal supervisory or regulating agency or body within a reasonable time	Serious$1-$100,000

Table 10—Violations related to record keeping and notification for foreign branches and subsidiaries

5.3.1 Harm done in the case of violations related to record keeping and notification for foreign branches and subsidiaries Failing to keep a record of the fact that a foreign branch or subsidiary cannot comply with and AML/ATF policies and the reasons why it cannot do so, and failing to report it to FINTRAC and the supervisory/regulatory body, can result in ML/TF risks and AML/ATF gaps through the RE's operations in foreign jurisdictions. When the non-compliance of a foreign branch or subsidiary is not detected, understood, assessed and mitigated, it presents significant risk. This failure could interfere with Canada's understanding of the ML/TF and compliance risks associated with a foreign jurisdiction and could affect Canada's international commitments to fight against ML/TF.

5.3.2 Penalty determination for violations related to record keeping and notification for foreign branches and subsidiaries FINTRAC has identified four levels of harm related to these violations based on the RE's and Canada's ability to understand, assess and mitigate ML/TF risks related to foreign operations. The above-mentioned penalty ranges ($1 to $1,000 for compliance policy violations, and $1 to $100,000 for Minister's directive violations) are divided into four even intervals to show the various levels of harm. The highest harm category for both violations is assigned the prescribed maximum amounts of $1,000 and $100,000. The lowest of the four levels of harm has a penalty determination of $250 and $25,000. Penalty amounts may be reduced

based on mitigating factors; however, they must be enough to encourage a change in compliance behaviour.

The table below details the levels of harm, the types of non-compliance and the description of harm along with their corresponding penalties.

When deficiencies fall into more than one harm category, the penalty is determined at the highest harm category, and is not cumulative.

Level of harm	Type of non-compliance	Harm description	Penalty (not considering mitigating factors)
Compliance policy:	Minister's directive:		
Level 1	No record of fact and reasons; FINTRAC and supervisor/regulator not notified	Completely impedes Canadian authorities' and the RE's ability to assess the exception and consider associated risks for mitigation measures at both the national and RE level	$1,000
Level 2	Record of facts and reasons exists but FINTRAC and supervisor/regulator are not notified	Impedes all Canadian authorities' ability to assess the exception and consider the associated risks for mitigation measures at a national level.	$750

Level of harm	Type of non-compliance	Harm description	Penalty (not considering mitigating factors)
Level 3	No record of fact and reasons but FINTRAC and supervisor/regulator are notified	Although the proper Canadian authorities are made aware of the exceptions, documentation deficiencies can lead to inaccurate or incomplete ML/TF risk assessments of the exceptions, leading to ineffective measures at the RE level	$500
Level 4	Record of facts and reasons exists; FINTRAC and supervisor/regulator notified but not within a reasonable time	Diminishes the Canadian authorities' ability to assess the exception and consider the associated risks in an efficient manner	$250

Table 11—Levels of harm and penalties for violations related to record keeping and notification for foreign branches and subsidiaries

5.3.3 Level 1 harm—No record of fact and reasons; FINTRAC and supervisor/regulator not notified When an RE makes no effort to understand the facts and reasons why a foreign branch or subsidiary cannot comply with AML/ATF standards similar to those of Canada, does not record those facts and reasons, and fails to notify FINTRAC and its supervisor or regulator; this poses the highest level of risk because the RE is not able to detect, assess and mitigate the ML/TF risk, and Canada cannot evaluate the risk on the regime at large. Therefore, the penalty is determined at the prescribed maximum, $1,000 for compliance policy violations, and $100,000 for a minister's directive violations.

5.3.4 Level 2 harm—Record of facts and reasons exists but FINTRAC and supervisor/regulator are not notified When FINTRAC and other supervisory or regulatory bodies are not notified of the facts and reasons why a foreign branch or subsidiary cannot comply, while mitigation measures may be in place at the RE, partners in Canada's AML/ATF regime would not be aware of the risks, nor would they be able to coordinate their compliance efforts and take measures to mitigate ML/TF risks for Canada. If the foreign compliance exception had regime-wide implications, FINTRAC would not have the opportunity to consider risk mitigation measures with other stakeholders such as the Department of Finance. Therefore, the penalty is set at $750 for compliance policy violations, and $75,000 for minister's directive violations.

5.3.5 Level 3 harm—No record of fact and reasons although FINTRAC and supervisor/regulator are notified If an RE notifies FINTRAC and its principal supervisory or regulatory body but fails to keep a record that contains accurate, complete and up-to-date information on the facts and reasons, the harm done is lesser because the proper government bodies are made aware of the exceptions. However, documentation deficiencies can lead to inaccurate or incomplete ML/TF risk assessments of the exceptions, leading to ineffective measures at the RE level. Therefore, the penalty is set at $500 for compliance policy violations, and $50,000 for ministerial directive violations.

5.3.6 Level 4 harm—Record of facts and reasons exists; FINTRAC and supervisor/regulator notified but not within a reasonable time If a record of the facts and reasons is kept, and FINTRAC and the principal supervisory or regulatory bodies are notified, but not in a timely manner, the efficient use of the information for risk assessment and compliance purposes, at a national level, would be affected. Therefore, the penalty is set at $250 for compliance policy violations, and $25,000 for minister's directive violations.

6. Violations related to including prescribed information in prescribed electronic funds transfers (travel rule)

REs that conduct EFTs in the course of their activities must make sure that each transfer includes the name, address and account number, or other reference number of the requesting client. When an RE receives an EFT in the course of its activities, it must take reasonable measures to ensure that any transfer includes the same information.

Information that identifies the parties to a transaction is essential in establishing the origin and the flow of funds which are needed for analysis, investigations and the prosecution of ML/TF offences. The information can be used by the RE for risk assessment, transaction reporting and other compliance requirements, where applicable.

Provision of the Act	Provision of the PCMLTFR	Description	Classification of Violation
9.5(a)	66.1(1) and (2)	Failure of a prescribed person or entity to include prescribed information in prescribed electronic funds transfers	Minor$1-$1,000
9.5(b)	66.1(1) and (2)	Failure of a prescribed person or entity to take reasonable measures to ensure that any transfer that the person or entity receives includes prescribed information	Minor$1-$1,000

Table 12—Violations related to including prescribed information in prescribed EFTs (travel rule)

6.1 Harm done in the case of violations related to including prescribed information in prescribed EFTs (travel rule)

If the prescribed information is missing from a transfer, the harm is the same as the harm posed by not keeping a record. See the guide on harm done assessment for record keeping violations for the harm rationale.

6.2 Penalty determination for violations related to including prescribed information in prescribed EFTs (travel rule)

The harm of not including prescribed information in a prescribed EFT is the same as the harm posed by not keeping a record, therefore the same penalty applies. See the guide on harm done assessment for record keeping violations for the penalty determination.

7. Violations related to the requirement to assist FINTRAC

This section outlines FINTRAC's approach to the violations related to the requirement to assist FINTRAC in its mandate of ensuring compliance, including the harm assessment and penalty calculation.

7.1 Violations related to the requirement to provide an authorized person with reasonable assistance and information reasonably required, or provide information in accordance with a notice

FINTRAC is mandated to ensure REs' compliance with Parts 1 and 1.1 of the Act. In order to fulfill this mandate, it is essential for FINTRAC to have reasonable assistance from REs and access to reasonably required information when conducting compliance activities, like examinations.

Provision of the Act	Description	Classification of Violation
62(2)	Failure to give reasonable assistance and information reasonably required to an authorized person	Serious$1-$100,000
63.1(2)	Failure to provide, in accordance with a notice, documents or other information reasonably required by an authorized person	Serious$1-$100,000

Table 13—Violations related to the requirement to provide an authorized person with reasonable assistance and information reasonably required, or provide information in accordance with a notice

7.2 Harm done in the case of violations related to the requirement to provide an authorized person with reasonable assistance and information reasonably required, or provide information in accordance with a notice

Failing to give an authorized person reasonable assistance and to provide them with any information with respect to the administration of Part 1 and 1.1 of the Act and its regulations, or in accordance with a served notice, interferes with FINTRAC's compliance activities and its mandate under subsection 40(e) of the Act. These activities include examination planning and outreach. If FINTRAC is unable to ensure compliance, the regime's ability to detect, prevent and deter

ML/TF and to mitigate risk is affected. FINTRAC cannot maintain a database of transaction reports or it cannot ensure the proper client identification and record keeping measures are in place in support of financial intelligence for investigations and prosecutions of ML/TF offences.

7.3 Penalty determination for violations related to the requirement to provide an authorized person with reasonable assistance and information reasonably required, or provide information in accordance with a notice

When an RE does not give reasonable assistance, the information reasonably required, or provide the information reasonably required in accordance with a notice, FINTRAC's ability to effectively and efficiently ensure compliance with the Act and its regulations is affected. This shows an RE's unwillingness to cooperate, or an attempt to operate outside of the Act and its requirements. Therefore, this violation results in the prescribed maximum penalty of $100,000. FINTRAC will consider mitigating factors in its determination of the penalty.

Administrative monetary penalties policy

The purpose of FINTRAC's Administrative monetary penalties (AMPs) program is to encourage future compliance with the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (the Act) and its regulations, and to promote a change in behaviour. The AMP program supports FINTRAC's mandate by providing a measured and proportionate response to particular instances of non-compliance. FINTRAC is committed to working with reporting entities (REs) to help them achieve compliance. AMPs are not issued automatically in response to non-compliance, as typically other compliance actions are taken to change behaviour before a penalty is considered.

Purpose

The purpose of this policy is to provide a framework for the determination of an AMP; and to summarize the principles and guidelines that are used by FINTRAC to issue an AMP.

Our operating principles and framework

The purpose of the AMP program is to support FINTRAC's efforts to ensure compliance with the Act and its regulations by providing a measured response to non-compliance issues. The program's guiding principles are:

Objectivity: FINTRAC officers will conduct themselves professionally during an assessment and in their communications with an RE. FINTRAC officers will make objective assessments based on the facts and circumstances of each case, ensuring fair and reasonable decisions.

Reasonableness: FINTRAC officers will exercise professional judgement when assessing an RE's compliance with the Act and its regulations. This involves considering the circumstances and all relevant factors prior to considering an AMP.

Transparency: FINTRAC officers will make sure that the expectations about compliance are communicated in a clear manner throughout the assessment process. REs will be provided with FINTRAC's findings and observations, and will be given the opportunity to ask questions and respond to the non-compliance identified before the findings are finalized.

Fairness: An RE has the right to understand the case being made for an AMP, and will have a fair opportunity to respond.

Consistency: FINTRAC officers follow established policies and procedures to make sure that similar REs, with the same types and extent of non-compliance, can expect to be treated in a similar manner.

Documentation: FINTRAC officers will rely on facts and document those facts and any other information to support their analysis and findings.

Background and application

FINTRAC works with businesses and law enforcement to combat money laundering (ML) and terrorist activity financing (TF). By effectively identifying clients and keeping records, REs help deter criminal activity and are able to provide law enforcement with evidence for the investigation and prosecution of ML/TF offenses. By reporting the required financial transactions to FINTRAC, REs are supplying it with the information that it needs to carry out its mandate, support law enforcement partners, and contribute to the protection of the integrity of Canada's financial system and the safety of Canadians.

FINTRAC's compliance framework recognizes that the success of Canada's Anti-Money Laundering / Anti-Terrorist Financing (AML/ATF) regime depends on the concrete application of the regulatory measures designed to detect, prevent and deter ML/TF activity. Our own compliance effort aims to bring awareness and understanding of the requirements under the Act and its regulations, to deter non-compliance, and to assist in the detection of ML/TF in support of the efforts of the police and intelligence communities. FINTRAC's risk-based compliance program includes activities of increasing intensity across a range of options (see Figure 1 below). We focus our efforts on promoting awareness, providing assistance and conducting compliance assessments where they will be most effective, but may enforce penalties in the case of non-compliance.

Figure 1 – FINTRAC compliance activities

The graphic shows the awareness, assistance as well as assessment and enforcement compliance activities from low intensity to high intensity.

Awareness activities include: outreach and compliance assessment reports (CARs).

Assistance activities include: engagement, support, policy interpretations and money services business registry.

Assessment and enforcement activities include: CARs, observation letters, reporting entity validations, reports monitoring, compliance meetings, desk exams, onsite exams, follow-up exams, administrative monetary penalties and non-compliance disclosures.

Assessing non-compliance

In the normal course of our compliance activities, we identify instances of non-compliance with the Act and its regulations. We assess the severity of each non-compliance issue by understanding both the extent and the root cause of the non-compliance. Each non-compliance issue is assessed for its impact on FINTRAC's mandate and on the achievement of the objectives of the Act. To determine a suitable response to address a non-compliance result, we will consider the result in a holistic context, including other factors such as the RE's compliance history.

Addressing non-compliance

Following the completion of a compliance assessment, and depending on the extent of the non-compliance identified, FINTRAC may decide:

1. to take no further action;
2. to conduct follow-up compliance activities;
3. to issue an AMP to encourage a change in behaviour; or
4. to disclose relevant information to law enforcement for investigation and prosecution of non-compliance offences under the Act and its regulations.

Authority to issue an AMP

The following outlines the framework applicable when FINTRAC has decided that an AMP is the most suitable option to address a specific non-compliance result.

FINTRAC may issue an AMP and serve a notice of violation when it has **reasonable grounds to believe** that an RE has violated a requirement of the Act and its regulations.

AMPs are not issued automatically in response to non-compliance. AMPs are one tool that is available to FINTRAC and are used to address repeated non-compliant behaviour. AMPs may also be used when there are significant issues of non-compliance or a high impact on FINTRAC's mandate or on the objectives of the Act and its regulations. An AMP is generally used when other compliance options have failed.

Categories of violations

The Proceeds of Crime (Money Laundering) and Terrorist Financing Administrative Monetary Penalties Regulations (AMP Regulations) list the non-compliance violations that could be the basis of an AMP. The AMP Regulations categorize violations by degree of importance, and assign the following penalty ranges:

Minor violation	$1 to $1,000 per violation
Serious violation	$1 to $100,000 per violation
Very serious violation	$1 to $100,000 per violation for an individual $1 to $500,000 per violation for an entity

Categories of violations

The limits above apply to each violation, and multiple violations can result in a total amount that exceeds these limits.

Criteria for determining an AMP amount

The Act and the AMP Regulations set out three criteria that must be taken into account when determining a penalty amount:

- The purpose of AMPs, which is to encourage compliance, not to punish (non-punitive);
- The harm done by the violation; and
- The RE's history of compliance.

We present the methods that we use to determine the penalty amount, along with the factors that we consider in our assessment when we issue an AMP.

FINTRAC will take a reasonable approach in the calculation of penalty amounts. We consider an AMP to be effective when the penalty amount is proportional to the harm done and prompts a change in behaviour toward future compliance. These amounts are in keeping with the type and extent of the violations, given the circumstances of each case.

The following guidelines are in place as benchmarks to assist FINTRAC officers in the calculation of a penalty amount, while taking into consideration the circumstances of each case. As a result, relevant mitigating factors will be carefully considered at each step and may reduce the actual penalty determined.

Step 1: Harm done assessment FINTRAC defines "harm" as the degree to which a violation interferes with achieving the objectives of the Act (section 3, Act) or with FINTRAC's ability to carry out its mandate (section 40, Act).

The AMP Regulations classify all violations by degree of importance. They also determine the minimum and maximum penalty amounts for each level.

In assessing the harm done by a violation, FINTRAC considers both the potential and the resulting harm. "Resulting harm" means separate violations that come from the original violation. For example, when the compliance policies and procedures do not address how to report large cash transactions, the resulting harm is the unreported large cash transactions.

The first test to assess the harm done when calculating a penalty amount is to determine whether the reporting entity has completely failed to meet a requirement or only in part. For some violations, this is obvious; the requirement was met or it was not met. Other violations require further analysis. For example, when a client is not identified under the prescribed circumstances, the requirement is not met. When compliance policies and procedures are missing a component, the requirement is met in part.

When an RE has completely failed to meet a requirement, the base penalty amount that is typically considered for that violation is the maximum amount set out by the AMP Regulations. This is because completely failing to meet a statutory requirement is what interferes the most with achieving the objectives of the Act and FINTRAC's ability to fulfil its mandate.

When an RE has failed to meet part of a requirement, the base penalty amount determined for each violation depends on the part that is non-compliant and the extent of the failure. The extent of the failure is measured using assessment criteria that have been established based on the level of interference with achieving the objectives of the Act and FINTRAC's mandate.

Step 2: Compliance history and non-punitive adjustment The second step in a penalty calculation looks at both the compliance history of the RE and the AMP's purpose, which is to encourage compliance, not to punish (non-punitive).

FINTRAC adjusts the penalty amount for each violation (determined in Step 1 above), based on whether or not the RE has previously been levied an AMP for the violation.

For a first-time violation, the penalty is typically reduced by two-thirds. For a violation occurring a second time (meaning that the RE had been penalized for this very same violation on a previous occasion), the penalty is typically reduced by one-third. For violations occurring a third time or more (again, meaning that the RE had been penalized for the same violation on two or more previous occasions), the full base penalty amount will typically be applied.

AMP program – roles and responsibilities within FINTRAC

FINTRAC's AMP program is centralized at our headquarters in Ottawa. This helps to ensure policies and processes are applied consistently across the country and to maintain the required separation of duties between compliance assessment such as compliance examinations and enforcement. This approach also

helps us monitor our program's effectiveness and allows us to quickly make policy and process improvements at the national level.

Following a compliance examination by FINTRAC regional offices located in Vancouver, Montreal and Toronto, we will review the findings to determine the most appropriate action to address the non-compliance. If the deficiencies and non-compliant behaviour justify an AMP consideration, the relevant regional office will make a recommendation, including the reasons, to headquarters. Upon receipt of the recommendation, headquarters undertakes an independent assessment of the findings and related information to determine whether we will proceed with an AMP.

AMP process

The AMP process begins with the issuance of a notice of violation and continues as outlined below:

Notice of violation

An RE subject to an AMP will receive a notice of violation that will include the following:

- The name and address of the RE that is subject to the AMP;
- The penalty amount;
- Payment instructions;
- Information on the right to make written representations to FINTRAC's Director and Chief Executive Officer (CEO), up to 30 days after receiving the notice of violation;
- Instructions on how to make representations to FINTRAC's Director and CEO, and where to obtain additional information on the AMP program;
- A list of the violations committed which will include the related legislative and regulatory provisions;
- The details of the penalty calculation, including the factors considered and the reasons; and
- A list of all the instances of the committed violations, including relevant references such as account numbers, transaction numbers, report numbers, etc.

A notice of violation must be issued no more than 2 years from the date when the non-compliance became known to FINTRAC.

In some cases, FINTRAC may exercise its discretion to offer to enter into a compliance agreement with the RE, which will include specific terms and conditions.

Payment of penalty

Upon receipt of a notice of violation, a person or entity can pay the penalty by completing the remittance form and submitting it with the payment in Canadian funds to:

FINTRAC

Finance Unit

24th Floor, 234 Laurier Avenue West

Ottawa, ON K1P 1H7

All payments of penalty amounts are to be made payable to the Receiver General for Canada. Payments can be made in the form of a certified cheque, money order, or bank draft.

If an RE pays the penalty indicated in the notice of violation, the RE is deemed to have committed the violations specified, and the AMP process ends.

Representations to FINTRAC's Director and CEO

An RE may request a review of a notice of violation. This can be done by making written representations on the violations or the penalty or both at the same time, to the Director and CEO of FINTRAC, within 30 days of receiving the notice of violation.

If an RE requests a review, FINTRAC's Director and CEO will decide on the balance of probabilities whether the RE committed the violation or not; and may impose the penalty proposed in the notice of violation, a lesser penalty or no penalty. A notice of decision will be issued to communicate the Director and CEO's decision and the reasons behind it.

Failure to pay or make representations and notice of penalty

If you receive a notice of violation and do not pay or make representations to FINTRAC's Director and CEO within 30 days, the AMP process will end, the violations will be upheld and a notice of penalty will be issued.

Notice of decision and right of appeal

An RE that receives a notice of decision from FINTRAC's Director and CEO has 30 days to exercise its right of appeal to the Federal Court of Canada.

The AMP process ends when an RE pays the penalty imposed in the notice of decision, or does not appeal the Director and CEO's decision within 30 days.

Should the Director and CEO not issue a notice of decision within 90 days of receiving your representation for review, you may appeal the proposed penalty in Federal Court within 30 days.

Federal Courts

The Federal Courts have the power to confirm, set aside or change a notice of decision issued by FINTRAC's Director and CEO. As long as the AMP is before the Federal Court, the Federal Court of Appeal, or the Supreme Court of Canada, the AMP process is considered to be ongoing.

Public notice

FINTRAC must make public, as soon as feasible, the name of the RE, the nature of the violation or default, and the amount of the penalty imposed in the following cases:

- An RE pays the penalty issued in a notice of violation.
- An RE neither pays the penalty issued in a notice of violation nor makes representations to FINTRAC's Director and Chief Executive Officer.
- An RE receives a notice of decision indicating that a violation has been committed.
- An RE enters into a compliance agreement with FINTRAC.
- An RE does not comply with a compliance agreement.

When publicizing the nature of the violation, FINTRAC may also include the reasons for its decision, including the relevant facts, analysis and considerations that formed part of the decision.

You can review the AMPs imposed by FINTRAC on the Public notice page.

Collection of penalties

The penalty amount is due 30 days after the notice of violation or notice of decision is received. Interest would begin to accrue on the day after the penalty was due. Any penalty that becomes payable is an outstanding debt to the Crown. FINTRAC will pursue outstanding AMP payments.

Guidance glossary

The glossary defines certain terms used throughout FINTRAC's guidance.

Definitions

Accountant

A chartered accountant, a certified general accountant, a certified management accountant or, if applicable, a chartered professional accountant. (comptable)

Accounting firm

An entity that is engaged in the business of providing accounting services to the public and has at least one partner, employee or administrator that is an

accountant. (cabinet d'expertise comptable)

Act

The Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA). (la Loi)

Administrative monetary penalties (AMPs)

Civil penalties that may be issued to reporting entities by FINTRAC for non-compliance with the PCMLTFA and associated Regulations. (pénalité administrative pécuniaire [PAP])

Affiliate

An entity is affiliated with another entity if one of them is wholly owned by the other, if both are wholly owned by the same entity or if their financial statements are consolidated. (entité du même groupe)

Annuity

Has the same meaning as in subsection 248(1) of the Income Tax Act. (rente)

Armoured cars

Persons or entities that are engaged in the business of transporting currency, money orders, traveller's cheques or other similar negotiable instruments. (Véhicules blindés)

As soon as practicable

A time period that falls in-between immediately and as soon as possible, within which a suspicious transaction report (STR) must be submitted to FINTRAC. The completion and submission of the STR should take priority over other tasks. In this context, the report must be completed promptly, taking into account the facts and circumstances of the situation. While some delay is permitted, it must have a reasonable explanation. (aussitôt que possible)

Attempted transaction

Occurs when an individual or entity starts to conduct a transaction that is not completed. For example, a client or a potential client walks away from conducting a $10,000 cash deposit. (opération tentée)

Authentic

In respect of verifying identity, means genuine and having the character of an original, credible, and reliable document or record. (authentique)

Authorized person

A person who is authorized under subsection 45(2). (personne autorisée)

Authorized user

A person who is authorized by a holder of a prepaid payment product account to have electronic access to funds or virtual currency available in the account by means of a prepaid payment product that is connected to it. (utilisateur autorisé)

Beneficial owner(s)

Beneficial owners are the individuals who are the trustees, and known beneficiaries and settlors of a trust, or who directly or indirectly own or control 25% or more of i) the shares of a corporation or ii) an entity other than a corporation or trust, such as a partnership. The ultimate beneficial owner(s) cannot be another corporation or entity; it must be the actual individual(s) who owns or controls the entity. (bénéficiaire effectif)

Beneficiary

A beneficiary is the individual or entity that will benefit from a transaction or to which the final remittance is made. (bénéficiaire)

Branch

A branch is a part of your business at a distinct location other than your main office. (succursale)

British Columbia notary corporation

An entity that carries on the business of providing notary services to the public in British Columbia in accordance with the Notaries Act, R.S.B.C. 1996, c. 334. (société de notaires de la Colombie-Britannique)

British Columbia notary public

A person who is a member of the Society of Notaries Public of British Columbia. (notaire public de la Colombie-Britannique)

Cash

Coins referred to in section 7 of the Currency Act, notes issued by the Bank of Canada under the Bank of Canada Act that are intended for circulation in Canada or coins or bank notes of countries other than Canada. (espèces)

Casino

A government, organization, board or operator that is referred to in any of paragraphs 5(k) to (k.3) of the Act. (casino)

Certified translator

An individual that holds the title of professional certified translator granted by a Canadian provincial or territorial association or body that is competent under Canadian provincial or territorial law to issue such certification. (traducteur agréé)

Clarification request

A clarification request is a method used to communicate with money services businesses (MSBs) or foreign money services businesses (FMSBs) when FINTRAC needs more information about their registration form. This request is usually sent by email. (demande de précisions)

Client

A person or entity that engages in a financial transaction with another person or entity. (client)

Client identification information

The identifying information that you have obtained on your clients, such as name, address, telephone number, occupation or nature of principal business, and date of birth for an individual. (renseignements d'identification du client)

Competent authority

For the purpose of the criminal record check submitted with an application for registration, a competent authority is any person or organization that has the legally delegated or invested authority, capacity, or power to issue criminal record checks. (autorité compétente)

Completed transaction

Is a transaction conducted by a person or entity, that is completed and results in the movement of funds, virtual currency, or the purchase or sale of an asset. (opération effectuée)

Completing action

With respect to a reportable transaction, information related to the instructions provided by the person or entity making the request to the reporting entity to

complete a transaction. For example, an individual arrives at a bank and requests to purchase a bank draft. The completing action is the details of how the reporting entity fulfilled the person or entity's instructions which led to the transaction being completed. This includes what the funds or virtual currency initially brought to the reporting entity was used for (see "disposition"). A transaction may have one or more completing actions depending on the instructions provided by the person or entity. (action d'achèvement)

Compliance officer

The individual, with the necessary authority, that you appoint to be responsible for the implementation of your compliance program. (agent de conformité)

Compliance policies and procedures

Written methodology outlining the obligations applicable to your business under the PCMLTFA and its associated Regulations and the corresponding processes and controls you put in place to address your obligations. (politiques et procédures de conformité)

Compliance program

All elements (compliance officer, policies and procedures, risk assessment, training program, effectiveness review) that you, as a reporting entity, are legally required to have under the PCMLTFA and its associated Regulations to ensure that you meet all your obligations. (programme de conformité)

Context

Clarifies a set of circumstances or provides an explanation of a situation or financial transaction that can be understood and assessed. (contexte)

Correspondent banking relationship

A relationship created by an agreement or arrangement under which an entity referred to in any of paragraphs 5(a), (b), (d),(e) and (e.1) or an entity that is referred to in section 5 and that is prescribed undertakes to provide to a prescribed foreign entity prescribed services or international electronic funds transfers, cash management or cheque clearing services. (relation de correspondant bancaire)

Country of residence

The country where an individual has lived continuously for 12 months or more. The individual must have a dwelling in the country concerned. For greater certainty, a person only has one country of residence no matter how many dwelling places they may have, inside or outside of that country. (pays de résidence)

Credit card acquiring business

A credit card acquiring business is a financial entity that has an agreement with a merchant to provide the following services:

- enabling a merchant to accept credit card payments by cardholders for goods and services and to receive payments for credit card purchases;
- processing services, payment settlements and providing point-of-sale equipment (such as computer terminals); and
- providing other ancillary services to the merchant.

Credit union central

A central cooperative credit society, as defined in section 2 of the Cooperative Credit Associations Act, or a credit union central or a federation of credit unions or caisses populaires that is regulated by a provincial Act other than one enacted by the legislature of Quebec. (centrale de caisses de crédit)

Crowdfunding platform

A website or an application or other software that is used to raise funds or virtual currency through donations. (plateforme de sociofinancement)

Crowdfunding platform services

The provision and maintenance of a crowdfunding platform for use by other persons or entities to raise funds or virtual currency for themselves or for persons or entities specified by them. (services de plateforme de sociofinancement)

Current

In respect of a document or source of information that is used to verify identity, is up to date, and, in the case of a government-issued photo identification document, must not have been expired when the ID was verified. (à jour)

Dealer in precious metals and stones

A person or entity that, in the course of their business activities, buys or sells precious metals, precious stones or jewellery. It includes a department or an agent of His Majesty in right of Canada or an agent or mandatary of His Majesty in right of a province when the department or the agent or mandatary carries out the activity, referred to in subsection 65(1), of selling precious metals to the public. (négociant en métaux précieux et pierres précieuses)

Deferred profit sharing plan

Has the same meaning as in subsection 248(1) of the Income Tax Act. (régime de participation différée aux bénéfices)

Deposit slip

A record that sets out:

1. (a) the date of the deposit;
2. (b) the name of the person or entity that makes the deposit;
3. (c) the amount of the deposit and of any part of it that is made in cash;
4. (d) the method by which the deposit is made; and
5. (e) the number of the account into which the deposit is made and the name of each account holder.

(relevé de dépôt)

Directing services

A business is directing services at persons or entities in Canada if at least one of the following applies:

- The business's marketing or advertising is directed at persons or entities located in Canada;
- The business operates a ".ca" domain name; or,
- The business is listed in a Canadian business directory.

Additional criteria may be considered, such as if the business describes its services being offered in Canada or actively seeks feedback from persons or entities in Canada. (diriger des services)

Distributed ledger

For the purpose of section 151 of the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFR), a digital ledger that is maintained by multiple persons or entities and that can only be modified by a consensus of those persons or entities. (registres distribués)

Disposition

With respect to a reportable transaction, the disposition is what the funds or virtual currency was used for. For example, an individual arrives at a bank with cash and purchases a bank draft. The disposition is the purchase of the bank draft. (répartition)

Electronic funds transfer

The transmission—by any electronic, magnetic or optical means—of instructions for the transfer of funds, including a transmission of instructions that is initiated and finally received by the same person or entity. In the case of SWIFT messages,

only SWIFT MT-103 messages and their equivalent are included. It does not include a transmission or instructions for the transfer of funds:

1. (a) that involves the beneficiary withdrawing cash from their account;
2. (b) that is carried out by means of a direct deposit or pre-authorized debit;
3. (c) that is carried out by cheque imaging and presentment
4. (d) that is both initiated and finally received by persons or entities that are acting to clear or settle payment obligations between themselves; or
5. (e) that is initiated or finally received by a person or entity referred to in paragraphs 5(a) to (h.1) of the Act for the purpose of internal treasury management, including the management of their financial assets and liabilities, if one of the parties to the transaction is a subsidiary of the other or if they are subsidiaries of the same corporation.

(télévirement)

Employees profit sharing plan

Has the same meaning as in subsection 248(1) of the Income Tax Act. (régime de participation des employés aux bénéfices)

Entity

A body corporate, a trust, a partnership, a fund or an unincorporated association or organization. (entité)

Facts

Actual events, actions, occurrences or elements that exist or are known to have happened or existed. Facts are not opinions. For example, facts surrounding a transaction or multiple transactions could include the date, time, location, amount or type of transaction or could include the account details, particular business lines, or the client's financial history. (faits)

Family member

For the purposes of subsection 9.3(1) of the Act, a prescribed family member of a politically exposed foreign person, a politically exposed domestic person or a head of an international organization is:

1. (a) their spouse or common-law partner;
2. (b) their child;
3. (c) their mother or father;

4. (d) the mother or father of their spouse or common-law partner; or

5. (e) a child of their mother or father.

(membre de la famille)

Fiat currency

A currency that is issued by a country and is designated as legal tender in that country. (monnaie fiduciaire)

Final receipt

In respect of an electronic funds transfer, means the receipt of the instructions by the person or entity that is to make the remittance to a beneficiary. (destinataire)

Financial entity

Means:

1. (a) an entity that is referred to in any of paragraphs 5(a), (b) and (d) to (f) of the Act;

2. (b) a financial services cooperative;

3. (c) a life insurance company, or an entity that is a life insurance broker or agent, in respect of loans or prepaid payment products that it offers to the public and accounts that it maintains with respect to those loans or prepaid payment products, other than:

4. (i) loans that are made by the insurer to a policy holder if the insured person has a terminal illness that significantly reduces their life expectancy and the loan is secured by the value of an insurance policy;

5. (ii) loans that are made by the insurer to the policy holder for the sole purpose of funding the life insurance policy; and

6. (iii) advance payments to which the policy holder is entitles that are made to them by the insurer;

7. (d) a credit union central when it offers financial services to a person, or to an entity that is not a member of that credit union central; and

8. (e) a department, or an entity that is an agent of His Majesty in right of Canada or an agent or mandatary of His Majesty in right of a province, when it carries out an activity referred to in section 76.

(entité financière)

Financial Action Task Force

The Financial Action Task Force on Money Laundering established in 1989. (Groupe d'action financière)

Financial services cooperative

A financial services cooperative that is regulated by an Act respecting financial services cooperatives, CQLR, c. C-67.3 or the Act respecting the Mouvement Desjardins, S.Q. 2000, c. 77, other than a caisse populaire. (coopérative de services financiers)

Foreign currency

A fiat currency that is issued by a country other than Canada. (devise)

Foreign currency exchange transaction

An exchange, at the request of another person or entity, of one fiat currency for another. (opération de change en devise)

Foreign currency exchange transaction ticket

A record respecting a foreign currency exchange transaction—including an entry in a transaction register—that sets out:

1. (a) the date of the transaction;
2. (b) in the case of a transaction of $3,000 or more, the name and address of the person or entity that requests the exchange, the nature of their principal business or their occupation and, in the case of a person, their date of birth;
3. (c) the type and amount of each of the fiat currencies involved in the payment made and received by the person or entity that requests the exchange;
4. (d) the method by which the payment is made and received;
5. (e) the exchange rates used and their source;
6. (f) the number of every account that is affected by the transaction, the type of account and the name of each account holder; and
7. (g) every reference number that is connected to the transaction and has a function equivalent to that of an account number.

(fiche d'opération de change en devise)

Foreign money services business

Persons and entities that do not have a place of business in Canada, that are engaged in the business of providing at least one of the following services that is directed at persons or entities in Canada, and that provide those services to their clients in Canada:

1. (i) foreign exchange dealing,
2. (ii) remitting funds or transmitting funds by any means or through any person, entity or electronic funds transfer network,
3. (iii) issuing or redeeming money orders, traveller's cheques or other similar negotiable instruments except for cheques payable to a named person or entity,
4. (iv) dealing in virtual currencies, or
5. (v) any prescribed service.

(entreprise de services monétaires étrangère)

Foreign state

Except for the purposes of Part 2, means a country other than Canada and includes any political subdivision or territory of a foreign state. (État étranger)

Funds

Means:

1. (a) cash and other fiat currencies, and securities, negotiable instruments or other financial instruments that indicate a title or right to or interest in them; or
2. (b) a private key of a cryptographic system that enables a person or entity to have access to a fiat currency other than cash.

For greater certainty, it does not include virtual currency. (fonds)

Head of an international organization

A person who, at a given time, holds—or has held within a prescribed period before that time—the office or position of head of

1. a) an international organization that is established by the governments of states;
2. b) an institution of an organization referred to in paragraph (a); or
3. c) an international sports organization.

Immediately

In respect of submitting a Terrorist Property Report (TPR), the time period within which a TPR must be submitted, which does not allow for any delay prior to submission. (immédiatement)

Information record

A record that sets out the name and address of a person or entity and:

1. (a) in the case of a person, their date of birth and the nature of their principal business or their occupation; and
2. (b) in the case of an entity, the nature of its principal business.

(dossier de renseignements)

Initiation

In respect of an electronic funds transfer, means the first transmission of the instructions for the transfer of funds. (amorcer)

Institutional trust

For the purpose of section 15 of the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFR), means a trust that is established by a corporation or other entity for a particular business purpose and includes a pension plan trust, a pension master trust, a supplemental pension plan trust, a mutual fund trust, a pooled fund trust, a registered retirement savings plan trust, a registered retirement income fund trust, a registered education savings plan trust, a group registered retirement savings plan trust, a deferred profit sharing plan trust, an employee profit sharing plan trust, a retirement compensation arrangement trust, an employee savings plan trust, a health and welfare trust, an unemployment benefit plan trust, a foreign insurance company trust, a foreign reinsurance trust, a reinsurance trust, a real estate investment trust, an environmental trust and a trust established in respect of endowment, a foundation or a registered charity. (fiducie institutionnelle)

International electronic funds transfer

An electronic funds transfer other than for the transfer of funds within Canada. (télévirement international)

Inter vivos trust

A personal trust, other than a trust created by will. (fiducie entre vifs)

Jewellery

Objects that are made of gold, silver, palladium, platinum, pearls or precious stones and that are intended to be worn as a personal adornment. (bijou)

Large cash transaction record

A record that indicates the receipt of an amount of $10,000 or more in cash in a single transaction and that contains the following information:

1. (a) the date of the receipt;
2. (b) if the amount is received for deposit into an account, the number of the account, the name of each account holder and the time of the deposit or an indication that the deposit is made in a night deposit box outside the recipient's normal business hours;
3. (c) the name and address of every other person or entity that is involved in the transaction, the nature of their principal business or their occupation and, in the case of a person, their date of birth;
4. (d) the type and amount of each fiat currency involved in the receipt;
5. (e) the method by which the cash is received;
6. (f) if applicable, the exchange rates used and their source;
7. (g) the number of every other account that is affected by the transaction, the type of account and the name of each account holder
8. (h) every reference number that is connected to the transaction and has a function equivalent to that of an account number;
9. (i) the purpose of the transaction;
10. (j) the following details of the remittance of, or in exchange for, the cash received:
    1. (i) the method of remittance;
    2. (ii) if the remittance is in funds, the type and amount of each type of funds involved;
    3. (iii) if the remittance is not in funds, the type of remittance and its value, if different from the amount of cash received; and
    4. (iv) the name of every person or entity involved in the remittance and their account number or policy number or, if they have no account number or policy number, their identifying number; and
11. (k) if the amount is received by a dealer in precious metals and precious stones for the sale of precious metals, precious stones or jewellery:
    1. (i) the type of precious metals, precious stones or jewellery;

2. (ii) the value of the precious metals, precious stones or jewellery, if different from the amount of cash received, and

3. (iii) the wholesale value of the precious metals, precious stones or jewellery.

Large virtual currency transaction record

A record that indicates the receipt of an amount of $10,000 or more in virtual currency in a single transaction and that contains the following information:

1. (a) the date of the receipt;
2. (b) if the amount is received for deposit into an account, the name of each account holder;
3. (c) the name and address of every other person or entity that is involved in the transaction, the nature of their principal business or their occupation and, in the case of a person, their date of birth;
4. (d) the type and amount of each virtual currency involved in the receipt;
5. (e) the exchange rates used and their source;
6. (f) the number of every other account that is affected by the transaction, the type of account and the name of each account holder;
7. (g) every reference number that is connected to the transaction and has a function equivalent to that of an account number;
8. (h) every transaction identifier, including the sending and receiving addresses; and
9. (i) if the amount is received by a dealer in precious metals and precious stones for the sale of precious metals, precious stones or jewellery:
10. (i) the type of precious metals, precious stones or jewellery;
11. (ii) the value of the precious metals, precious stones or jewellery, if different from the amount of virtual currency received; and
12. (iii) the wholesale value of the precious metals, precious stones or jewellery.

Life insurance broker or agent

A person or entity that is authorized under provincial legislation to carry on the business of arranging contracts of life insurance. (représentant d'assurance-vie)

Life insurance company

A life company or foreign life company to which the Insurance Companies Act applies or a life insurance company regulated by a provincial Act. (société

d'assurance-vie)

Listed person

Has the same meaning as in section 1 of the Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism. (personne inscrite)

Managing general agents (MGAs)

Life insurance brokers or agents that act as facilitators between other life insurance brokers or agents and life insurance companies. MGAs typically offer services to assist with insurance agents contracting and commission payments, facilitate the flow of information between insurer and agent, and provide training to, and compliance oversight of, insurance agents. (agent général de gestion)

Mandatary

A person who acts, under a mandate or agreement, for another person or entity. (mandataire)

Marketing or advertising

When a person or entity uses promotional materials such as advertisements, graphics for websites or billboards, etc., with the intent to promote money services business (MSB) services and to acquire business from persons or entities in Canada. (marketing ou publicité)

Minister

In relation to sections 24.1 to 39, the Minister of Public Safety and Emergency Preparedness and, in relation to any other provision of this Act, the Minister of Finance. (ministre)

Money laundering offence

An offence under subsection 462.31(1) of the Criminal Code. The United Nations defines money laundering as "any act or attempted act to disguise the source of money or assets derived from criminal activity." Essentially, money laundering is the process whereby "dirty money"—produced through criminal activity—is transformed into "clean money," the criminal origin of which is difficult to trace. (infraction de recyclage des produits de la criminalité)

Money laundering and terrorist financing indicators (ML/TF indicators)

Potential red flags that could initiate suspicion or indicate that something may be unusual in the absence of a reasonable explanation.

Money services business

A person or entity that has a place of business in Canada and that is engaged in the business of providing at least one of the following services:

1. (i) foreign exchange dealing,
2. (ii) remitting funds or transmitting funds by any means or through any person, entity or electronic funds transfer network,
3. (iii) issuing or redeeming money orders, traveller's cheques or other similar negotiable instruments except for cheques payable to a named person or entity,
4. (iv) dealing in virtual currencies, or
5. (v) any prescribed service.

(entreprise de services monétaires)

Money services business agent

An individual or entity authorized to deliver services on behalf of a money services business (MSB). It is not an MSB branch. (mandataire d'une entreprise de services monétaires)

Mortgage administrator

A person or entity, other than a financial entity, that is engaged in the business of servicing mortgage agreements on real property or hypothec agreements on immovables on behalf of a lender. (administrateur hypothécaire)

Mortgage broker

A person or entity that is authorized under provincial legislation to act as an intermediary between a lender and a borrower with respect to loans secured by mortgages on real property or hypothecs on immovables. (courtier hypothécaire)

Mortgage lender

A person or entity, other than a financial entity, that is engaged in the business of providing loans secured by mortgages on real property or hypothecs on immovables. (prêteur hypothécaire)

Nature of principal business

An entity's type or field of business. Also applies to an individual in the case of a sole proprietorship. (nature de l'entreprise principale)

New developments

Changes to the structure or operations of a business when new services, activities, or locations are put in place. For example, changes to a business model or business restructuring. (nouveaux développements)

New technologies

The adoption of a technology that is new to a business. For example, when a business adopts new systems or software such as transaction monitoring systems or client onboarding and identification tools. (nouvelles technologies)

No apparent reason

There is no clear explanation to account for suspicious behaviour or information. (sans raison apparente)

Occupation

The job or profession of an individual. (profession ou métier)

Person

An individual. (personne)

Person authorized to give instructions

In respect of an account, means a person who is authorized to instruct on the account or make changes to the account, such as modifying the account type, updating the account contact details, and in the case of a credit card account, requesting a limit increase or decrease, or adding or removing card holders. A person who is only able to conduct transactions on the account is not considered a person authorized to give instructions. (personne habilitée à donner des instructions)

Politically exposed domestic person

A person who, at a given time, holds—or has held within a prescribed period before that time—one of the offices or positions referred to in any of paragraphs (a) and (c) to (j) in or on behalf of the federal government or a provincial government or any of the offices or positions referred to in paragraphs (b) and (k):

1. (a) Governor General, lieutenant governor or head of government;
2. (b) member of the Senate or House of Commons or member of a legislature of a province;
3. (c) deputy minister or equivalent rank;

4. (d) ambassador, or attaché or counsellor of an ambassador;
5. (e) military officer with a rank of general or above;
6. (f) president of a corporation that is wholly owned directly by His Majesty in right of Canada or a province;
7. (g) head of a government agency;
8. (h) judge of an appellate court in a province, the Federal Court of Appeal or the Supreme Court of Canada;
9. (i) leader or president of a political party represented in a legislature;
10. (j) holder of any prescribed office or position; or
11. (k) mayor, reeve or other similar chief officer of a municipal or local government.

(national politiquement vulnérable)

Politically exposed foreign person

A person who holds or has held one of the following offices or positions in or on behalf of a foreign state:

1. (a) head of state or head of government;
2. (b) member of the executive council of government or member of a legislature;
3. (c) deputy minister or equivalent rank;
4. (d) ambassador, or attaché or counsellor of an ambassador;
5. (e) military officer with a rank of general or above;
6. (f) president of a state-owned company or a state-owned bank;
7. (g) head of a government agency;
8. (h) judge of a supreme court, constitutional court or other court of last resort;
9. (i) leader or president of a political party represented in a legislature; or
10. (j) holder of any prescribed office or position.

(étranger politiquement vulnérable)

Possibility

In regards to completing a suspicious transaction report (STR), the likelihood that a transaction may be related to a money laundering/terrorist financing (ML/TF) offence. For example, based on your assessment of facts, context and ML/TF indicators you have reasonable grounds to suspect that a transaction

is related to the commission or attempted commission of an ML/TF offence. (possibilité)

Precious metal

Gold, silver, palladium or platinum in the form of coins, bars, ingots or granules or in any other similar form. (métal précieux)

Precious stones

Diamonds, sapphires, emeralds, tanzanite, rubies or alexandrite. (pierre précieuse)

Prepaid payment product

A product that is issued by a financial entity and that enables a person or entity to engage in a transaction by giving them electronic access to funds or virtual currency paid to a prepaid payment product account held with the financial entity in advance of the transaction. It excludes a product that:

1. (a) enables a person or entity to access a credit or debit account or one that is issued for use only with particular merchants; or
2. (b) is issued for single use for the purposes of a retail rebate program.

(produit de paiement prépayé)

Prepaid payment product account

An account – other than an account to which only a public body or, if doing so for the purposes of humanitarian aid, a registered charity as defined in subsection 248(1) of the Income Tax Act, can add funds or virtual currency – that is connected to a prepaid payment product and that permits:

1. (a) funds or virtual currency that total $1,000 or more to be added to the account within a 24-hour period; or
2. (b) a balance of funds or virtual currency of $1,000 or more to be maintained.

(compte de produit de paiement prépayé)

Prescribed

Prescribed by regulations made by the Governor in Council. (Version anglaise seulement)

Probability

The likelihood in regards to completing a suspicious transaction report (STR) that a financial transaction is related to a money laundering/terrorist financing (ML/TF) offence. For example, based on facts, having reasonable grounds to believe that a transaction is probably related to the commission or attempted commission of an ML/TF offence. (probabilité)

Production order

A judicial order that compels a person or entity to disclose records to peace officers or public officers. (ordonnance de communication)

Public body

Means

1. (a) a department or an agent of His Majesty in right of Canada or an agent or mandatary of His Majesty in right of a province;
2. (b) an incorporated city or town, village, metropolitan authority, township, district, county, rural municipality or other incorporated municipal body in Canada or an agent or mandatary in Canada of any of them; and
3. (c) an organization that operates a public hospital and that is designated by the Minister of National Revenue as a hospital authority under the Excise Tax Act, or an agent or mandatary of such an organization.

(organisme public)

Real estate broker or sales representative

A person or entity that is authorized under provincial legislation to act as an agent or mandatary for purchasers or vendors in respect of the purchase or sale of real property or immovables. (courtier ou agent immobilier)

Real estate developer

A person or entity that, in any calendar year after 2007, has sold to the public, other than in the capacity of a real estate broker or sales representative:

1. (a) five or more new houses or condominium units;
2. (b) one or more new commercial or industrial buildings; or
3. (c) one or more new multi-unit residential buildings each of which contains five or more residential units, or two or more new multi-unit residential buildings that together contain five or more residential units.

(promoteur immobilier)

Reasonable measures

Steps taken to achieve a desired outcome, even if they do not result in the desired outcome. For example, this can include doing one or more of the following:

- asking the client,
- conducting open source searches,
- retrieving information already available, including information held in non-digital formats, or
- consulting commercially available information.

(mesures raisonnables)

Receipt of funds record

A record that indicates the receipt of an amount of funds and that contains the following information:

1. (a) the date of the receipt;
2. (b) if the amount is received from a person, their name, address and date of birth and the nature of their principal business or their occupation;
3. (c) if the amount is received from or on behalf of an entity, the entity's name and address and the nature of their principal business;
4. (d) the amount of the funds received and of any part of the funds that is received in cash;
5. (e) the method by which the amount is received;
6. (f) the type and amount of each fiat currency involved in the receipt;
7. (g) if applicable, the exchange rates used and their source;
8. (h) the number of every account that is affected by the transaction in which the receipt occurs, the type of account and the name of each account holder;
9. (i) the name and address of every other person or entity that is involved in the transaction, the nature of their principal business or their occupation and, in the case of a person, their date of birth;
10. (j) every reference number that is connected to the transaction and has a function equivalent to that of an account number; and
11. (k) the purpose of the transaction.

(relevé de réception de fonds)

Registered pension plan

Has the same meaning as in subsection 248(1) of the Income Tax Act. (régime de pension agréé)

Registered retirement income fund

Has the same meaning as in subsection 248(1) of the Income Tax Act. (fonds enregistré de revenu de retraite)

Reliable

In respect of information that is used to verify identity, means that the source is well known, reputable, and is considered one that you trust to verify the identity of the client. (fiable)

Representative for service

An individual in Canada that has been appointed by a person or entity that is a foreign money services business (FMSB), pursuant to the PCMLTFA, to receive notices and documents on behalf of the FMSB. (représentant du service)

Risk assessment

The review and documentation of potential money laundering/terrorist financing risks in order to help a business establish policies, procedures and controls to detect and mitigate these risks and their impact. (évaluation des risques)

Sanctions evasion

Sanctions evasion offence means an offence arising from the contravention of a restriction or prohibition established by an order or a regulation made under the United Nations Act, the Special Economic Measures Act or the Justice for Victims of Corrupt Foreign Officials Act (Sergei Magnitsky Law). (contournement des sanctions)

Securities dealer

A person or entity that is referred to in paragraph 5(g) of the Act. (courtier en valeurs mobilières)

Senior officer

In respect of an entity, means:

1. (a) a director of the entity who is one of its full-time employees;

2. (b) the entity's chief executive officer, chief operating officer, president, secretary, treasurer, controller, chief financial officer, chief accountant, chief auditor or chief actuary, or any person who performs any of those functions; or

3. (c) any other officer who reports directly to the entity's board of directors, chief executive officer or chief operating officer.

(cadre dirigeant)

Service agreement

An agreement between a money services business (MSB) and an organization according to which the MSB will provide any of the following MSB services on an ongoing basis:

- money transfers;
- foreign currency exchange;
- issuing or redeeming money orders, traveller's cheques or anything similar; or
- dealing in virtual currencies.
- Crowdfunding
- Armoured Cars

(accord de relation commerciale)

Settlor

A settlor is an individual or entity that creates a trust with a written trust declaration. The settlor ensures that legal responsibility for the trust is given to a trustee and that the trustee is provided with a trust instrument document that explains how the trust is to be used for the beneficiaries. A settlor includes any individual or entity that contributes financially to that trust, either directly or indirectly. (constituant)

Shell bank

A foreign financial institution that:

1. (a) does not have a place of business that:

2. (i) is located at a fixed address—where it employs one or more persons on a full-time basis and maintains operating records related to its banking activities—in a country in which it is authorized to conduct banking activities; and

3. (ii) is subject to inspection by the regulatory authority that licensed it to conduct banking activities; and

4. (b) is not controlled by, or under common control with, a depository institution, credit union or foreign financial institution that maintains

a place of business referred to in paragraph (a) in Canada or in a foreign country.

(banque fictive)

Signature

Includes an electronic signature or other information in electronic form that is created or adopted by a client of a person or entity referred to in section 5 of the Act and that is accepted by the person or entity as being unique to that client. (signature)

Signature card

In respect of an account, means a document that is signed by a person who is authorized to give instructions in respect of the account, or electronic data that constitutes the signature of such a person. (fiche-signature)

Source

The issuer or provider of information or documents for verifying identification. (source)

Source of funds or of virtual currency (VC)

The origin of the particular funds or VC used to carry out a specific transaction or to attempt to carry out a transaction. It is how the funds were acquired, not where the funds may have been transferred from. For example, the source of funds could originate from activities or occurrences such as employment income, gifts, the sale of a large asset, criminal activity, etc. (origine des fonds ou de la monnaie virtuelle (MV))

Source of wealth

The origin of a person's total assets that can be reasonably explained, rather than what might be expected. For example, a person's wealth could originate from an accumulation of activities and occurrences such as business undertakings, family estates, previous and current employment income, investments, real estate, inheritance, lottery winnings, etc. (origine de la richesse)

Starting action

With respect to a reportable transaction, information related to the instructions provided by the person or entity making the request to the reporting entity to start a transaction. For example, an individual arrives at a bank and requests to purchase a bank draft. The starting action is the details of the instructions for the purchase which includes the funds or virtual currency that the requesting

person or entity brought to the reporting entity. A transaction must have at least one starting action. (action d'amorce)

SWIFT

The Society for Worldwide Interbank Financial Telecommunication. (SWIFT)

Terrorist activity

Has the same meaning as in subsection 83.01(1) of the Criminal Code. (activité terroriste)

Terrorist activity financing offence

An offence under section 83.02, 83.03 or 83.04 of the Criminal Code or an offence under section 83.12 of the Criminal Code arising out of a contravention of section 83.08 of that Act.

A terrorist financing offence is knowingly collecting or giving property (such as money) to carry out terrorist activities. This includes the use and possession of any property to help carry out the terrorist activities. The money earned for terrorist financing can be from legal sources, such as personal donations and profits from a business or charitable organization or from criminal sources, such as the drug trade, the smuggling of weapons and other goods, fraud, kidnapping and extortion. (infraction de financement des activités terroristes)

Third party

Any individual or entity that instructs another individual or entity to act on their behalf for a financial activity or transaction. (tiers)

Threats to the security of Canada

Has the same meaning as in section 2 of the Canadian Security Intelligence Service Act. (menaces envers la sécurité du Canada)

Training program

A written and implemented program outlining the ongoing training for your employees, agents or other individuals authorized to act on your behalf. It should contain information about all your obligations and requirements to be fulfilled under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and its associated Regulations. (programme de formation)

Trust

A right of property held by one individual or entity (a trustee) for the benefit of another individual or entity (a beneficiary). (fiducie)

Trust company

A company that is referred to in any of paragraphs 5(d) to (e.1) of the Act. (société de fiducie)

Trustee

A trustee is the individual or entity authorized to hold or administer the assets of a trust. (fiduciaire)

Tutor

In the context of civil law, a person who has been lawfully appointed to the care of the person and property of a minor. (tuteur)

Two year effectiveness review

A review, conducted every two years (at a minimum), by an internal or external auditor to test the effectiveness of your policies and procedures, risk assessment, and training program. (examen bisannuel de l'efficacité)

Valid

In respect of a document or information that is used to verify identity, appears legitimate or authentic and does not appear to have been altered or had any information redacted. The information must also be valid according to the issuer, for example if a passport is invalid because of a name change, it is not valid for FINTRAC purposes. (valide)

Verify identity

To refer to certain information or documentation, in accordance with the prescribed methods, to identify a person or entity (client). (vérifier l'identité)

Very large corporation or trust

A corporation or trust that has minimum net assets of $75 million CAD on its last audited balance sheet. The corporation's shares or units have to be traded on a Canadian stock exchange or on a stock exchange designated under subsection 262(1) of the Income Tax Act. The corporation or trust also has to operate in a country that is a member of the Financial Action Task Force (FATF). (personne morale ou fiducie dont l'actif est très important)

Violation

A contravention of the Act or the regulations that is designated as a violation by regulations made under subsection 73.1(1). (violation)

Virtual currency

Means:

1. (a) a digital representation of value that can be used for payment or investment purposes that is not a fiat currency and that can be readily exchanged for funds or for another virtual currency that can be readily exchanged for funds; or
2. (b) a private key of a cryptographic system that enables a person or entity to have access to a digital representation of value referred to in paragraph (a).

(monnaie virtuelle)

Virtual currency exchange transaction

An exchange, at the request of another person or entity, of virtual currency for funds, funds for virtual currency or one virtual currency for another. (opération de change en monnaie virtuelle)

Virtual currency exchange transaction ticket

A record respecting a virtual currency exchange transaction—including an entry in a transaction register—that sets out:

1. (a) the date of the transaction;
2. (b) in the case of a transaction of $1,000 or more, the name and address of the person or entity that requests the exchange, the nature of their principal business or their occupation and, in the case of a person, their date of birth;
3. (c) the type and amount of each type of funds and each of the virtual currencies involved in the payment made and received by the person or entity that requests the exchange;
4. (d) the method by which the payment is made and received;
5. (e) the exchange rates used and their source;
6. (f) the number of every account that is affected by the transaction, the type of account and the name of each account holder;
7. (g) every reference number that is connected to the transaction and has a function equivalent to that of an account number; and
8. (h) every transaction identifier, including the sending and receiving addresses.

(fiche d'opération de change en monnaie virtuelle)

Working days

In respect of an electronic funds transfer (EFT) report or a large virtual currency transaction report, a working day is a day between and including Monday to Friday. It excludes Saturday, Sunday, and a public holiday. (jour ouvrable)

Politically exposed persons and heads of international organizations guidance for account-based reporting entity sectors

Overview

Financial entities(FEs), securities dealers and casinos (account-based reporting entities) have politically exposed persons (PEPs) and heads of international organizations (HIOs) requirements under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and associated Regulations. However, some requirements and the examples given in this guidance only apply to certain reporting entities (REs).

References to PEPs in this guidance include both foreign and domestic PEPs, unless otherwise specified.

1. When or for whom must I make a PEP, HIO, family member or close associate determination?

You must take reasonable measures to make an account related PEP, HIO, family member or close associate (of foreign PEP only, in certain circumstances) determination:

- when you open an account;
- for authorized users of prepaid payment product accounts (PPPAs) (FEs only);
- when you conduct periodic monitoring of existing account holders;
- when you conduct periodic monitoring of authorized users of PPPAs (FEs only);
- when you detect a fact about existing account holders that indicates a PEP or HIO connection; and
- when you detect a fact about authorized users of PPPAs that indicates a PEP or HIO connection (FEs only).

See Account-related PEP or HIO determination below, for an explanation of your requirements in these instances.

If you are an FE or a casino then you must also take reasonable measures to make PEP, HIO, family member or close associate determinations for the following transactions:

- initiation of an international electronic funds transfer (EFT) in the amount of $100,000 or more;
- final receipt of an international EFT in the amount of $100,000 or more;
- receipt of cash or an amount of VC equivalent to $100,000 or more (casinos only);
- transfers of an amount of VC equivalent to $100,000 or more (FEs only);
- receipt of an amount of VC equivalent to $100,000 or more for remittance to a beneficiary (FEs only); and
- payment(s) of $100,000 or more to a PPPA (FEs only).

See Transaction-related PEP or HIO determination below, for an explanation of your requirements in these instances.

Account-related PEP or HIO determinations

Account opening As an FE, a securities dealer, or a casino, you must take reasonable measures to determine whether a person for whom you open an account is a PEP, HIO, family member of one of those persons, or close associate of a foreign PEP.Footnote 1

Authorized user of PPPA (FEs only) As an FE, you must take reasonable measures to determine whether a person identified as an authorized user of a PPPA is a PEP, HIO, family member of one of those persons, or close associate of a foreign PEP.Footnote 2

Periodic monitoring of existing account holders and authorized users of PPPAs As an FE, a securities dealer, or a casino, you must periodically take reasonable measures to determine whether a person who holds an account is a PEP, HIO, family member of one of those persons, or close associate of a foreign PEP.Footnote 3

As an FE, you must also periodically take reasonable measures to determine whether an authorized user of a PPPA is a PEP, HIO, family member of one of those persons, or close associate of a foreign PEP.Footnote 4

Detecting a fact about existing account holders and authorized users of PPPAs As an FE, a securities dealer, or a casino, if you or any of your employees or officers detect a fact that constitutes reasonable grounds to suspect that a person who holds an account is a PEP, HIO, or family member or close associate of one of these persons, you must take reasonable measures to determine whether they are such a person.Footnote 5

As an FE, if you or any of your employees or officers detect a fact that constitutes reasonable grounds to suspect that an authorized user of a PPPA is a PEP, HIO, or family member or close associate of one of these persons, you must take reasonable measures to determine whether they are such a person.Footnote 6

For more information about what it means to detect a fact about a PEP or HIO, see FINTRAC's Politically exposed persons and heads of international organizations guidance.

Transaction-related PEP or HIO determinations

Initiation of an international electronic funds transfer (EFT) in the amount of $100,000 or more As an FE or a casino, you must take reasonable measures to determine whether a person who requests that you initiate an international EFT in the amount of $100,000 or more is a PEP, HIO, or family member or close associate of one of these persons.Footnote 7

Final receipt of an international EFT in the amount of $100,000 or more As an FE or a casino, you must take reasonable measures to determine whether a beneficiary for whom you finally receive an international EFT in the amount of $100,000 or more is a PEP, HIO, or family member or close associate of one of these persons.Footnote 8

Receipt of cash or an amount of VC equivalent to $100,000 or more (casinos only) As a casino, you must take reasonable measures to determine whether a person from whom you receive cash or an amount of VC equivalent to $100,000 or more is a PEP, HIO, or family member or close associate of one of these persons.Footnote 9

Transfer of an amount of VC equivalent to $100,000 or more (FEs only) As an FE, you must take reasonable measures to determine whether a person who requests that you transfer an amount of VC equivalent to $100,000 or more is a PEP, HIO, or family member or close associate of one of these persons.Footnote 10

Receipt of an amount of VC equivalent to $100,000 or more for remittance to a beneficiary (FEs only) As an FE, you must take reasonable measures to determine whether a beneficiary for whom you receive an amount of VC equivalent to $100,000 or more is a PEP, HIO, or family member or close associate of one of these persons.Footnote 11

Payment in the amount of $100,000 or more to a PPPA (FEs only) As an FE, you must take reasonable measures to determine whether a person who makes a payment in the amount of $100,000 or more to a PPPA is a PEP, HIO, or family member or close associate of one of these persons.Footnote 12

2. What are the exceptions to making a PEP, HIO, family member or close associate determination?

You do not have to make a PEP, HIO, family member or close associate determination (as applicable) for the following:

1. If you previously determined that a person is a foreign PEP or a family member of a foreign PEP.Footnote 13
2. If you are an **FE** or **securities dealer** you do not need to determine if a person who is a member of a group plan account is a PEP, HIO or a family member or close associate of a PEP or HIO, if:Footnote 14
   - the person's member contributions are made by the sponsor of the group plan or by payroll deduction; **and**
   - the identity of the entity that is the plan sponsor has been verified in accordance with subsection 109(1) or 112(1) of the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations.
3. If you are an **FE**, you do not have to make a PEP determination or keep the associated records for your activities in respect of the processing of payments by credit card or by prepaid payment products for a merchant.Footnote 15
4. If you are an **FE** or **casino**, that initiates or is the final recipient of an international EFT of $100,000 or more, by means of a credit/debit card or a prepaid payment product where the beneficiary has an agreement with the payment service provider that permits payment by that means for the provision of goods and services, you do not need to determine if the person is a PEP, HIO or a family member or close associate of a PEP or HIO.Footnote 16

3. What measures do I need to take after making a PEP, HIO, family member or close associate determination?

Account-related measures

Foreign PEPs As an FE, a securities dealer or a casino, when you **open an account**, **conduct periodic monitoring**, or **detect a fact,** and you determine that a person who holds an account or is an authorized user of a PPPA (FEs only) is a foreign PEP or family member or close associate of a foreign PEP, you must:Footnote 17

- take reasonable measures to establish the source of the funds or source of the VC that is or is expected to be deposited into the account in question and to establish the source of the person's wealth;
- obtain the approval of a member of senior management to keep the account open; and
- take your enhanced measures, including taking additional measures to verify the person's identity, conducting enhanced ongoing monitoring and taking any other enhanced measures to mitigate the risks posed by the

person.

Domestic PEPs or HIOs As an FE, a securities dealer or a casino, when you **open an account**, **conduct periodic monitoring**, or **detect a fact,** and you determine that a person who holds an account or is an authorized user (FEs) is a domestic PEP, HIO, or family member or close associate, of a domestic PEP or HIO, **and** based on your risk assessment, you consider there to be a **high risk** of a money laundering (ML) or terrorist activity financing (TF) offence being committed, you must:Footnote 18

- take reasonable measures to establish the source of the funds or source of the VC that is or is expected to be deposited into the account in question and to establish the source of the person's wealth;
- obtain the approval of a member of senior management to keep the account open; and
- take your enhanced measures, including taking additional measures to verify the person's identity, conducting enhanced ongoing monitoring and taking any other enhanced measures to mitigate the risks posed by the person.

When you **detect a fact about an existing account,** and determine that a person is a close associate of a domestic PEP or HIO, **and** based on your risk assessment, you consider there to be a **high risk** of an ML or TF offence being committed, you must:Footnote 19

- take reasonable measures to establish the source of the funds or source of the VC that is or is expected to be deposited into the account in question and to establish the source of the person's wealth;
- obtain the approval of a member of senior management to keep the account open; and
- take your enhanced measures, including taking additional measures to verify the person's identity, conducting enhanced ongoing monitoring and taking any other enhanced measures to mitigate the risks posed by the person.

Prescribed timing for taking measures When you **open an account** for or **detect a fact** about a PEP, HIO, or family member or close associate of one of these persons, you have **30 days** after the day on which you open the account or you detect a fact to, as applicable:Footnote 20

- take reasonable measures to establish the source of the funds or source of the VC that is or is expected to be deposited into the account in question and to establish the source of the person's wealth; and
- obtain the approval of a member of senior management to keep the account open.

Transaction-related measures

Foreign PEPs

FEs When you **initiate an international EFT** for a personin the amount **of $100,000 or more** or you **process a payment to a PPPA** for a person in the amount **of $100,000 or more** and determine that the person is a foreign PEP, or a family member or close associate of a foreign PEP, you must:Footnote 21

- take reasonable measures to establish the source of the funds used for the transaction and to establish the source of the person's wealth; and
- ensure that a member of senior management reviews the transaction.

When you **transfer an amount of VC** equivalent to **$100,000 or more** for a person that you determine is a foreign PEP, or a family member or close associate of a foreign PEP, you must:Footnote 22

- take reasonable measures to establish the source of the VC used for the transaction and to establish the source of the person's wealth; and
- ensure that a member of senior management reviews the transaction.

When you **receive for a beneficiary an international EFT or an amount of VC** equivalent to **$100,000 or more** and determine that the beneficiary is a foreign PEP, or a family member or close associate of a foreign PEP, you must ensure that a member of senior management reviews the transaction.Footnote 23

Casinos When you **initiate an international EFT** in the amount **of $100,000 or more, finally receive an international EFT for a beneficiary** in the amount **of $100,000 or more**, or **receive cash, or an amount of VC equivalent to, $100,000 or more,** and determine that a person is a foreign PEP, or a family member or close associate of a foreign PEP, you must:Footnote 24

- take reasonable measures to establish the source of the funds or source of the VC used for the transaction and to establish the source of the person's wealth; and
- ensure that a member of senior management reviews the transaction.

Domestic PEPs or HIOs

FEs When you **initiate an international EFT** in the amount **of $100,000 or more** or **process a payment to a PPPA** in the amount **of $100,000 or more**, for a person that you determine is a domestic PEP, HIO, or family member or close associate of a domestic PEP or HIO **and,** based on your risk assessment, you consider there to be a **high risk** of an ML or TF offence being committed, you must:Footnote 25

- take reasonable measures to establish the source of the funds used for the transaction and to establish the source of the person's wealth; and
- ensure that a member of senior management reviews the transaction.

When you **transfer an amount of VC** equivalent to **$100,000 or more,** and determine that a person is a domestic PEP, HIO, or family member or close associate of a domestic PEP or HIO, **and** based on your risk assessment, you consider there to be a **high risk** of an ML or TF offence being committed, you must:Footnote 26

- take reasonable measures to establish the source of the VC used for the transaction and to establish the source of the person's wealth; and
- ensure that a member of senior management reviews the transaction.

When you **receive for a beneficiary an international EFT or an amount of VC equivalent to $100,000 or more** and determine that the beneficiary is a domestic PEP, HIO, or family member or close associate of a domestic PEP or HIO, **and** based on your risk assessment, you consider there to be a **high risk** of an ML or TF offence being committed, you must ensure that a member of senior management reviews the transaction.Footnote 27

Casinos When you **initiate an international EFT** in the amount **of $100,000 or more**, **finally receive for a beneficiary an international EFT** in the amount **of $100,000 or more,** or **receive cash or an amount of VC** equivalent to **$100,000 or more,** and determine that a person is a domestic PEP, HIO, or family member or close associate of a domestic PEP or HIO, **and** based on your risk assessment, you consider there to be a **high risk** of an ML or TF offence being committed, you must:Footnote 28

- take reasonable measures to establish the source of the funds or source of the VC used for the transaction and to establish the source of the person's wealth; and
- ensure that a member of senior management reviews the transaction.

Prescribed timing for taking measures As an FE or a casino, for the transactions referred to above, you have **30 days** after the day on which the transaction is conducted to, as applicable:Footnote 29

- take reasonable measures to make a PEP, HIO, family member, or close associate determination, and if applicable, establish the source of the funds or source of the VC used for the transaction and to establish the person's source of wealth, and ensure that a member of senior management reviews the transaction; **or**
- take reasonable measures to make a PEP, HIO, family member, or close associate determination, and if applicable, ensure that a member of senior management reviews the transaction.

4. What PEP, HIO, family member or close associate records do I need to keep?

You must keep the following records related to your determination that a person is a PEP, HIO, or a family member or close associate of a PEP or HIO:

PEP and HIO account records

If you determine that a person is a foreign PEP, a family member, or close associate of a foreign PEP, a high-risk domestic PEP, high-risk HIO or high-risk family member or high-risk close associate of one of these persons, and you obtained the approval of a member of senior management to keep an account open, you must keep a record of:Footnote 30

- the office or position and the name of the organization or institution of the PEP or HIO;
- the date of the determination;
- the source of the funds or VC, if known, that is or is expected to be deposited into the account or paid to the PPPA;
- the source of the person's wealth, if known;
- the name of the member of senior management who approved keeping the account open; and
- the date of that approval.

In the case of family members and close associates of PEPs and HIOs, you may also want to keep a record of the nature of the relationship between the person and the PEP or HIO, as applicable.

Retention: You must keep PEP and HIO account records for at least five years from the day the account to which they relate is closed.Footnote 31

PEP and HIO transaction records

If as an FE or a casino, you **review** one of the above-mentioned transactions (see Transaction related PEP or HIO determinations) for which you have made a PEP or HIO determination, you must keep a record of:Footnote 32

- the office or position and the name of the organization or institution of the PEP or HIO;
- the date of the determination;
- the source of the funds or source of the VC used for the transaction, if known;
- the source of the person's wealth, if known;
- the name of the member of senior management who reviewed the transaction; and
- the date of that review.

In the case of family members and close associates of PEPs and HIOs, you may also want to include in the record the nature of the relationship between the

person and the PEP or HIO, as applicable.

Retention: You must keep transaction records for at least 5 years from the day on which the last business transaction is conducted.Footnote 33

Politically exposed persons and heads of international organizations guidance for non-account-based reporting entity sectors : FINTRAC's compliance guidance

This guidance explains the requirement to make a politically exposed person and head of international organizations determination for non-account-based reporting entity sectors.

1. Who must comply

The following non-account-based reporting entities have requirements regarding politically exposed persons and heads of international organizations under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and associated Regulations:

- Accountants
- Agents of the Crown
- British Columbia notaries
- Dealers in precious metals and precious stones
- Real estate developers, brokers and sales representatives
- Money services businesses, and foreign money services businesses
- Mortgage administrators, mortgage brokers and mortgage lenders

For **life insurance companies, brokers and agents**, consult: Politically exposed persons and heads of international organizations guidance for life insurance companies, brokers and agents.

For more information about your obligations to determine who is a politically exposed person, a head of an international organization, or a person related or closely associated to one of those persons, and clarity on terminology and related considerations (e.g. who is considered a member of senior management), consult: Politically exposed persons and heads of international organizations.

2. When to make a determination

You must take reasonable measures to determine whether a person with whom you enter into a business relationship is a politically exposed person, a head of an international organization, a family member of one of those persons, or a close associate of a foreign politically exposed person (in certain circumstances) when you:

- enter into a business relationship
- conduct periodic monitoring of a business relationship, and
- detect a fact that constitutes reasonable grounds to suspect they are politically exposed person or head of an international organization , family member, or close associate

You must also take reasonable measures to make a determination regarding politically exposed persons, heads of international organizations, family members or close associates to one of those persons for certain transactions. Consult the Transaction-related politically determinations section of this guidance.

Business relationship-related determinations

Entering into a business relationship You must take reasonable measures to determine whether a person with whom you enter into a business relationship is a politically exposed person, head of an international organization, family member of one of those persons, or close associate of a foreign politically exposed person.

Periodic monitoring of business relationships You must periodically take reasonable measures to determine whether a person with whom you have a business relationship is a politically exposed person, a head of an international organization, a family member of one of those persons, or close associate of a foreign politically exposed person.

Detecting a fact about existing business relationships If you, or any of your employees or officers, detects a fact that constitutes reasonable grounds to suspect that a person with whom you have a business relationship is a politically exposed person, head of an international organization, or a family member or close associate of one of these persons, you must take reasonable measures to determine whether they are such a person.

Transaction-related determinations

You must take reasonable measures to determine whether a person is a politically exposed person, a head of an international organization, a family member or close associate of one of those persons for certain transactions, as applicable:

Accountants, agents of the Crown, British Columbia notaries, dealers in precious metals and precious stones, mortgage administrators, mortgage brokers and mortgage lenders, and real estate developers, brokers and sale representatives

- Receipt of an amount of $100,000 or more in cash or an amount of virtual currency equivalent to $100,000 or more

Money services businesses and foreign money services businesses You must determine requestor when:

- Initiation of an international electronic funds transfer in the amount of $100,000 or more
- Transfer of an amount of virtual currency equivalent to $100,000 or more
- Transport of an amount of $100,000 or more in cash, money orders, traveler's cheques, or other similar negotiable instruments or an amount of virtual currency equivalent to $100,000 or more

You must determine beneficiary when:

- Final receipt of an international electronic funds transfer in the amount of $100,000 or more
- Receipt of an amount of virtual currency equivalent to $100,000 or more for remittance to a beneficiary

3. What are the exceptions

You do not have to make a politically exposed person or family member determination if you already determined that a person is a foreign politically exposed person or a family member of a foreign politically exposed person.

4. What measures to take

In this section

- Business relationship-related measures
- Transaction-related measures

Business relationship-related measures

Measures for foreign politically exposed persons When you **enter into a business relationship**, **conduct periodic monitoring of business relationships**, or **detect a fact about an existing business relationship,** and determine that a person is a foreign politically exposed person or family member or close associate of a foreign politically exposed person, you must:

- take reasonable measures to establish the person's source of wealth, and
- take enhanced measures, including the following:
  - taking additional measures to verify the person's identity
  - conducting enhanced ongoing monitoring of the business relationship
  - taking any other enhanced measures to mitigate the risks posed by the person

Measures for domestic politically exposed persons or heads of international organizations When you **enter into a business relationship**,

conduct periodic monitoring of business relationships, or **detect a fact about an existing business relationship,** and determine that a person is a domestic politically exposed person, head of an international organization, or family member of a domestic politically exposed person or head of an international organization, and based on your risk assessment, you consider there to be a **high risk** of a money laundering or terrorist activity financing offence being committed, you must:

- take reasonable measures to establish the person's source of wealth, and
- take enhanced measures, including the following:
  - taking additional measures to verify the person's identity
  - conducting enhanced ongoing monitoring of the business relationship
  - taking any other enhanced measures to mitigate the risks posed by the person

When you **detect a fact about an existing business relationship,** and determine that a person is a close associate of a domestic politically exposed person or head of an international organization, and based on your risk assessment, you consider there to be a **high risk** of a money laundering or terrorist financing offence being committed, you must:

- take reasonable measures to establish the person's source of wealth, and
- take enhanced measures, including the following:
  - taking additional measures to verify the person's identity
  - conducting enhanced ongoing monitoring of the business relationship
  - taking any other enhanced measures to mitigate the risks posed by the person

Timing to establish the source of wealth When you **enter into a business relationship** with, or **detect a fact** about a politically exposed person, head of an international organization, or family member or close associate of one of these persons, you have **30 days** after the day on which you enter into the business relationship or detect a fact to take reasonable measures to establish the source of a person's wealth, if applicable.

Transaction-related measures

Measures for foreign politically exposed persons Accountants, agents of the Crown, British Columbia notaries, dealers in precious metals and precious stones, mortgage administrators, mortgage brokers or mortgage lenders and real estate developers, brokers or sales representatives

When you receive an amount of $100,000 or more in cash or an amount of virtual currency equivalent to $100,000 or more, and determine that a person is a foreign politically exposed person or family member or close associate of a foreign politically exposed person, you must:

- take reasonable measures to establish the source of the cash or source of the virtual currency used for the transaction and the source of the person's wealth, and
- ensure that a member of senior management reviews the transaction

Money services businesses and foreign money services businesses

When in providing services to people located in Canada, you conduct one of the following transactions:

- initiating an international electronic funds transfer in an amount of $100,000 or more
- transferring an amount of virtual currency equivalent to $100,000 or more
- transporting an amount of $100,000 or more in cash, money orders, traveler's cheques, or other similar negotiable instruments (except for cheques payable to a named person or entity) or an amount of virtual currency equivalent to $100,000 or more

and you determine that the person is a foreign politically exposed person or family member or close associate of a foreign politically exposed person, you must:

- take reasonable measures to establish the source of the funds or virtual currency used for the transaction and to establish the source of the person's wealth, and
- ensure that a member of senior management reviews the transaction

When in providing services to people located in Canada, you:

- finally receive an international electronic funds transfer or an amount of virtual currency equivalent to $100,000 or more for a beneficiary
- and determine that the person is a foreign politically exposed person or family member or close associate of a foreign politically exposed person

You must ensure that a member of senior management reviews the transaction.

Measures for domestic politically exposed persons or heads of international organizations Accountants, agents of the Crown, British Columbia notaries, dealers in precious metals and precious stones, mortgage administrators, mortgage brokers or mortgage lenders, and real estate developers, brokers or sales representatives

When you:

- receive an amount of $100,000 or more in cash or an amount of virtual currency equivalent to $100,000 or more **,** and
- determine that the person is a domestic politically exposed person, head of an international organization, or family member or close associate of a domestic politically exposed person or head of an international organization, **and**

- based on your risk assessment, you consider there to be a **high risk** of a money laundering or terrorist financing offence being committed

You must:

- take reasonable measures to establish the source of the funds or source of the virtual currency used for the transaction and to establish the source of the person's wealth, and
- ensure that a member of senior management reviews the transaction

Money services businesses and foreign money services businesses

When in providing services to people located in Canada, you:

- initiate an international electronic funds transfer in the amount of $100,000 or more at the request of a person, and
- determine that the person is a domestic politically exposed person, head of an international organization, or family member or close associate of a domestic politically exposed person or head of an international organization, **and**
- based on your risk assessment, you consider there to be a **high risk** of a money laundering or terrorist financing offence being committed

You must:

- take reasonable measures to establish the source of the funds used for the transaction and to establish the source of the person's wealth, and
- ensure that a member of senior management reviews the transaction

When in providing services to people located in Canada, you:

- transfer an amount of virtual currency equivalent to $100,000 or more, and
- determine that the person is a domestic politically exposed person, head of an international organization, or family member or close associate of a domestic politically exposed person or head of an international organization, **and**
- based on your risk assessment, you consider there to be a **high risk** of a money laundering or terrorist financing offence being committed

You must:

- take reasonable measures to establish the source of the virtual currency used for the transaction and to establish the source of the person's wealth, and
- ensure that a member of senior management reviews the transaction

When in providing services to people located in Canada, you:

- receive for a beneficiary an international electronic funds transfer or an amount of virtual currency equivalent to $100,000 or more, and

- determine that the beneficiary is a domestic politically exposed person, head of an international organization, or family member or close associate of a domestic politically exposed person or head of an international organization, **and**
- based on your risk assessment, you consider there to be a **high risk** of a money laundering or terrorist financing offence being committed

You must ensure that a member of senior management reviews the transaction.

Prescribed timing for taking measures Accountants, agents of the Crown, British Columbia notaries, dealers in precious metals and precious stones, mortgage administrators, mortgage brokers or mortgage lenders, and real estate developers, brokers or sales representatives

When you **receive an amount of $100,000 or more in cash or an amount of virtual currency equivalent to $100,000 or more**, you have **30 days** after the day on which the transaction is conducted to:

1. take reasonable measures to determine whether a person is a politically exposed person, a head of an international organization, a family member, or close associate, and
2. if you make such a determination, take reasonable measures to:
   - establish the source of the cash or source of the virtual currency used for the transaction
   - establish the person's source of wealth, and
   - ensure that a member of senior management reviews the transaction

Money services businesses and foreign money services businesses

In providing services to people located in Canada, for the applicable transactions referred to above in this section, you have **30 days** after the day on which the transaction is conducted to:

1. take reasonable measures to determine whether a person is a politically exposed person, a head of an international organization, a family member or close associate, and
2. if you make such a determination:
   - establish the source of the funds or source of the virtual currency used for the transaction, and
   - establish the person's source of wealth,
   - and ensure that a member of senior management reviews the transaction

or

1. take reasonable measures to determine whether a person is a politically exposed person, a head of an international organization, a family member or close associate, and

2. if you make such a determination, ensure that a member of senior management reviews the transaction

5. What records to keep

Records on business relationships involving politically exposed persons and heads of international organizations

When you **enter into a business relationship**, **conduct periodic monitoring of business relationships**, or **detect a fact about an existing business relationship,** and determine that the person is a politically exposed person, a head of an international organization, or a family member or close associate of one of those persons, you must keep a record of:

- the office or position and the name of the organization or institution of the politically exposed person or head of an international organization
- the date of the determination, and
- the source of the person's wealth, if known

Retention: You must keep records on business relationships involving politically exposed persons and heads of international organizations for at least five years after the day on which they were created.

Records on transactions involving politically exposed persons and head of international organizations

Accountants, agents of the Crown, British Columbia notaries, dealers in precious metals and precious stones, mortgage administrators, mortgage brokers or mortgage lenders, and real estate developers, brokers or sales representatives

If senior management **reviews** a transaction where you had **received an amount of $100,000 or more in cash or an amount of virtual currency equivalent to $100,000 or more** for which you determined a person was a politically exposed person or a head of an international organization, then you must keep a record of:

- the office or position and the name of the organization or institution of the politically exposed person or head of an international organization or a family member or close associate of one of those persons
- the date of the determination
- the source of the cash or virtual currency used for the transaction, if known
- the source of the person's wealth, if known
- the name of the member of senior management who reviewed the transaction, and
- the date of that review

In the case of family members and close associates of politically exposed persons and heads of international organizations, you may also want to include in the

record the nature of the relationship between the person and the politically exposed person or head of an international organization, as applicable.

Retention: If you review a prescribed transaction involving a politically exposed person or a head of an international organization, then you must keep these transaction records for at least 5 years after the day on which they were created.

Money services businesses and foreign money services businesses

If, when providing services to people located in Canada, you review an applicable prescribed transaction listed under Transaction-related politically exposed person or head of an international organization determinations for which you have determined a person is a politically exposed person or a head of an international organization determination, then you must keep a record of:

- the office or position and the name of the organization or institution of the politically exposed person or head of an international organization
- the date of the determination
- the source of the funds or source of the virtual currency used for the transaction (if known)
- the source of the person's wealth (if known)
- the name of the member of senior management who reviewed the transaction, and
- the date of that review

You may also want to include in the record the nature of the relationship between the family member or close associate and the politically exposed person or head of an international organization, as applicable.

Retention: If you review a prescribed transaction involving a politically exposed person or a head of an international organization transaction, then you must keep these transaction records for at least 5 years from the day on which the last business transaction is conducted.

Record keeping requirements for financial entities

Overview

Financial entities (FEs) have record keeping requirements under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and associated Regulations.

This guidance outlines certain record keeping requirements for FEs.

1. What records must I keep and what must they contain?

You must keep the following records:

1. Reports – a copy of every report sent to FINTRAC
    - Suspicious Transaction Reports
    - Terrorist Property Reports
    - Large Cash Transaction Reports
    - Large Virtual Currency Transaction Reports
    - Electronic Funds Transfer Reports
2. Large cash transaction records
3. Large virtual currency transaction records
4. Records of transactions of $3,000 or more
5. Records of electronic funds transfers of $1,000 or more
6. Records of virtual currency transfers in amounts equivalent to $1,000 or more
7. Foreign currency exchange transaction tickets
8. Virtual currency exchange transaction tickets
9. Account records
    - Records for account holders and persons authorized to give instructions
    - Signature cards
    - Intended use of an account
    - Applications
    - Account operating agreements
    - Debit and credit memos
    - Deposit slips
    - Account statements
    - Cleared cheque records
    - Credit arrangement records
10. Credit card account and transaction records
11. Prepaid payment product account and transaction records
12. Trust records

****Note:** When you are required to keep records about clients, you should beas descriptive as possible. Being descriptive when recording the nature of the principal business or occupation of a client will help determine whether a transaction or activity is consistent with what would be expected for that client. For example, when the client's occupation is "manager", the record should reflect the area of management, such as "hotel reservations manager" or "retail clothing store manager". When an entity's principal business area is "sales", the record should specify the type of sales, such as "pharmaceutical sales" or "retail sales".

a. Reports – a copy of every report sent to FINTRAC

You must keep a copy of every report that you submit to FINTRAC as a record.

Suspicious Transaction Reports When you submit a Suspicious Transaction Report (STR) to FINTRAC, you must keep a copy of it.Footnote 1

Retention: At least five years after the day the STR was submitted.Footnote

Terrorist Property Reports When you submit a Terrorist Property Report (TPR) to FINTRAC, you must keep a copy of it.Footnote 3

Retention: At least five years after the day the TPR was submitted.Footnote 4

Large Cash Transaction Reports When you submit a Large Cash Transaction Report (LCTR) to FINTRAC, you must keep a copy of it.Footnote 5

Retention: At least five years from the date the LCTR was created.Footnote 6

Large Virtual Currency Transaction Reports When you submit a Large Virtual Currency Transaction Report (LVCTR) to FINTRAC, you must keep a copy of it.Footnote 7

Retention: At least five years from the date the LVCTR was created.Footnote 8

Electronic Funds Transfer Reports When you submit an Electronic Funds Transfer Report (EFTR) to FINTRAC, you must keep a copy of it.Footnote 9

Retention: At least five years from the date the EFTR was created.Footnote 10

b. Large cash transaction records

You must keep a large cash transaction record when you receive $10,000 or more in cash.Footnote 11

If you authorize a person or an entity to receive funds on your behalf, and that person or entity receives $10,000 or more in cash in accordance with the authorization, you are deemed to have received the amount when it is received by the person or entity, and you must keep a large cash transaction record.Footnote 12

****Note**: This requirement is subject to the 24-hour rule.Footnote 13

A large cash transaction record must include:Footnote 14

- the date you received the cash;
- if the amount is received for deposit into an account:
  - the account number(s);
  - the name of each account holder—if the cash was deposited into more than one client account, all names must be included in the record; and

  - the time of the deposit, if it was made during your normal business hours, or an indication of "night deposit" if the deposit was made outside of your normal business hours;
- for any person involved in the transaction (including the person from whom you received the cash), their name, address, date of birth, and occupation, or in the case of a sole proprietor, the nature of their principal business;
- for any entity involved in the transaction (including the entity from which you received the cash), their name, address and nature of their principal business;
- the type and amount of each fiat currency received;
- the purpose of the transaction (for example, the cash was used to purchase a money order, etc.);
- the method by which you received the cash (for example, in person, by mail, by armoured car, etc.);
- the exchange rates used and their source (if applicable);
- if other accounts are affected by the transaction, include:
  - the account number and type of account (for example, business, personal, etc.); and
  - the name of each account holder;
- every reference number connected to the transaction that is meant to be similar to an account number;
- the following details about the remittance (i.e. the disposition) of, or exchange for, the cash received:
  - the method of remittance (for example, wire transfer, money order, etc.);
  - if the remittance is in funds, the type and amount of each type of funds involved;
  - if the remittance is not in funds, the type of remittance (for example, virtual currency, etc.) and value if different from the amount received in cash; and
  - the name of every person or entity involved in the remittance, their account number or policy number. If there is no account or policy number, their identifying number.

Retention: At least five years from the date the large cash transaction record was created.Footnote 15

c. Large virtual currency transaction records

You must keep a large virtual currency (VC) transaction record when you receive VC in an amount equivalent to $10,000 or more.Footnote 16

If you authorize a person or an entity to receive VC on your behalf, and that person or entity receives VC in an amount equivalent to $10,000 or more in accordance with the authorization, you are deemed to have received the VC when it is received by the person or entity, and you must keep a large VC

transaction record.Footnote 17

****Note**: This requirement is subject to the 24-hour rule.Footnote 18

A large VC transaction record must include:Footnote 19

- the date you received the VC;
- if you received the amount for deposit into an account, the name of each account holder;
- for any person involved in the transaction (including the person from whom you received the VC), their name, address, date of birth, and their occupation, or in the case of a sole proprietor, the nature of their principal business;
- for any entity involved in the transaction (including the entity from which you received the VC), their name, address and the nature of their principal business;
- the type and amount of each VC involved in the receipt;
- the exchange rates used and their source;
- if other accounts are affected by the transaction, include:
  - the account number and type of account; and
  - the name of each account holder;
- every reference number connected to the transaction that is meant to be similar to an account number; and
- every transaction identifier (this may include a transaction hash or similar identifier, if applicable), and every sending and receiving address.

Retention: At least five years from the date the large virtual currency transaction record was created.Footnote 20

d. Records of transactions of $3,000 or more

Issuance of traveller's cheques, money orders or similar negotiable instruments When you receive $3,000 or more in funds or an equivalent amount in VC, from a person or entity, for the issuance of traveller's cheques, money orders or other similar negotiable instruments you must record:Footnote 21

- the date you received the funds or VC;
- if you received the amount from a person, their name, address, date of birth and their occupation, or in the case of a sole proprietor, the nature of their principal business;
- if you receive the amount from an entity, its name, address and nature of its principal business;
- the amount received;
- the type and amount of each type of funds and each type of the VC's involved;
- if an account is affected by the transaction:
  - the account number and account type; and
  - the name of each account holder;

- every reference number that is connected to the transaction that is meant to be similar to an account number;
- if the received amount is in VC, every transaction identifier including transaction hashes or similar identifiers (if applicable), and every sending and receiving addresses.

Redemption of money orders When you redeem one or more money orders, for a total value of $3,000 or more, in funds or in an equivalent amount of VC you must record:Footnote 22

- the date the money orders were redeemed;
- if the client is a person, their name, address, date of birth and their occupation, or in the case of a sole proprietor, the nature of their principal business;
- if the client is an entity, its name, address and nature of its principal business;
- the total amount of the money orders or money orders;
- the name of the issuer of each money order;
- if an account is affected by the redemption:
  - the account number and account type; and
  - the name of each account holder;
- every reference number connected to the redemption that is meant to be similar to an account number; and
- if the redemption involves VC, every transaction identifier, including transaction hashes or similar identifiers (as applicable), and every sending and receiving address.

Retention: At least five years from the date the record for a transaction of $3,000 or more was created.Footnote 23

e. Records of electronic fund transfers of $1,000 or more

Initiating an international electronic funds transfer of $1,000 or more When you initiate, at the request of a person or an entity, an international electronic funds transfer or any other electronic funds transfer (EFT) that is a SWIFT MT-103 message or equivalent valued at $1,000 or more you must record:Footnote 24

- the date the EFT was initiated;
- the type and amount of each type of funds involved in the initiation;
- if the client is a person, their name, address, date of birth, telephone number and their occupation, or in the case of a sole proprietor, the nature of their principal business;
- if the client is an entity, its name, address, telephone number and nature of its principal business;
- the exchange rates used and their source;
- the name and address of each beneficiary;

- if an account is affected by the initiation
  - the account number and account type; and
  - the name of each account holder;
- the number of every account that is affected by the EFT, other than those affected by the initiation; and
- every reference number that is connected to the EFT and is meant to be similar to an account number.

Sending an international EFT of $1,000 or more When you send, as an intermediary, an international EFT of $1,000 or more that was initiated by another reporting entity, you must record:Footnote 25

- the date the EFT was sent;
- if fiat currencies were exchanged in the course of sending the EFT, the type and amount of each fiat currency involved in the exchange;
- the exchange rates used and their source;
- for every account affected by the sending:
  - the account number and account type; and
  - the name of each account holder;
- every reference number connected to sending the EFT that is meant to be similar to an account number;
- the name and address of the person or entity who requested the initiation of the EFT, unless after taking reasonable measures that information was not included with the transfer and it is not otherwise known; and
- the name and address of each beneficiary, unless after taking reasonable measures that information was not included with the transfer and it is not otherwise known.

Final receipt of an international EFT of $1,000 or more When you are the final recipient of an international EFT of $1,000 or more, you must record:Footnote 26

- the date the EFT was finally received;
- the type and amount of each type of funds involved in the final receipt;
- the name, address, date of birth and nature of the principal business, in the case of a sole proprietor, or occupation of each person who is a beneficiary;
- the name, address and nature of the principal business of each entity that is a beneficiary;
- the date of the remittance;
- the exchange rates used for the remittance and their source;
- if the remittance is in funds, the type and amount of each type of funds involved in the remittance;
- if the remittance is not in funds, the type of remittance (for example, virtual currency, precious stones, etc.), and its value, if different from the amount of funds finally received;
- for every account affected by the final receipt or remittance:

    - the account number and account type; and
    - the name of each account holder;
- every reference number connected to the EFT that is meant to be similar to an account number;
- the name and address of the person or entity that requested the initiation of the EFT, unless after taking reasonable measures, that information was not included with the transfer and it is not otherwise known; and
- the number of every account that is affected by the EFT, other than those affected by the final receipt or remittance.

****Note:** When you initiate, send as an intermediary, or finally receive an EFT, you must include with the transfer the prescribed information in accordance with the travel rule. Please see FINTRAC's travel rule guidance for more information.

Retention: At least five years from the date the EFT record was created.Footnote 27

f. Records of virtual currency transfers in amounts equivalent to $1,000 or more

VC transfer in an amount equivalent to $1,000 or more When you transfer VC in an amount equivalent to $1,000 or more at the request of a person or entity, you must record:Footnote 28

- the date of the transfer;
- the type and amount of each VC that is involved in the transfer;
- if the client is a person, their name, address, date of birth and occupation, or in the case of a sole proprietor, the nature of their principal business;
- if the client is an entity, its name, address and the nature of its principal business;
- the name and address of each beneficiary;
- for every account affected by the transfer:
    - the account number and account type; and
    - the name of each account holder;
- every reference number connected to the transaction that is meant to be similar to an account number;
- every transaction identifier including transaction hashes or similar identifiers (if applicable) and every sending and receiving address; and
- the exchange rates used and their source.

Receipt of VC in an amount equivalent to $1,000 or more for remittance to a beneficiary When you receive VC in an amount equivalent to $1,000 or more for remittance to a beneficiary, you must record: Footnote 29

- the date of the receipt;
- the type and amount of each VC that is received;

- if the beneficiary is a person, the name, address, date of birth and occupation, or in the case of a sole proprietor, the nature of their principal business of each beneficiary;
- if the beneficiary is an entity, the name, address and the nature of principal business of each beneficiary;
- the date of the remittance;
- the exchange rates used for the remittance and their source;
- if the remittance is in VC, the type and amount of each VC involved in the remittance;
- if the remittance is not in VC, the type and value of the remittance, if different from the value of the received VC;
- for every account affected by the transaction:
  - the account number and account type; and
  - the name of each account holder;
- every reference number connected to the transaction that is meant to be similar to an account number;
- every transaction identifier, including transaction hashes or similar identifiers (if applicable), and every sending and receiving address; and
- the name and address of the person or entity that requested the transfer, unless that information was not, despite the taking of reasonable measures, included with the transfer and is not otherwise known.

****Note:** When you transfer VC, you must include with the transfer the prescribed information in accordance with the travel rule. When you receive VC, you must take reasonable measures to ensure that the transfer includes the prescribed information. Please see FINTRAC's travel rule guidance for more information.

Retention: At least five years from the date the VC transfer or VC receipt record was created.Footnote 30

g. Foreign currency exchange transaction tickets

You must keep a transaction ticket, which may take the form of an entry in a transaction register, for every foreign currency exchange transaction you conduct, regardless of the amount.Footnote 31 Each transaction ticket must include:Footnote 32

- the date of the transaction;
- if the transaction was of $3,000 or more and requested by a person, their name, address, date of birth and occupation, or in the case of a sole proprietor, the nature of their principal business;
- if the transaction was of $3,000 or more and requested by an entity, its name, address and the nature of its principal business;
- type and amount of each fiat currency received from the client and the type and amount of each fiat currency given to the client;
- the method by which the payment was made and received;

- the exchange rates used and their source;
- for every account affected by the transaction:
  - the account number and account type; and
  - the name of each account holder;
- every reference number that is connected to the transaction that is meant to be similar to that of an account number.

Retention: At least five years from the date the foreign exchange transaction record was created.Footnote 33

h. VC exchange transaction tickets

You must keep a VC exchange transaction ticket, which may take the form of an entry in a transaction register, for every VC exchange transaction you conduct, regardless of the amount.Footnote 34 Each transaction ticket must include:Footnote 35

- the date of the transaction;
- if the VC transaction was equivalent to $1,000 or more and requested by a person, their name, address, date of birth and occupation, or in the case of a sole proprietor, the nature of their principal business;
- if the VC transaction was equivalent to $1,000 or more and requested by an entity, its name, address and the nature of its principal business;
- the type and amount of each fund and each VC involved in the payment made and received by the client;
- the method (VC currency exchange business) by which the payment was made and received;
- the exchange rates used and their source;
- for every account affected by the transaction:
  - the account number and account type; and
  - the name of each account holder;
- every reference number connected to the transaction that is meant to be similar to that of an account number; and
- every transaction identifier, including transaction hashes or similar identifiers (if applicable), and every sending and receiving address.

Retention: At least five years from the date the VC exchange transaction record was created.Footnote 36

i. Account records

For every account opened for a client, you must keep the following records:

Records for account holders and persons authorized to give instructions You must keep a record for every account holder (person, corporation, or other entity) and for every other person (up to three, in the case of a business account) who is authorized to give instructions in respect of the account.Footnote 37

For a **person,** the record must include their name, address, date of birth and their occupation, or in the case of a sole proprietor, the nature of their principal business.Footnote 38

For an account holder that is **a corporation or an entity other than a corporation**, the record must include its name, address and the nature of its principal business.Footnote 39

For a **corporation**, you must also keep a copy of the part of its official corporate records that contains any provision relating to the power to bind the corporation regarding the account.Footnote 40 This could be found in, for example:

- the articles of incorporation; or
- the bylaws of the corporation that set out the officers duly authorized to sign on behalf of the corporation, such as the president, treasurer, vice-president, comptroller, etc.

Retention: At least five years from the date the record was created. However, if this information is kept in one of the other account records, then the retention of that other record applies – at least five years from the date the account is closed.Footnote 41

Signature cards You must keep a signature card for every person authorized to give instructions on an account you open.Footnote 42 It can include the person's handwritten signature or an electronic signature that was created or adopted by the person.

An electronic signature can be numeric, character-based, or biometric, so long as it is unique to the person and a record can be kept. An electronic signature may also be encrypted. For example, a client's personal identification number (PIN) can be used as an electronic signature. FINTRAC's expectation is that it will be possible to review a signature card record during an examination, but the electronic signature does not need to be unencrypted.

You can keep a single signature card for a client that holds multiple accounts; you do not need to create a new signature card every time a client opens a subsequent account.

Retention: At least five years from the date the account was closed.Footnote 43

Intended use of an account You must keep a record of the intended use of an account.Footnote 44

Examples of the intended use of personal accounts include, but are not limited to:

- general chequing services, such as payment of family and household expenses;
- saving to fund a large purchase, retirement, or for a child's education; or

- receiving directly deposited employment or pension income.

Examples of the intended use of business accounts include, but are not limited to:

- depositing of daily business receipts (sales, etc.);
- making payments to employees (payroll);
- general business operating expenses; or
- making payments to suppliers.

Retention: At least five years from the date the account was closed.Footnote 45

Applications You must also keep a record of every application in respect of an account.Footnote 46

Retention: At least five years from the date the account was closed.Footnote 47

Account operating agreements You must keep every account operating agreement that you create or receive. An account operating agreement is a document that outlines the agreement between you and your client about the account's operation. For example, an application for a deposit account or a mortgage can include a reference to a separate document setting out the terms and conditions of the account's operation. The account operating agreement record in that case would include both the application and the separate document.Footnote 48

Retention: At least five years from the date the account was closed.Footnote 49

Debit and credit memos You must keep every debit and credit memo that you create or receive regarding an account. However, you do not need to keep a debit memo that relates to another account held at the same branch.Footnote 50 That is, you do not have to keep duplicate debit memos. If you have kept a debit memo in relation to two accounts at a given branch, you are only required to keep one memo on record.

Retention: At least five years from the date the debit or credit memo was created.Footnote 51

Deposit slips You must keep a deposit slip for every deposit to an account.Footnote 52 A deposit slip means a record that includes: Footnote 53

- the date of the deposit;
- the name of the person or entity that made the deposit;
- the amount of the deposit, and any part of the deposit that was made in cash;

- the method by which the deposit was made; and
- the number of the account the deposit went into and the name of each account holder.

Retention: At least five years from the date the deposit slips were created.Footnote 54

Account statements You must keep a copy of every account statement you send to an account holder.Footnote 55

Retention: At least five years from the date the account statements were created.Footnote 56

Cleared cheque records You must keep a record of every cleared cheque drawn on an account, and a copy of every cleared cheque that is deposited to an account.Footnote 57

This does not apply to cheques drawn from an account and deposited to an account at the same branch.

It also does not apply if an image of the cheque has been recorded electronically or on microfilm, which can be readily reproduced, and it can be readily ascertained where the image is recorded.

Retention: At least five years from the date the cleared cheques records were created and at least five years from the date the image was recorded in the case of a microfilm or electronic medium.Footnote 58

Credit arrangement records You are required to keep the following information with respect to a credit arrangement that you have entered into with a client: Footnote 59

- a record of the client's financial capacity;
- the terms of the credit arrangement;
- the nature of the client's principal business or their occupation; and
- if the client is a person, the name and address of their business or place of work.

Retention: At least five years from the date the account was closed.Footnote 60

j. Credit card account and related transaction records

Records for account holders and persons authorized to give instructions You must keep a record for every credit card account holder (person, corporation, or other entity) and for every other person (up to three, in the case of a business account) that is authorized to give instructions in respect of the account.Footnote 61

For a **person,** the record must include their name, address, date of birth and occupation or, in the case of a sole proprietor, the nature of their principal business.Footnote 62

For an account holder that is **a corporation or an entity other than a corporation**, the record must include its name, address and the nature of its principal business.Footnote 63

For **a corporation**, you must also keep a copy of the part of its official corporate records that contains provisions relating to the power to bind the corporation in respect of the credit card account or credit card transactions.Footnote 64 This could be found in, for example:

- the articles of incorporation; or
- the bylaws of the corporation that set out the officers duly authorized to sign on behalf of the corporation, such as the president, treasurer, vice-president, comptroller, etc.

Retention: At least five years from the date the record was created. However, if this information is kept in one of the other credit card account records, then the retention of that other record applies – at least five years from the date the account is closed. Footnote 65

Other account records You must keep the following records for every credit card account:

- every credit card application related to the account;Footnote 66 and
- a copy of every credit card statement that you sent to an account holder.Footnote 67

Retention: You must keep a credit card application for at least five years from the date the account was closed and credit card statements for at least five years from the day they were created.Footnote 68

Transaction records You must keep the following records when transactions are related to a credit card account:

- a foreign currency exchange transaction ticket for every foreign currency exchange transaction (See Foreign currency exchange transaction tickets);Footnote 69
- a VC exchange transaction ticket for every VC exchange transaction (See VC exchange transaction tickets);Footnote 70
- a record of the initiation of an international EFT of $1,000 or more that was requested by a person or an entity and for which the funds were transferred from the account (See Initiating an EFT of $1,000 or more);Footnote 71and
- a record of the final receipt of an international EFT of $1,000 or more that was remitted to a beneficiary by payment to the credit card account (See Final receipt of an international EFT of $1,000 or more).Footnote 72

Retention: At least five years from the date the transaction records were created.Footnote 73

k. Prepaid payment product account and transaction records

Records for account holders and authorized users You must keep a record for every prepaid payment product (PPP) account holder (person, corporation, or other entity) and for every authorized user.Footnote 74

For a **person,** the record must include their name, address, date of birth, occupation and in the case of a sole proprietor, the nature of their principal business.Footnote 75

For each PPP account holder that is **a corporation or an entity other than a corporation**, the record must include its name, address and the nature of its principal business.Footnote 76

When you open a PPP account for a **corporation**, you must also keep a copy of the part of its official corporate records that contains any provision relating to the power to bind the corporation in respect of the PPP account or PPP account transactions.Footnote 77

Retention: At least five years from the date the record was created. However, if this information is kept in one of the other account records, then the retention of that other record applies – at least five years from the date the account is closed.Footnote 78

Other account records You must keep the following records for every PPP account:

- every application related to the PPP account;Footnote 79
- every debit and credit memo you created or received related to the PPP account;Footnote 80
- a copy of every account statement sent to the holder of the PPP account;Footnote 81 and
- a prepaid payment product slip for every payment made to the PPP accountFootnote 82 that includes:
  - the date of the payment;
  - the name of the person or entity that made the payment;
  - the type and amount of each type of funds or each of the VC's involved in the payment;
  - the method by which the payment was made;
  - the name of each PPP account holder; and
  - the account number and, if different, the number that identifies the PPP that is connected to the account.Footnote 83

Retention: You must keep PPP account applications for at least five years from the date the account was closed and the other records listed above for at least five years from the date they were created.Footnote 84

PPP account transaction records You must keep the following records when transactions are related to a PPP account:

- a foreign currency exchange transaction ticket for every foreign currency exchange transaction (See Foreign currency exchange transaction tickets);Footnote 85
- a VC exchange transaction ticket for every VC exchange transaction (See VC exchange transaction tickets);Footnote 86
- a record of the initiation of an international EFT of $1,000 or more that was requested by a person or an entity for which the funds were transferred from a PPP account (See Initiating an EFT of $1,000 or more);Footnote 87
- a record of the final receipt of an international EFT of $1,000 or more that was remitted to a beneficiary by payment to a PPP account (See Final receipt of an EFT of $1,000 or more);Footnote 88
- a record of the transfer of VC in amount equivalent to $1,000 or more from a PPP account (See VC transfer in an amount equivalent to $1,000 or more);Footnote 89 and
- a record of the receipt of VC in an amount equivalent to $1,000 or more that was remitted to a beneficiary by payment to a PPP account (See Receipt of VC in an amount equivalent to $1,000 or more).Footnote 90

Retention: At least five years from the date the transaction records were created.Footnote 91

** **Note**: Please see FINTRAC's Prepaid payment products and prepaid payment product accounts guidance for more information.

l. Trust records

A trust company is an FE that is regulated by the Trust and Loan Companies Act or by an equivalent provincial Act. Trust companies have record keeping obligations related to the trusts for which they are the trustee.

A trust is a legal agreement by which financial assets are held by a person or an entity (a trustee) in trust for the benefit of another person, group of persons or entity (beneficiaries). The settlor of a trust is the person or entity that creates a trust with a written trust declaration.

You must keep the following records for every trust for which you are trustee, in addition to the transaction and account records listed previously in this guidance:Footnote 92

- a copy of the trust deed;

- if the settlor is a person, their name, address, date of birth and occupation or, in the case of a sole proprietor, the nature of their principal business; and
- if the settlor is an entity, its name, address and nature of its principal business.

You may also have record keeping obligations for certain institutional and inter vivos trusts. Institutional trusts are established by a corporation, partnership or other entity for a particular business purpose. Whereas, inter vivos trusts are established by a living person for the benefit of another person, such as a trust created by a parent for a child so that the trust's assets can be distributed to the child (beneficiary) during or after the parent's (settlor) lifetime.

If the trust is an institutional trust and the settlor is a corporation, you have to keep a copy of the part of the official corporate records that contains provisions relating to the power to bind the settlor/corporation in respect of the trust.

If the trust is an inter vivos trust (personal trust other than a trust created by a will), you have to keep a record about each of the beneficiaries that are known to you which must include:Footnote 93

- if the beneficiary is a person, their name, date of birth, address, telephone number and occupation or, in the case of a sole proprietor, the nature of their principal business;
- if the beneficiary is an entity, its name, address, telephone number and the nature of its principal business.

This information needs to be recorded for each beneficiary known to you at the time you become trustee of the trust.

2. What are my responsibilities when maintaining records?

In order to comply with your record keeping requirements, you must keep records in such a manner that they can be provided to FINTRAC within 30 days of a request.Footnote 94 The records may also be requested through a judicial order by law enforcement to support an investigation of money laundering or terrorist activity financing. A record (or a copy) may be kept in a machine-readable or electronic form, so long as a paper copy can easily be produced.Footnote 95

Employees who keep records for you are not required to keep them after their employment ends. The same is true for persons in a contractual relationship with you, when the contractual relationship ends, they no longer have to keep records for you.Footnote 96 You have to obtain and keep the records that were kept for you by an employee or a contractor before the end of the person's employment or contract.

There may be situations where you are required to keep records for purposes other than complying with your obligations under the PCMLTFA. For example,

a federal or provincial regulator may require you to keep records in addition to those described in this guidance. If this is the case, you must still meet the requirements described in this guidance. For example, the retention period for your records can be longer than what is described, but it cannot be shorter.

3. What are the exceptions to the record keeping requirements?

If you are required to keep a record with information that is readily available in other records, you do not have to record the information again.Footnote 97

For example, when you keep a copy of a large cash transaction report (LCTR) you may choose to use this as your large cash transaction record for the same transaction, so long as **all of the information** that would otherwise be kept in the large cash transaction record is captured within the report. Any requirement related to keeping the large cash transaction record would still apply, such as verifying identity.

EFTs conducted by credit/debit card or PPP You do not need to keep the following records associated with a credit/debit card or PPP transaction if the beneficiary has an agreement with the payment service provider that allows for the payment of goods and services by those means when you:Footnote 98

- initiate, send or are the final recipient of an international EFT of $1,000 or more; or
- initiate or are the final recipient of an international EFT of $1,000 or more where the funds are transferred from or to a credit card or PPP account.

Payment card processing activities

If you are processing credit card or PPP payments on behalf of a merchant (for example, credit card acquiring), the record keeping requirements described in this guidance do not apply to those activities.Footnote 99

A credit card acquiring business is an FE that has an agreement with a merchant to provide the following services:

- enabling the merchant to accept credit card payments by cardholders for goods and services and to receive payment for credit card purchases;
- processing services, payment settlements and providing point-of-sale equipment (such as computer terminals); and
- providing other ancillary services to the merchant.

Financial entities, public bodies, and very large corporations or trusts

You do not have to keep a large cash transaction record or a large VC transaction record if the cash or VC was received from another FE, a public body, or a person who is acting on behalf of a client that is an FE or public body.Footnote 100

If you receive $3,000 or more from a client that is an FE, or a person who is acting on behalf of a client that is an FE, for the issuance of traveller's cheques, money orders or other similar negotiable instruments, you are not required to keep a record of the transaction.Footnote 101

If you open an account, a credit card account, a PPP account, or conduct a transaction for a public body, a very large corporation or trust, or a subsidiary of those entities if the financial statements of the subsidiary are consolidated with those of the public body, very large corporation or trust, you are not required to keep the following records:Footnote 102

- Records of transactions of $3,000 or more;
- Records of EFTs of $1,000 or more;
- Records of VC transfers and receipt equivalent to $1,000 or more;
- Foreign currency exchange transaction records;
- VC exchange transaction records;
- Account records;
- PPP account records;
- Credit card account records; and
- Trust records.

Virtual currency

When you transfer or receive VC as compensation for the validation of a transaction that is recorded in a distributed ledger, **or** when you exchange, transfer, or receive a nominal amount of VC for the sole purpose of validating a different transaction or a transfer of information, you do not need to keep a record of: Footnote 103

- large VC transactions;
- transfers of $1,000 or more in VC at the request of a person or entity;
- receipt of $1,000 or more in VC for remittance to a beneficiary; or
- VC exchange transaction tickets.

Other record keeping exempted activities You do not have to keep the transaction and account records identified in this guidance for the following activities:Footnote 104

- the sale of an exempt policy as defined in subsection 306(1) of the Income Tax Regulations;
- the sale of a group life insurance policy that does not provide for a cash surrender value or a savings component;
- the sale of an immediate or deferred annuity that is paid for entirely with funds that are directly transferred from a registered pension plan or from a pension plan that is required to be registered under the Pension Benefits Standards Act, 1985, or similar provincial legislation;
- the sale of a registered annuity policy or a registered retirement income fund;

- the sale of an immediate or deferred annuity that is paid for entirely with the proceeds of a group life insurance policy;
- a transaction that is part of a reverse mortgage or a structured settlement;
- the opening of an account for the deposit and sale of shares from a corporate demutualization or the privatization of a Crown corporation;
- the opening of an account in the name of an affiliate of an FE, if that affiliate carries out activities that are similar to those of persons and entities referred to in paragraphs 5(a) to (g) of the PCMLTFA;
- the opening of a registered plan account, including a locked-in retirement plan account, a registered retirement savings plan account and a group registered retirement savings plan account;
- the opening of an account established in accordance with the escrow requirements of a Canadian securities regulator, the Canadian stock exchange, or any provincial legislation;
- the opening of an account where the account holder or settlor is a pension fund that is regulated under federal or provincial legislation;
- the opening of an account in the name of or in respect of which, instructions are authorized to be given by an FE, a securities dealer or a life insurance company or by an investment fund that is regulated under provincial securities legislation; or
- an account opened solely to provide customer accounting services to a securities dealer.

These exceptions do not apply to large cash transactions, large VC transactions, or suspicious transactions.

Group Plans If you open a group plan account (other than those for which exceptions already apply) you do **not** have to keep a signature card for a person who is a member of the plan if:

- the identity of the entity that is the plan sponsor has been verified; and
- the individual member contributions are made by the sponsor of the plan or by payroll deductions.Footnote 105

When to verify the identity of persons and entities—Financial entities

Overview

This guidance on client identification describes **when** financial entities (FEs) must verify the identity of persons and entities as required by the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and associated Regulations.

Who is this guidance for

- Financial entities

1. When do I have to verify the identity of persons and entities?

As an FE, you must verify the identity of clients for the following:

1. Large cash transactions
2. Large virtual currency (VC) transactions
3. Suspicious transactions
4. Issuing or redeeming money orders, traveller's cheques or other similar negotiable instruments of $3,000 or more
5. Initiating an international electronic funds transfer (EFT)—or any other EFT that is a SWIFT MT-103 message or its equivalent—of $1,000 or more
6. Remitting funds to the beneficiary of an international EFT of $1,000 or more
7. Transferring VC in an amount equivalent to $1,000 or more
8. Remitting VC to a beneficiary in an amount equivalent to $1,000 or more
9. Foreign currency exchange transactions of $3,000 or more
10. VC exchange transactions in amounts equivalent to $1,000 or more
11. Accounts—account holders and persons authorized to give instructions
12. Credit card accounts—account holders
13. Prepaid payment product (PPP) accounts
    - Account holders
    - Authorized users
    - Payments of $1,000 or more to PPP account
14. Trusts—settlors or co-trustees of a trust

a. Large cash transactions

You must verify the identity of every person or entity from which you receive $10,000 or more in cash when the transaction takes place.Footnote 1 This includes a situation where you are deemed to have received cash because you have authorized another person or entity to receive it on your behalf.

****Note**: This obligation is subject to the 24-hour rule.

b. Large virtual currency (VC) transactions

You must verify the identity of every person or entity from which you receive VC in an amount equivalent to $10,000 or more when the transaction takes place.Footnote 4 This includes a situation where you are deemed to have received VC because you have authorized another person or entity to receive it on your behalf.Footnote 5

****Note**: This obligation is subject to the 24-hour rule.

c. Suspicious transactions

You must take reasonable measures to verify the identity of every person or entity that conducts or attempts to conduct a suspicious transaction, regardless of the transaction amount, and including transactions that would normally be exempt from client identification requirements, before sending a Suspicious Transaction Report (STR).Footnote 7

d. Issuing or redeeming money orders, traveller's cheques or other similar negotiable instruments of $3,000 or more

You must verify the identity of every person who requests that you issue or redeem money orders, traveller's cheques or similar negotiable instruments of $3,000 or more when the transaction is being requested. Footnote 8

e. Initiating an international electronic funds transfer (EFT)—or any other EFT that is a SWIFT MT-103 message or its equivalent—of $1,000 or more

You must verify the identity of every person who requests the initiation of an international EFT or any other EFT that is a SWIFT MT-103 or its equivalent, including domestic SWIFT MT-103, of $1,000 or more when the transaction is being requested.Footnote 9

f. Remitting funds to the beneficiary of an international EFT of $1,000 or more

You must verify the identity of every person you remit funds to who is the beneficiary of an international EFT of $1,000 or more when the transaction takes place.Footnote 10

g. Transferring VC in an amount equivalent to $1,000 or more

You must verify the identity of every person who requests the transfer of VC in an amount equivalent to $1,000 or more when the transaction is being requested.Footnote 11

h. Remitting VC to a beneficiary in an amount equivalent to $1,000 or more

You must verify the identity of every person you remit VC to as the beneficiary of a transfer that is equivalent to $1,000 or more when the transaction takes place.Footnote 12

i. Foreign currency exchange transactions of $3,000 or more

You must verify the identity of every person who requests a foreign currency exchange of $3,000 or more when the transaction takes place.Footnote 13

j. VC exchange transactions in amounts equivalent to $1,000 or more

You must verify the identity of every person who requests that you exchange VC for funds, funds for VC, or one VC for another, in an amount equivalent to $1,000 or more when the transaction is being requested.Footnote 14

k. Accounts—Account holders and persons authorized to give instructions

Account holders You must verify the identity of every person, corporation, and entity other than a corporation for which you open an account.Footnote 15 You must do this **before** the first transaction other than when the initial deposit is carried out.Footnote 16

Persons authorized to give instructions You must verify the identity of every person authorized to give instructions on an account before the first transaction, other than the initial deposit, is carried out on the account.Footnote 17

This includes verifying the identity of the individual members of a **group plan account** who are authorized to give instructions **,** when a contribution to the plan is made in respect of the member.Footnote 18

You cannot open an account for a person, corporation, or other entity if you cannot verify their identity in accordance with the Regulations.Footnote 19

l. Credit card accounts—account holders

You must verify the identity of every person, corporation, and other entity for which you open a credit card accountFootnote 20 before the credit card can be activated.Footnote 21 If credit cards are issued for persons other than the account holder, you must record their information if they are authorized to give instructions on an account, but you do not have to verify their identity.

For example, a parent applying for a credit card account requests that a credit card be issued on that account for their child, and that child be authorized to give instructions on that account. In this example, the parent's identity has to be verified because the parent is the account holder, the child's identity does not need to be verified.

If there are two or more co-applicants for a credit card account (in other words, if a credit card account is opened in the name of more than one person), the identification requirement applies to all co-applicants.

m. Prepaid payment product (PPP) accounts

Account holders You must verify the identity of every person, corporation, and other entity for which you open a PPP accountFootnote 22 before the PPP account is activated.Footnote 23

Authorized users You must also verify the identity of every authorized user of the PPP accountFootnote 24 before the first transaction is carried out.Footnote 25

Payments of $1,000 or more to PPP Accounts You must verify the identity of every person, corporation, and other entity that makes a payment of $1,000 or more to a PPP accountFootnote 26 when the transaction takes place.Footnote 27

n. Trusts—settlors or co-trustees of a trust

If you are a trust company, you must verify the identity of every person who is the **settlor** of an inter vivos trust for which you are a trustee.Footnote 28

You must also verify the identity of a corporation or an entity other than a corporation that is the **settlor** of an institutional trust for which you are a trustee.Footnote 29

You must verify the identity of any person who is authorized to act as **co-trustee** of a trust.Footnote 30 If an entity is authorized to act as **co-trustee** of a trust, you must verify its identity and the identity of all persons authorized to give instructions on its behalf (up to three).Footnote 31

You must verify the identity of a person or an entity within 15 days after the day on which the trust company becomes the trustee.Footnote 32

2. What is the difference between verifying identity and keeping client identification information up to date?

As part of your ongoing monitoring requirements for business relationships, you must keep client identification information up to date, at a frequency that will vary based on your risk assessment, and as outlined in your policies and procedures.Footnote 33 This does not require you to re-identify clients in accordance with the methods to verify identity. As explained in the ongoing monitoring guidance, the requirement is only for you to keep client identification information up to date. This is understood to be information that you have about your client such as their name and address. In the case of a person, this would also include, but is not limited to, the nature of their principal business or their occupation; and in the case of an entity, the nature of its principal business.

3. What are the exceptions to client identification requirements?

You do not have to re-identify a person or an entity if you previously did so using the methods specified by the Regulations in place at the time, and kept the associated records, so long as you have no doubts about the information used.Footnote 34

Large cash transactions

You do not have to verify the identity of a person or entity that conducts a large cash transaction if:

- you receive the cash from another FE or a public body, or from a person who is acting on behalf of a client that is an FE or a public body;Footnote 35 or
- the amount received is deposited to a business account or is deposited in an automated banking machine (including a quick drop or night deposit).Footnote 36

Large VC transactions

You do not have to verify the identity of a person or entity that conducts a large VC transaction if you receive the VC from a client that is an FE or a public body, or from a person acting on behalf of a client that is an FE or public body.Footnote 37

When you transfer or receive VC as compensation for the validation of a transaction that is recorded in a distributed ledger **or** you exchange, transfer or receive a nominal amount of VC for the sole purpose of validating another transaction or a transfer of information – you do not need to keep a large VC transaction record and do not need to verify identity.Footnote 38

Suspicious transactions

You do not have to take reasonable measures to verify the identity of the person or entity that conducts or attempts to conduct a suspicious transaction if:

- you have already verified the identity of the person or entity and have no doubts about the identification information;Footnote 39 or
- you believe that verifying the identity of the person or entity would inform them that you are submitting an STR.Footnote 40

EFT by credit/debit card or PPP

Your client identification requirements do not apply when you carry out the following transactions for a person by means of a credit/debit card or PPP, if the beneficiary has an agreement with the payment service provider that permits payments by those means for goods and services:Footnote 41

- initiate an international EFT of $1,000 or more; or
- are the final recipient of an international EFT, or of a VC transfer equivalent to $1000 or more and remit the funds to the beneficiary.

Payment card processing activities

Client identification requirements do not apply to processing credit card or PPP payments on behalf of a merchant.Footnote 42

Public bodies, very large corporations and trusts

When opening an account, including a credit card account, PPP account or trust account, you do not have to verify the identity of a person or entity if it is for:Footnote 43

- a public body;
- a very large corporation or trust; or
- a subsidiary of those types of entities, if the financial statements of the subsidiary are consolidated with those of the public body, or very large corporation or trust.

Account openings

You do not have to verify the identity of the person that opens an account, is authorized to give instructions in respect of an account, opens a credit card account, or is the settlor or co-trustee of a trust in the following circumstances:Footnote 44

- if the person already has an account with you and opens a subsequent account;
- if the person is authorized on a business account, so long as you have verified the identity of at least three persons authorized to give instructions on the account. If one of the three identified persons leaves the business, you must verify the identity of another person authorized on the account;
- an account that is opened for the sale of mutual funds where there are reasonable grounds to believe that the client's identity has been verified by a securities dealer in accordance with the Regulations in respect of:
  - the sale of the mutual funds for which the account has been opened, or
  - a transaction that is part of a series of transactions that includes that sale; and
- an account that is opened at the request of an entity for the deposit, by a life insurance company affiliated with that entity, of a death benefit under a life insurance policy or annuity where:
  - the account is opened in the name of a beneficiary that is a person;
  - only the death benefit may be deposited in the account, and;

– the policy or annuity contract, under which the death benefit claim was made, has been in existence for at least two years before the death benefit claim was made.

Other activities exempted from client identification requirements

You do not have to verify the identity of persons and entities, as listed in this guidance, for the following:Footnote 45

- the sale of an exempt policy as defined in subsection 306(1) of the Income Tax Regulations;
- the sale of a group life insurance policy that does not provide for a cash surrender value or a savings component;
- the sale of an immediate or deferred annuity that is paid for entirely with funds that are directly transferred from a registered pension plan or from a pension plan that must be registered under the Pension Benefits Standards Act, 1985 or similar provincial legislation;
- the sale of a registered annuity policy or a registered retirement income fund;
- the sale of an immediate or deferred annuity that is paid for entirely with funds from the proceeds of a group life insurance policy;
- a transaction that is part of a reverse mortgage (a loan based on the equity of a home) or a structured settlement (a financial or insurance arrangement to resolve a personal injury claim);
- the opening of an account for the deposit and sale of shares from a corporate demutualization or the privatization of a Crown corporation;
- the opening of an account in the name of an affiliate of an FE, if that affiliate carries out activities that are similar to those of persons and entities referred to in paragraphs 5(a) to (g) of the Act;
- the opening of a registered plan account, including a locked-in retirement plan account, a registered retirement savings plan account, and a group registered retirement savings plan account;
- the opening of an account established pursuant to the escrow requirements of a Canadian securities regulator or Canadian stock exchange or any provincial legislation;
- the opening of an account where the account holder or settlor is a pension fund that is regulated under federal or provincial legislation;
- the opening of an account in the name of, or in respect of which instructions are authorized to be given by an FE, a securities dealer, a life insurance company, or an investment fund that is regulated under provincial securities legislation; and
- the opening of an account solely to provide customer accounting services to a securities dealer.

These exceptions do not apply to large cash transactions, large VC transactions, or suspicious transactions.

Group Plans

If you open a group plan account, other than those for which exceptions already apply, you do **not** have to verify the identity of the individual members of the plan if:

- the identity of the entity that is the plan sponsor has been verified; and
- the individual member contributions are made by the sponsor of the plan or by payroll deduction.

Correspondent banking relationship requirements : FINTRAC's compliance guidance

From: Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)

This guidance explains the correspondent banking relationship requirements under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (the Act) and associated Regulations that apply to financial entities.

In this guidance

Related links

Related acts and regulations

- Proceeds of Crime (Money Laundering) and Terrorist Financing Act
- Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations
- Proceeds of Crime (Money Laundering) and Terrorist Financing Suspicious Transaction Reporting Regulations

Related guidance

- Compliance program requirements
- Risk assessment guidance
- Reporting suspicious transactions to FINTRAC
- Special Bulletin on financial activity associated with suspected sanctions evasion

- Report suspected sanctions evasion
- Reporting terrorist property to FINTRAC
- Voluntary self-declaration of non-compliance

Related resources

- Policy interpretations database
- Penalties for non-compliance
- Guidance glossary
- Learning resources for businesses

1. Who must comply

The following Canadian financial entities are subject to the correspondent banking requirement if it enters into a correspondent banking relationship:

- bank
- cooperative credit society
- credit union
- caisse populaire
- federally or provincially regulated trust or loan company
- unregulated trust company
- financial services cooperative
- life insurance company, or an entity that is a life insurance broker or agent, that offers loans or prepaid payment products to the public, **or** maintains accounts for these loans or prepaid payment products, other than:
  - loans made by the insurer to a policy holder if the insured person has a terminal illness that significantly reduces their life expectancy and the loan is secured by the value of an insurance policy
  - loans made by the insurer to a policy holder for the sole purpose of funding the life insurance policy
  - advance payments made by the insurer to a policy holder who is entitled to them
- credit union central when it offers financial services to non-members
- an agent of the Crown when it accepts deposit liabilities while providing financial services to the public
- loan companies regulated by a Provincial Act

Legal references

- Proceeds of Crime (Money Laundering) and Terrorist Financing Act, S.C. 2000, Chapter.17, paragraphs 5(a),(b), (d), (e), (e.1), and (f)

- Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations, SOR/2002-184, section 16(1)

2. What is a correspondent banking relationship

A correspondent banking relationship is created by an agreement or arrangement between a prescribed foreign financial institution and a Canadian financial entity (as defined above). In this relationship, the Canadian financial entity provides prescribed services to the foreign financial institution or international electronic funds transfers, cash management, or cheque clearing services.

Legal references

- Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations, SOR/2002-184, subsection 9.4 (3)

3. What must I do to meet the requirements

Before you enter into a correspondent banking relationship, you **must**:

- Obtain information about the foreign financial institution and its activities to fulfil the related **verifying** and **record keeping requirements** outlined in this guidance.
- Ensure that the foreign financial institution is not a shell bank.
  - If it is a shell bank, you **cannot** enter into the correspondent banking relationship.
- Obtain the approval of senior management to enter into the correspondent banking relationship.
- Set out in writing your obligations and the foreign financial institution's obligations for the correspondent banking services (for example, your correspondent banking agreement or arrangement, or product agreements).

When you enter into a correspondent banking relationship, you **must also** do the following:

- Periodically conduct ongoing monitoring of the correspondent banking relationship, at a frequency appropriate to the level of risk determined in your risk assessment, for the purpose of:
  - detecting any suspicious transactions that you are required to report to FINTRAC
  - keeping the information that is required to enter into a correspondent banking relationship up to date
  - ensure that the foreign financial institution has appropriate anti-money laundering and anti-terrorist financing measures in place
  - reassessing the level of risk associated with the foreign financial institution's transactions, and

  - determining whether the transactions or activities are consistent with the information obtained about the foreign financial institution and with your risk assessment

- Verify the name and address of the foreign financial institution by examining a copy of:
  - the foreign financial institution's banking licence
  - its banking charter
  - the authorization or certification to operate that is issued by the competent authority under the legislation of the jurisdiction in which the foreign financial institution was incorporated
  - its certificate of incorporation, or
  - a similar document.

- Take reasonable measures to verify, based on publicly available information, if civil or criminal penalties have been imposed on the foreign financial institution for not respecting anti-money laundering, or anti-terrorist financing requirements, and
  - **if penalties have been imposed**, you must monitor all transactions conducted in the context of the correspondent banking relationship to detect any suspicious transactions that must be reported to FINTRAC.

- Take reasonable measures to assess, based on publicly available information:
  - the reputation of the foreign financial institution with respect to its compliance with anti-money laundering and anti-terrorist financing requirements, and
  - the quality of the anti-money laundering and anti-terrorist financing supervision of the jurisdiction in which the foreign financial institution was incorporated, and the jurisdiction that it conducts transactions in the context of the correspondent banking relationship.

- Take reasonable measures to determine the nature of the clientele and markets served by the foreign financial institution.

- Take reasonable measures to ascertain whether the foreign financial institution has anti-money laundering, and anti-terrorist financing policies and procedures in place, including procedures for the approval of the opening of new accounts, and
  - **if the reasonable measures you took were unsuccessful or the policies and procedures are not in place**, you must take reasonable measures to monitor all transactions conducted in the context of the correspondent banking relationship for the purpose of detecting suspicious transactions.

- As part of your risk assessment within your compliance program, you must assess and document money laundering, or terrorist activity financing risks related to your correspondent banking relationships.

Legal references

- Proceeds of Crime (Money Laundering) and Terrorist Financing Act
  - section 7
  - subsection 9.31(1)
  - subsection 9.4(1)
- Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations, SOR/2002-184
  - subsection 16(3.1)
  - paragraphs 90(a), 90(b) and 90(c)
  - subsection 16(3)
  - paragraph 156(c) (i)
- Proceeds of Crime (Money Laundering) and Terrorist Financing Suspicious Transaction Reporting Regulations, SOR/2001-317
  - section 9

4. What correspondent banking relationship records do I need to keep

When you enter into a correspondent banking relationship, you must keep the following records:

- A record of the foreign financial institution's name and address, primary business line and the names of its directors.
- A copy of the foreign financial institution's most recent annual report or audited financial statement.
- A copy of one of the following:
  - the foreign financial institution's banking license, banking charter, authorization or certification to operate issued by the competent authority under the legislation of the jurisdiction in which it was incorporated
  - its certificate of incorporation, or
  - a similar document.
- A copy of the correspondent banking agreement or arrangement, or product agreements, defining the respective responsibilities of your financial entity and of the foreign financial institution.
- A record of the anticipated correspondent banking account activity of the foreign financial institution, including the products or services to be used.

- A written statement from the foreign financial institution that it does not have, directly or indirectly, a correspondent banking relationship with a shell bank.
- A written statement from the foreign financial institution that it is in compliance with anti-money laundering, and anti-terrorist financing legislation in every jurisdiction in which it operates.
- A record of measures taken to determine the nature of the clientele and markets served by the foreign financial institution.
- A record of the measures taken to ascertain whether any civil or criminal penalties have been imposed on the foreign financial institution for not respecting anti-money laundering, and anti-terrorist financing requirements, and the results of those measures.
- A record of the measures taken to assess the reputation of the foreign financial institution with respect to its compliance with anti-money laundering and anti-terrorist financing requirements and the result of those measures.
- A record of the measures taken to assess the quality of the anti-money laundering and anti-terrorist financing supervision of the jurisdiction in which the foreign financial institution is incorporated and the jurisdiction in which it conducts transactions in the context of the correspondent banking relationship, and the results of those measures.
- A copy of every Suspicious Transaction Report and Terrorist Property Report sent to FINTRAC as a result of your correspondent banking relationship(s).

Retention: At least five years after the day on which the last business transaction is conducted.

Legal references

- Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations, SOR/2002-184
  - subsection 16(2)
  - paragraph 148 (1)(b)

5. What must I do if the client of a foreign financial institution has direct access to the services I provide

If, as part of a correspondent banking relationship, a client of the foreign financial institution has direct access to services you provide, you must take reasonable measures to verify whether the foreign financial institution:

- has met requirements that are consistent with your requirements for verifying client identification for this client, and

- has agreed to provide relevant client identification information to you upon request.

Legal references

- Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations, SOR/2002-184
  - section 91

6. What are the exceptions to correspondent banking relationship requirements

For a correspondent banking relationship, you do not need to keep account opening and transaction records (other than what is included in this Guidance) when you open an account for a foreign financial institution.

Also, certain correspondent banking relationship requirements do not apply to your activities related to the processing of payments by credit card or prepaid payment product for a merchant, including:

- Keeping correspondent banking relationships records (as listed under What correspondent banking relationship records do I need to keep)
- Taking reasonable measures to determine whether the foreign financial institution has anti-money laundering and anti-terrorist financing policies and procedures in place, including procedures for the approval of the opening of new accounts, and
  - **if the reasonable measures you took were unsuccessful or the policies and procedures are not in place**, you must take reasonable measures to monitor all transactions conducted in the context of the correspondent banking relationship for the purpose of detecting suspicious transactions and terrorist activities.
- Periodically conducting ongoing monitoring of the correspondent banking relationship, at a frequency appropriate to the level of risk determined in your risk assessment, for the purpose of:
  - detecting any suspicious or terrorist activity financing transactions that you are required to report to FINTRAC
  - keeping the information that is required to enter a correspondent banking relationship (see above) up to date
  - reassessing the level of risk associated with the foreign financial institution's transactions and activities related to the correspondent banking relationship, and
  - determining whether transactions and activities are consistent with the information obtained, through the risk assessment, of the foreign financial institution

Legal references

- Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations, SOR/2002-184
  - section 16
  - section 150

For assistance

If you have questions on your requirements, please contact FINTRAC by email at guidelines-lignesdirectrices@fintrac-canafe.gc.ca.

Definitions

Accountant

A chartered accountant, a certified general accountant, a certified management accountant or, if applicable, a chartered professional accountant. (comptable)

Reference:

Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFR), SOR/2002-184, s. 1(2).

Accounting firm

An entity that is engaged in the business of providing accounting services to the public and has at least one partner, employee or administrator that is an accountant. (cabinet d'expertise comptable)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Act

The Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA). (la Loi)

Reference:

Proceeds of Crime (Money Laundering) and Terrorist Financing Administrative Monetary Penalties Regulations (PCMLTFAMPR), SOR/2007-292, s. 1, Proceeds of Crime (Money Laundering) and Terrorist Financing Registration Regulations (PCMLTFRR), SOR/2007-121, s. 1, PCMLTFR, SOR/2002-184, s. 1(2), and Proceeds of Crime (Money Laundering) and Terrorist Financing Suspicious Transaction Reporting Regulations (PCMLTFSTRR), SOR/2001-317, s. 1(2).

Administrative monetary penalties (AMPs)

Civil penalties that may be issued to reporting entities by FINTRAC for non-compliance with the PCMLTFA and associated Regulations. (pénalité administrative pécuniaire [PAP])

Affiliate

An entity is affiliated with another entity if one of them is wholly owned by the other, if both are wholly owned by the same entity or if their financial statements are consolidated. (entité du même groupe)

Reference:

PCMLTFR, SOR/2002-184, s. 4.

Annuity

Has the same meaning as in subsection 248(1) of the Income Tax Act. (rente)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Armoured cars

Persons or entities that are engaged in the business of transporting currency, money orders, traveller's cheques or other similar negotiable instruments. (Véhicules blindés)

As soon as practicable

A time period that falls in-between immediately and as soon as possible, within which a suspicious transaction report (STR) must be submitted to FINTRAC. The completion and submission of the STR should take priority over other tasks. In this context, the report must be completed promptly, taking into account the facts and circumstances of the situation. While some delay is permitted, it must have a reasonable explanation. (aussitôt que possible)

Attempted transaction

Occurs when an individual or entity starts to conduct a transaction that is not completed. For example, a client or a potential client walks away from conducting a $10,000 cash deposit. (opération tentée)

Authentic

In respect of verifying identity, means genuine and having the character of an original, credible, and reliable document or record. (authentique)

Authorized person

A person who is authorized under subsection 45(2). (personne autorisée)

Reference:

Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA), S.C. 2000, c 17, s. 2(1).

Authorized user

A person who is authorized by a holder of a prepaid payment product account to have electronic access to funds or virtual currency available in the account by means of a prepaid payment product that is connected to it. (utilisateur autorisé)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Beneficial owner(s)

Beneficial owners are the individuals who are the trustees, and known beneficiaries and settlors of a trust, or who directly or indirectly own or control 25% or more of i) the shares of a corporation or ii) an entity other than a corporation or trust, such as a partnership. The ultimate beneficial owner(s) cannot be another corporation or entity; it must be the actual individual(s) who owns or controls the entity. (bénéficiaire effectif)

Beneficiary

A beneficiary is the individual or entity that will benefit from a transaction or to which the final remittance is made. (bénéficiaire)

Branch

A branch is a part of your business at a distinct location other than your main office. (succursale)

British Columbia notary corporation

An entity that carries on the business of providing notary services to the public in British Columbia in accordance with the Notaries Act, R.S.B.C. 1996, c. 334. (société de notaires de la Colombie-Britannique)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

British Columbia notary public

A person who is a member of the Society of Notaries Public of British Columbia. (notaire public de la Colombie-Britannique)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Cash

Coins referred to in section 7 of the Currency Act, notes issued by the Bank of Canada under the Bank of Canada Act that are intended for circulation in Canada or coins or bank notes of countries other than Canada. (espèces)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2) and PCMLTFSTRR, SOR/2001-317, s. 1(2).

Casino

A government, organization, board or operator that is referred to in any of paragraphs 5(k) to (k.3) of the Act. (casino)

Reference:

PCMLTFR, SOR/2002-184, s 1(2) and PCMLTFSTRR, SOR/2001-317, s. 1(2).

Certified translator

An individual that holds the title of professional certified translator granted by a Canadian provincial or territorial association or body that is competent under Canadian provincial or territorial law to issue such certification. (traducteur agréé)

Clarification request

A clarification request is a method used to communicate with money services businesses (MSBs) or foreign money services businesses (FMSBs) when FINTRAC needs more information about their registration form. This request is usually sent by email. (demande de précisions)

Client

A person or entity that engages in a financial transaction with another person or entity. (client)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 2(1).

Client identification information

The identifying information that you have obtained on your clients, such as name, address, telephone number, occupation or nature of principal business, and date of birth for an individual. (renseignements d'identification du client)

Competent authority

For the purpose of the criminal record check submitted with an application for registration, a competent authority is any person or organization that has the legally delegated or invested authority, capacity, or power to issue criminal record checks. (autorité compétente)

Completed transaction

Is a transaction conducted by a person or entity, that is completed and results in the movement of funds, virtual currency, or the purchase or sale of an asset. (opération effectuée)

Completing action

With respect to a reportable transaction, information related to the instructions provided by the person or entity making the request to the reporting entity to complete a transaction. For example, an individual arrives at a bank and requests to purchase a bank draft. The completing action is the details of how the reporting entity fulfilled the person or entity's instructions which led to the transaction being completed. This includes what the funds or virtual currency initially brought to the reporting entity was used for (see "disposition"). A transaction may have one or more completing actions depending on the instructions provided by the person or entity. (action d'achèvement)

Compliance officer

The individual, with the necessary authority, that you appoint to be responsible for the implementation of your compliance program. (agent de conformité)

Compliance policies and procedures

Written methodology outlining the obligations applicable to your business under the PCMLTFA and its associated Regulations and the corresponding processes and controls you put in place to address your obligations. (politiques et procédures de conformité)

Compliance program

All elements (compliance officer, policies and procedures, risk assessment, training program, effectiveness review) that you, as a reporting entity, are legally required to have under the PCMLTFA and its associated Regulations to ensure that you meet all your obligations. (programme de conformité)

Context

Clarifies a set of circumstances or provides an explanation of a situation or financial transaction that can be understood and assessed. (contexte)

Correspondent banking relationship

A relationship created by an agreement or arrangement under which an entity referred to in any of paragraphs 5(a), (b), (d),(e) and (e.1) or an entity that is referred to in section 5 and that is prescribed undertakes to provide to a prescribed foreign entity prescribed services or international electronic funds transfers, cash management or cheque clearing services. (relation de correspondant bancaire)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 9.4(3) and PCMLTFR, SOR/2002-184, s. 16(1)(b).

Country of residence

The country where an individual has lived continuously for 12 months or more. The individual must have a dwelling in the country concerned. For greater cer-

tainty, a person only has one country of residence no matter how many dwelling places they may have, inside or outside of that country. (pays de résidence)

Credit card acquiring business

A credit card acquiring business is a financial entity that has an agreement with a merchant to provide the following services:

- enabling a merchant to accept credit card payments by cardholders for goods and services and to receive payments for credit card purchases;
- processing services, payment settlements and providing point-of-sale equipment (such as computer terminals); and
- providing other ancillary services to the merchant.

(entreprise d'acquisition de cartes de crédit)Credit union central

A central cooperative credit society, as defined in section 2 of the Cooperative Credit Associations Act, or a credit union central or a federation of credit unions or caisses populaires that is regulated by a provincial Act other than one enacted by the legislature of Quebec. (centrale de caisses de crédit)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Crowdfunding platform

A website or an application or other software that is used to raise funds or virtual currency through donations. (plateforme de sociofinancement)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Crowdfunding platform services

The provision and maintenance of a crowdfunding platform for use by other persons or entities to raise funds or virtual currency for themselves or for persons or entities specified by them. (services de plateforme de sociofinancement)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Current

In respect of a document or source of information that is used to verify identity, is up to date, and, in the case of a government-issued photo identification document, must not have been expired when the ID was verified. (à jour)

Dealer in precious metals and stones

A person or entity that, in the course of their business activities, buys or sells precious metals, precious stones or jewellery. It includes a department or an agent of His Majesty in right of Canada or an agent or mandatary of His Majesty

in right of a province when the department or the agent or mandatary carries out the activity, referred to in subsection 65(1), of selling precious metals to the public. (négociant en métaux précieux et pierres précieuses)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Deferred profit sharing plan

Has the same meaning as in subsection 248(1) of the Income Tax Act. (régime de participation différée aux bénéfices)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Deposit slip

A record that sets out:

1. (a) the date of the deposit;
2. (b) the name of the person or entity that makes the deposit;
3. (c) the amount of the deposit and of any part of it that is made in cash;
4. (d) the method by which the deposit is made; and
5. (e) the number of the account into which the deposit is made and the name of each account holder.

(relevé de dépôt)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Directing services

A business is directing services at persons or entities in Canada if at least one of the following applies:

- The business's marketing or advertising is directed at persons or entities located in Canada;
- The business operates a ".ca" domain name; or,
- The business is listed in a Canadian business directory.

Additional criteria may be considered, such as if the business describes its services being offered in Canada or actively seeks feedback from persons or entities in Canada. (diriger des services)

Distributed ledger

For the purpose of section 151 of the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFR), a digital ledger that is maintained by multiple persons or entities and that can only be modified by a consensus of those persons or entities. (registres distribués)

Reference:

PCMLTFR, SOR/2002-184, s. 151(2).

Disposition

With respect to a reportable transaction, the disposition is what the funds or virtual currency was used for. For example, an individual arrives at a bank with cash and purchases a bank draft. The disposition is the purchase of the bank draft. (répartition)

Electronic funds transfer

The transmission—by any electronic, magnetic or optical means—of instructions for the transfer of funds, including a transmission of instructions that is initiated and finally received by the same person or entity. In the case of SWIFT messages, only SWIFT MT-103 messages and their equivalent are included. It does not include a transmission or instructions for the transfer of funds:

1. (a) that involves the beneficiary withdrawing cash from their account;
2. (b) that is carried out by means of a direct deposit or pre-authorized debit;
3. (c) that is carried out by cheque imaging and presentment
4. (d) that is both initiated and finally received by persons or entities that are acting to clear or settle payment obligations between themselves; or
5. (e) that is initiated or finally received by a person or entity referred to in paragraphs 5(a) to (h.1) of the Act for the purpose of internal treasury management, including the management of their financial assets and liabilities, if one of the parties to the transaction is a subsidiary of the other or if they are subsidiaries of the same corporation.

(télévirement)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Employees profit sharing plan

Has the same meaning as in subsection 248(1) of the Income Tax Act. (régime de participation des employés aux bénéfices)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Entity

A body corporate, a trust, a partnership, a fund or an unincorporated association or organization. (entité)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 2(1).

Facts

Actual events, actions, occurrences or elements that exist or are known to have happened or existed. Facts are not opinions. For example, facts surrounding a transaction or multiple transactions could include the date, time, location, amount or type of transaction or could include the account details, particular business lines, or the client's financial history. (faits)

Family member

For the purposes of subsection 9.3(1) of the Act, a prescribed family member of a politically exposed foreign person, a politically exposed domestic person or a head of an international organization is:

1. (a) their spouse or common-law partner;
2. (b) their child;
3. (c) their mother or father;
4. (d) the mother or father of their spouse or common-law partner; or
5. (e) a child of their mother or father.

(membre de la famille)

Reference:

PCMLTFR, SOR/2002-184, s. 2(1).

Fiat currency

A currency that is issued by a country and is designated as legal tender in that country. (monnaie fiduciaire)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2) and PCMLTFSTRR, SOR/2001-317, s. 1(2).

Final receipt

In respect of an electronic funds transfer, means the receipt of the instructions by the person or entity that is to make the remittance to a beneficiary. (destinataire)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Financial entity

Means:

1. (a) an entity that is referred to in any of paragraphs 5(a), (b) and (d) to (f) of the Act;
2. (b) a financial services cooperative;
3. (c) a life insurance company, or an entity that is a life insurance broker or agent, in respect of loans or prepaid payment products that it offers to the public and accounts that it maintains with respect to those loans or prepaid payment products, other than:
4. (i) loans that are made by the insurer to a policy holder if the insured person has a terminal illness that significantly reduces their life expectancy and the loan is secured by the value of an insurance policy;
5. (ii) loans that are made by the insurer to the policy holder for the sole purpose of funding the life insurance policy; and
6. (iii) advance payments to which the policy holder is entitles that are made to them by the insurer;
7. (d) a credit union central when it offers financial services to a person, or to an entity that is not a member of that credit union central; and
8. (e) a department, or an entity that is an agent of His Majesty in right of Canada or an agent or mandatary of His Majesty in right of a province, when it carries out an activity referred to in section 76.

(entité financière)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Financial Action Task Force

The Financial Action Task Force on Money Laundering established in 1989. (Groupe d'action financière)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 2(1).

Financial services cooperative

A financial services cooperative that is regulated by an Act respecting financial services cooperatives, CQLR, c. C-67.3 or the Act respecting the Mouvement Desjardins, S.Q. 2000, c. 77, other than a caisse populaire. (coopérative de services financiers)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Foreign currency

A fiat currency that is issued by a country other than Canada. (devise)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Foreign currency exchange transaction

An exchange, at the request of another person or entity, of one fiat currency for another. (opération de change en devise)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Foreign currency exchange transaction ticket

A record respecting a foreign currency exchange transaction—including an entry in a transaction register—that sets out:

1. (a) the date of the transaction;
2. (b) in the case of a transaction of $3,000 or more, the name and address of the person or entity that requests the exchange, the nature of their principal business or their occupation and, in the case of a person, their date of birth;
3. (c) the type and amount of each of the fiat currencies involved in the payment made and received by the person or entity that requests the exchange;
4. (d) the method by which the payment is made and received;
5. (e) the exchange rates used and their source;
6. (f) the number of every account that is affected by the transaction, the type of account and the name of each account holder; and
7. (g) every reference number that is connected to the transaction and has a function equivalent to that of an account number.

(fiche d'opération de change en devise)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Foreign money services business

Persons and entities that do not have a place of business in Canada, that are engaged in the business of providing at least one of the following services that is directed at persons or entities in Canada, and that provide those services to their clients in Canada:

1. (i) foreign exchange dealing,
2. (ii) remitting funds or transmitting funds by any means or through any person, entity or electronic funds transfer network,
3. (iii) issuing or redeeming money orders, traveller's cheques or other similar negotiable instruments except for cheques payable to a named person or entity,
4. (iv) dealing in virtual currencies, or
5. (v) any prescribed service.

(entreprise de services monétaires étrangère)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 5(h.1), PCMLTFRR, SOR/2007-121, s. 1 and PCMLTFR, SOR/2002-184, s. 1(2).

Foreign state

Except for the purposes of Part 2, means a country other than Canada and includes any political subdivision or territory of a foreign state. (État étranger)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 2(1).

Funds

Means:

1. (a) cash and other fiat currencies, and securities, negotiable instruments or other financial instruments that indicate a title or right to or interest in them; or
2. (b) a private key of a cryptographic system that enables a person or entity to have access to a fiat currency other than cash.

For greater certainty, it does not include virtual currency. (fonds)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2) and PCMLTFSTRR, SOR/2001-317, s. 1(2).

Head of an international organization

A person who, at a given time, holds—or has held within a prescribed period before that time—the office or position of head of

1. a) an international organization that is established by the governments of states;
2. b) an institution of an organization referred to in paragraph (a); or

3. c) an international sports organization.

(dirigeant d'une organisation internationale)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 9.3(3).

Immediately

In respect of submitting a Terrorist Property Report (TPR), the time period within which a TPR must be submitted, which does not allow for any delay prior to submission. (immédiatement)

Information record

A record that sets out the name and address of a person or entity and:

1. (a) in the case of a person, their date of birth and the nature of their principal business or their occupation; and
2. (b) in the case of an entity, the nature of its principal business.

(dossier de renseignements)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Initiation

In respect of an electronic funds transfer, means the first transmission of the instructions for the transfer of funds. (amorcer)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Institutional trust

For the purpose of section 15 of the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFR), means a trust that is established by a corporation or other entity for a particular business purpose and includes a pension plan trust, a pension master trust, a supplemental pension plan trust, a mutual fund trust, a pooled fund trust, a registered retirement savings plan trust, a registered retirement income fund trust, a registered education savings plan trust, a group registered retirement savings plan trust, a deferred profit sharing plan trust, an employee profit sharing plan trust, a retirement compensation arrangement trust, an employee savings plan trust, a health and welfare trust, an unemployment benefit plan trust, a foreign insurance company trust, a foreign reinsurance trust, a reinsurance trust, a real estate investment trust, an environmental trust and a trust established in respect of endowment, a foundation or a registered charity. (fiducie institutionnelle)

Reference:

PCMLTFR, SOR/2002-184, s. 15(2).

International electronic funds transfer

An electronic funds transfer other than for the transfer of funds within Canada. (télévirement international)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Inter vivos trust

A personal trust, other than a trust created by will. (fiducie entre vifs)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Jewellery

Objects that are made of gold, silver, palladium, platinum, pearls or precious stones and that are intended to be worn as a personal adornment. (bijou)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Large cash transaction record

A record that indicates the receipt of an amount of $10,000 or more in cash in a single transaction and that contains the following information:

1. (a) the date of the receipt;
2. (b) if the amount is received for deposit into an account, the number of the account, the name of each account holder and the time of the deposit or an indication that the deposit is made in a night deposit box outside the recipient's normal business hours;
3. (c) the name and address of every other person or entity that is involved in the transaction, the nature of their principal business or their occupation and, in the case of a person, their date of birth;
4. (d) the type and amount of each fiat currency involved in the receipt;
5. (e) the method by which the cash is received;
6. (f) if applicable, the exchange rates used and their source;
7. (g) the number of every other account that is affected by the transaction, the type of account and the name of each account holder
8. (h) every reference number that is connected to the transaction and has a function equivalent to that of an account number;
9. (i) the purpose of the transaction;

10. (j) the following details of the remittance of, or in exchange for, the cash received:

    1. (i) the method of remittance;

    2. (ii) if the remittance is in funds, the type and amount of each type of funds involved;

    3. (iii) if the remittance is not in funds, the type of remittance and its value, if different from the amount of cash received; and

    4. (iv) the name of every person or entity involved in the remittance and their account number or policy number or, if they have no account number or policy number, their identifying number; and

11. (k) if the amount is received by a dealer in precious metals and precious stones for the sale of precious metals, precious stones or jewellery:

    1. (i) the type of precious metals, precious stones or jewellery;

    2. (ii) the value of the precious metals, precious stones or jewellery, if different from the amount of cash received, and

    3. (iii) the wholesale value of the precious metals, precious stones or jewellery.

(relevé d'opération importante en espèces)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Large virtual currency transaction record

A record that indicates the receipt of an amount of $10,000 or more in virtual currency in a single transaction and that contains the following information:

1. (a) the date of the receipt;

2. (b) if the amount is received for deposit into an account, the name of each account holder;

3. (c) the name and address of every other person or entity that is involved in the transaction, the nature of their principal business or their occupation and, in the case of a person, their date of birth;

4. (d) the type and amount of each virtual currency involved in the receipt;

5. (e) the exchange rates used and their source;

6. (f) the number of every other account that is affected by the transaction, the type of account and the name of each account holder;

7. (g) every reference number that is connected to the transaction and has a function equivalent to that of an account number;

8. (h) every transaction identifier, including the sending and receiving addresses; and

9. (i) if the amount is received by a dealer in precious metals and precious stones for the sale of precious metals, precious stones or jewellery:

10. (i) the type of precious metals, precious stones or jewellery;

11. (ii) the value of the precious metals, precious stones or jewellery, if different from the amount of virtual currency received; and

12. (iii) the wholesale value of the precious metals, precious stones or jewellery.

(relevé d'opération importante en monnaie virtuelle)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Life insurance broker or agent

A person or entity that is authorized under provincial legislation to carry on the business of arranging contracts of life insurance. (représentant d'assurance-vie)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Life insurance company

A life company or foreign life company to which the Insurance Companies Act applies or a life insurance company regulated by a provincial Act. (société d'assurance-vie)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Listed person

Has the same meaning as in section 1 of the Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism. (personne inscrite)

Reference:

PCMLTFSTRR, SOR/2001-317, s. 1(2).

Managing general agents (MGAs)

Life insurance brokers or agents that act as facilitators between other life insurance brokers or agents and life insurance companies. MGAs typically offer services to assist with insurance agents contracting and commission payments, facilitate the flow of information between insurer and agent, and provide training to, and compliance oversight of, insurance agents. (agent général de gestion)

Mandatary

A person who acts, under a mandate or agreement, for another person or entity. (mandataire)

Marketing or advertising

When a person or entity uses promotional materials such as advertisements, graphics for websites or billboards, etc., with the intent to promote money services business (MSB) services and to acquire business from persons or entities in Canada. (marketing ou publicité)

Minister

In relation to sections 24.1 to 39, the Minister of Public Safety and Emergency Preparedness and, in relation to any other provision of this Act, the Minister of Finance. (ministre)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 2(1).

Money laundering offence

An offence under subsection 462.31(1) of the Criminal Code. The United Nations defines money laundering as "any act or attempted act to disguise the source of money or assets derived from criminal activity." Essentially, money laundering is the process whereby "dirty money"—produced through criminal activity—is transformed into "clean money," the criminal origin of which is difficult to trace. (infraction de recyclage des produits de la criminalité)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 2(1).

Money laundering and terrorist financing indicators (ML/TF indicators)

Potential red flags that could initiate suspicion or indicate that something may be unusual in the absence of a reasonable explanation. [Indicateurs de blanchiment d'argent (BA) et de financement du terrorisme (FT) (indicateurs de BA/FT)]

Money services business

A person or entity that has a place of business in Canada and that is engaged in the business of providing at least one of the following services:

1. (i) foreign exchange dealing,
2. (ii) remitting funds or transmitting funds by any means or through any person, entity or electronic funds transfer network,
3. (iii) issuing or redeeming money orders, traveller's cheques or other similar negotiable instruments except for cheques payable to a named person or entity,
4. (iv) dealing in virtual currencies, or

5. (v) any prescribed service.

(entreprise de services monétaires)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 5(h), PCMLTFRR, SOR/2007-121, s. 1 and PCMLTFR, SOR/2002-184, s. 1(2).

Money services business agent

An individual or entity authorized to deliver services on behalf of a money services business (MSB). It is not an MSB branch. (mandataire d'une entreprise de services monétaires)

Mortgage administrator

A person or entity, other than a financial entity, that is engaged in the business of servicing mortgage agreements on real property or hypothec agreements on immovables on behalf of a lender. (administrateur hypothécaire)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 5(i), PCMLTFRR,SOR/2002-184, subsection 1(2)

Mortgage broker

A person or entity that is authorized under provincial legislation to act as an intermediary between a lender and a borrower with respect to loans secured by mortgages on real property or hypothecs on immovables. (courtier hypothécaire)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 5(i), PCMLTFRR,SOR/2002-184, subsection 1(2)

Mortgage lender

A person or entity, other than a financial entity, that is engaged in the business of providing loans secured by mortgages on real property or hypothecs on immovables. (prêteur hypothécaire)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 5(i), PCMLTFRR,SOR/2002-184, subsection 1(2)

Nature of principal business

An entity's type or field of business. Also applies to an individual in the case of a sole proprietorship. (nature de l'entreprise principale)

New developments

Changes to the structure or operations of a business when new services, activities, or locations are put in place. For example, changes to a business model or business restructuring. (nouveaux développements)

New technologies

The adoption of a technology that is new to a business. For example, when a business adopts new systems or software such as transaction monitoring systems or client onboarding and identification tools. (nouvelles technologies)

No apparent reason

There is no clear explanation to account for suspicious behaviour or information. (sans raison apparente)

Occupation

The job or profession of an individual. (profession ou métier)

Person

An individual. (personne)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 2(1).

Person authorized to give instructions

In respect of an account, means a person who is authorized to instruct on the account or make changes to the account, such as modifying the account type, updating the account contact details, and in the case of a credit card account, requesting a limit increase or decrease, or adding or removing card holders. A person who is only able to conduct transactions on the account is not considered a person authorized to give instructions. (personne habilitée à donner des instructions)

Politically exposed domestic person

A person who, at a given time, holds—or has held within a prescribed period before that time—one of the offices or positions referred to in any of paragraphs (a) and (c) to (j) in or on behalf of the federal government or a provincial government or any of the offices or positions referred to in paragraphs (b) and (k):

1. (a) Governor General, lieutenant governor or head of government;
2. (b) member of the Senate or House of Commons or member of a legislature of a province;
3. (c) deputy minister or equivalent rank;
4. (d) ambassador, or attaché or counsellor of an ambassador;
5. (e) military officer with a rank of general or above;

6. (f) president of a corporation that is wholly owned directly by His Majesty in right of Canada or a province;
7. (g) head of a government agency;
8. (h) judge of an appellate court in a province, the Federal Court of Appeal or the Supreme Court of Canada;
9. (i) leader or president of a political party represented in a legislature;
10. (j) holder of any prescribed office or position; or
11. (k) mayor, reeve or other similar chief officer of a municipal or local government.

(national politiquement vulnérable)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 9.3(3).

Politically exposed foreign person

A person who holds or has held one of the following offices or positions in or on behalf of a foreign state:

1. (a) head of state or head of government;
2. (b) member of the executive council of government or member of a legislature;
3. (c) deputy minister or equivalent rank;
4. (d) ambassador, or attaché or counsellor of an ambassador;
5. (e) military officer with a rank of general or above;
6. (f) president of a state-owned company or a state-owned bank;
7. (g) head of a government agency;
8. (h) judge of a supreme court, constitutional court or other court of last resort;
9. (i) leader or president of a political party represented in a legislature; or
10. (j) holder of any prescribed office or position.

(étranger politiquement vulnérable)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Possibility

In regards to completing a suspicious transaction report (STR), the likelihood that a transaction may be related to a money laundering/terrorist financing

(ML/TF) offence. For example, based on your assessment of facts, context and ML/TF indicators you have reasonable grounds to suspect that a transaction is related to the commission or attempted commission of an ML/TF offence. (possibilité)

Precious metal

Gold, silver, palladium or platinum in the form of coins, bars, ingots or granules or in any other similar form. (métal précieux)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 2(1).

Precious stones

Diamonds, sapphires, emeralds, tanzanite, rubies or alexandrite. (pierre précieuse)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Prepaid payment product

A product that is issued by a financial entity and that enables a person or entity to engage in a transaction by giving them electronic access to funds or virtual currency paid to a prepaid payment product account held with the financial entity in advance of the transaction. It excludes a product that:

1. (a) enables a person or entity to access a credit or debit account or one that is issued for use only with particular merchants; or
2. (b) is issued for single use for the purposes of a retail rebate program.

(produit de paiement prépayé)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Prepaid payment product account

An account – other than an account to which only a public body or, if doing so for the purposes of humanitarian aid, a registered charity as defined in subsection 248(1) of the Income Tax Act, can add funds or virtual currency – that is connected to a prepaid payment product and that permits:

1. (a) funds or virtual currency that total $1,000 or more to be added to the account within a 24-hour period; or
2. (b) a balance of funds or virtual currency of $1,000 or more to be maintained.

(compte de produit de paiement prépayé)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Prescribed

Prescribed by regulations made by the Governor in Council. (Version anglaise seulement)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 2(1).

Probability

The likelihood in regards to completing a suspicious transaction report (STR) that a financial transaction is related to a money laundering/terrorist financing (ML/TF) offence. For example, based on facts, having reasonable grounds to believe that a transaction is probably related to the commission or attempted commission of an ML/TF offence. (probabilité)

Production order

A judicial order that compels a person or entity to disclose records to peace officers or public officers. (ordonnance de communication)

Public body

Means

1. (a) a department or an agent of His Majesty in right of Canada or an agent or mandatary of His Majesty in right of a province;
2. (b) an incorporated city or town, village, metropolitan authority, township, district, county, rural municipality or other incorporated municipal body in Canada or an agent or mandatary in Canada of any of them; and
3. (c) an organization that operates a public hospital and that is designated by the Minister of National Revenue as a hospital authority under the Excise Tax Act, or an agent or mandatary of such an organization.

(organisme public)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Real estate broker or sales representative

A person or entity that is authorized under provincial legislation to act as an agent or mandatary for purchasers or vendors in respect of the purchase or sale of real property or immovables. (courtier ou agent immobilier)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Real estate developer

A person or entity that, in any calendar year after 2007, has sold to the public, other than in the capacity of a real estate broker or sales representative:

1. (a) five or more new houses or condominium units;
2. (b) one or more new commercial or industrial buildings; or
3. (c) one or more new multi-unit residential buildings each of which contains five or more residential units, or two or more new multi-unit residential buildings that together contain five or more residential units.

(promoteur immobilier)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Reasonable measures

Steps taken to achieve a desired outcome, even if they do not result in the desired outcome. For example, this can include doing one or more of the following:

- asking the client,
- conducting open source searches,
- retrieving information already available, including information held in non-digital formats, or
- consulting commercially available information.

(mesures raisonnables)Receipt of funds record

A record that indicates the receipt of an amount of funds and that contains the following information:

1. (a) the date of the receipt;
2. (b) if the amount is received from a person, their name, address and date of birth and the nature of their principal business or their occupation;
3. (c) if the amount is received from or on behalf of an entity, the entity's name and address and the nature of their principal business;
4. (d) the amount of the funds received and of any part of the funds that is received in cash;
5. (e) the method by which the amount is received;
6. (f) the type and amount of each fiat currency involved in the receipt;
7. (g) if applicable, the exchange rates used and their source;

8. (h) the number of every account that is affected by the transaction in which the receipt occurs, the type of account and the name of each account holder;

9. (i) the name and address of every other person or entity that is involved in the transaction, the nature of their principal business or their occupation and, in the case of a person, their date of birth;

10. (j) every reference number that is connected to the transaction and has a function equivalent to that of an account number; and

11. (k) the purpose of the transaction.

(relevé de réception de fonds)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Registered pension plan

Has the same meaning as in subsection 248(1) of the Income Tax Act. (régime de pension agréé)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Registered retirement income fund

Has the same meaning as in subsection 248(1) of the Income Tax Act. (fonds enregistré de revenu de retraite)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Reliable

In respect of information that is used to verify identity, means that the source is well known, reputable, and is considered one that you trust to verify the identity of the client. (fiable)

Representative for service

An individual in Canada that has been appointed by a person or entity that is a foreign money services business (FMSB), pursuant to the PCMLTFA, to receive notices and documents on behalf of the FMSB. (représentant du service)

Risk assessment

The review and documentation of potential money laundering/terrorist financing risks in order to help a business establish policies, procedures and controls to detect and mitigate these risks and their impact. (évaluation des risques)

Sanctions evasion

Sanctions evasion offence means an offence arising from the contravention of a restriction or prohibition established by an order or a regulation made under the United Nations Act, the Special Economic Measures Act or the Justice for Victims of Corrupt Foreign Officials Act (Sergei Magnitsky Law). (contournement des sanctions)

Securities dealer

A person or entity that is referred to in paragraph 5(g) of the Act. (courtier en valeurs mobilières)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Senior officer

In respect of an entity, means:

1. (a) a director of the entity who is one of its full-time employees;
2. (b) the entity's chief executive officer, chief operating officer, president, secretary, treasurer, controller, chief financial officer, chief accountant, chief auditor or chief actuary, or any person who performs any of those functions; or
3. (c) any other officer who reports directly to the entity's board of directors, chief executive officer or chief operating officer.

(cadre dirigeant)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Service agreement

An agreement between a money services business (MSB) and an organization according to which the MSB will provide any of the following MSB services on an ongoing basis:

- money transfers;
- foreign currency exchange;
- issuing or redeeming money orders, traveller's cheques or anything similar; or
- dealing in virtual currencies.
- Crowdfunding
- Armoured Cars

(accord de relation commerciale) Settlor

A settlor is an individual or entity that creates a trust with a written trust declaration. The settlor ensures that legal responsibility for the trust is given to a trustee and that the trustee is provided with a trust instrument document

that explains how the trust is to be used for the beneficiaries. A settlor includes any individual or entity that contributes financially to that trust, either directly or indirectly. (constituant)

Shell bank

A foreign financial institution that:

1. (a) does not have a place of business that:
2. (i) is located at a fixed address—where it employs one or more persons on a full-time basis and maintains operating records related to its banking activities—in a country in which it is authorized to conduct banking activities; and
3. (ii) is subject to inspection by the regulatory authority that licensed it to conduct banking activities; and
4. (b) is not controlled by, or under common control with, a depository institution, credit union or foreign financial institution that maintains a place of business referred to in paragraph (a) in Canada or in a foreign country.

(banque fictive)

Reference:

PCMLTFR, SOR/2002-184, s. 1(1).

Signature

Includes an electronic signature or other information in electronic form that is created or adopted by a client of a person or entity referred to in section 5 of the Act and that is accepted by the person or entity as being unique to that client. (signature)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Signature card

In respect of an account, means a document that is signed by a person who is authorized to give instructions in respect of the account, or electronic data that constitutes the signature of such a person. (fiche-signature)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Source

The issuer or provider of information or documents for verifying identification. (source)

Source of funds or of virtual currency (VC)

The origin of the particular funds or VC used to carry out a specific transaction or to attempt to carry out a transaction. It is how the funds were acquired, not where the funds may have been transferred from. For example, the source of funds could originate from activities or occurrences such as employment income, gifts, the sale of a large asset, criminal activity, etc. (origine des fonds ou de la monnaie virtuelle (MV))

Source of wealth

The origin of a person's total assets that can be reasonably explained, rather than what might be expected. For example, a person's wealth could originate from an accumulation of activities and occurrences such as business undertakings, family estates, previous and current employment income, investments, real estate, inheritance, lottery winnings, etc. (origine de la richesse)

Starting action

With respect to a reportable transaction, information related to the instructions provided by the person or entity making the request to the reporting entity to start a transaction. For example, an individual arrives at a bank and requests to purchase a bank draft. The starting action is the details of the instructions for the purchase which includes the funds or virtual currency that the requesting person or entity brought to the reporting entity. A transaction must have at least one starting action. (action d'amorce)

SWIFT

The Society for Worldwide Interbank Financial Telecommunication. (SWIFT)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Terrorist activity

Has the same meaning as in subsection 83.01(1) of the Criminal Code. (activité terroriste)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 2(1).

Terrorist activity financing offence

An offence under section 83.02, 83.03 or 83.04 of the Criminal Code or an offence under section 83.12 of the Criminal Code arising out of a contravention of section 83.08 of that Act.

A terrorist financing offence is knowingly collecting or giving property (such as money) to carry out terrorist activities. This includes the use and possession of any property to help carry out the terrorist activities. The money earned for terrorist financing can be from legal sources, such as personal donations and profits from a business or charitable organization or from criminal sources, such

as the drug trade, the smuggling of weapons and other goods, fraud, kidnapping and extortion. (infraction de financement des activités terroristes)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 2(1).

Third party

Any individual or entity that instructs another individual or entity to act on their behalf for a financial activity or transaction. (tiers)

Threats to the security of Canada

Has the same meaning as in section 2 of the Canadian Security Intelligence Service Act. (menaces envers la sécurité du Canada)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 2(1).

Training program

A written and implemented program outlining the ongoing training for your employees, agents or other individuals authorized to act on your behalf. It should contain information about all your obligations and requirements to be fulfilled under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and its associated Regulations. (programme de formation)

Trust

A right of property held by one individual or entity (a trustee) for the benefit of another individual or entity (a beneficiary). (fiducie)

Trust company

A company that is referred to in any of paragraphs 5(d) to (e.1) of the Act. (société de fiducie)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Trustee

A trustee is the individual or entity authorized to hold or administer the assets of a trust. (fiduciaire)

Tutor

In the context of civil law, a person who has been lawfully appointed to the care of the person and property of a minor. (tuteur)

Two year effectiveness review

A review, conducted every two years (at a minimum), by an internal or external auditor to test the effectiveness of your policies and procedures, risk assessment, and training program. (examen bisannuel de l'efficacité)

Valid

In respect of a document or information that is used to verify identity, appears legitimate or authentic and does not appear to have been altered or had any information redacted. The information must also be valid according to the issuer, for example if a passport is invalid because of a name change, it is not valid for FINTRAC purposes. (valide)

Verify identity

To refer to certain information or documentation, in accordance with the prescribed methods, to identify a person or entity (client). (vérifier l'identité)

Very large corporation or trust

A corporation or trust that has minimum net assets of $75 million CAD on its last audited balance sheet. The corporation's shares or units have to be traded on a Canadian stock exchange or on a stock exchange designated under subsection 262(1) of the Income Tax Act. The corporation or trust also has to operate in a country that is a member of the Financial Action Task Force (FATF). (personne morale ou fiducie dont l'actif est très important)

Violation

A contravention of the Act or the regulations that is designated as a violation by regulations made under subsection 73.1(1). (violation)

Reference:

PCMLTFA, S.C. 2000, c 17, s. 2(1).

Virtual currency

Means:

1. (a) a digital representation of value that can be used for payment or investment purposes that is not a fiat currency and that can be readily exchanged for funds or for another virtual currency that can be readily exchanged for funds; or

2. (b) a private key of a cryptographic system that enables a person or entity to have access to a digital representation of value referred to in paragraph (a).

(monnaie virtuelle)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2) and PCMLTFSTRR, SOR/2001-317, s. 1(2).

Virtual currency exchange transaction

An exchange, at the request of another person or entity, of virtual currency for funds, funds for virtual currency or one virtual currency for another. (opération de change en monnaie virtuelle)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Virtual currency exchange transaction ticket

A record respecting a virtual currency exchange transaction—including an entry in a transaction register—that sets out:

1. (a) the date of the transaction;
2. (b) in the case of a transaction of $1,000 or more, the name and address of the person or entity that requests the exchange, the nature of their principal business or their occupation and, in the case of a person, their date of birth;
3. (c) the type and amount of each type of funds and each of the virtual currencies involved in the payment made and received by the person or entity that requests the exchange;
4. (d) the method by which the payment is made and received;
5. (e) the exchange rates used and their source;
6. (f) the number of every account that is affected by the transaction, the type of account and the name of each account holder;
7. (g) every reference number that is connected to the transaction and has a function equivalent to that of an account number; and
8. (h) every transaction identifier, including the sending and receiving addresses.

(fiche d'opération de change en monnaie virtuelle)

Reference:

PCMLTFR, SOR/2002-184, s. 1(2).

Working days

In respect of an electronic funds transfer (EFT) report or a large virtual currency transaction report, a working day is a day between and including Monday to Friday. It excludes Saturday, Sunday, and a public holiday. (jour ouvrable)

Date Modified: 2024-10-11

Money laundering and terrorist financing indicators—Financial entities

From: Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)

Overview

ML/TF indicators are potential red flags that could initiate suspicion or indicate that something may be unusual in the absence of a reasonable explanation. Red flags typically stem from one or more factual characteristics, behaviours, patterns or other contextual factors that identify irregularities related to financial transactions or attempted transactions. These often present inconsistencies with what is expected of your client based on what you know about them.

The ML/TF indicators in this guidance were developed by FINTRAC through a three-year review of ML/TF cases, a review of high quality STRs, published literature by international organizations such as the Financial Action Task Force (FATF) and the Egmont Group, and consultation with reporting entity sectors. These ML/TF indicators do not cover every possible situation but were developed to provide you with a general understanding of what is or could be unusual or suspicious. On its own, a single ML/TF indicator may not appear suspicious. However, observing an ML/TF indicator could lead you to conduct an assessment of the transaction(s) to determine whether there are further facts, contextual elements or additional ML/TF indicators that assist in establishing reasonable grounds to suspect the commission or attempted commission of an ML/TF offence which requires the submission of an STR.

Criminal organizations often combine various methods in different ways in order to avoid the detection of ML/TF. If you detect unusual or suspicious behaviour or a transaction that prompts the need for an assessment, ML/TF indicators combined with facts and context can help you determine if there are **reasonable grounds to suspect** that the transaction is related to the commission or attempted commission of an ML/TF offence. These ML/TF indicators may also be used to explain or articulate the rationale for your reasonable grounds to suspect in the narrative portion of an STR, as they provide valuable information from a financial intelligence perspective.

Important considerations

One piece of the puzzle

The ML/TF indicators in this guidance are not an exhaustive list of ML/TF indicators to support all suspicious scenarios. These ML/TF indicators should be considered as examples to guide the development of your own process to determine when you have reasonable grounds to suspect that the transaction or attempted transaction is related to the commission or attempted commission of

an ML/TF offence. These ML/TF indicators are one piece of the puzzle and are designed to complement your own STR process and can be used in conjunction with other publicly available ML/TF indicators.

During an assessment, FINTRAC will review your compliance policies and procedures to see how you use ML/TF indicators within your STR process. Part of the assessment will include evaluating how the actual policies follow your documented approach and determining its effectiveness with respect to the use of ML/TF indicators. This can include a review of transactions to determine how your STR process identifies potential STRs and assesses them using facts, context and ML/TF indicators. For example, you may be asked to provide an explanation if you have not reported an STR for a client you have assessed as high risk and that client's activity also matches against multiple ML/TF indicators.

Combination of facts, context and ML/TF indicators

If the context surrounding a transaction is suspicious, it could lead you to assess a client's financial transactions. Facts, context and ML/TF indicators need to be assessed to determine whether there are reasonable grounds to suspect that the transaction is related to the commission or attempted commission of an ML/TF offence. On its own, a single financial transaction or ML/TF indicator may not appear suspicious. However, this does not mean you should stop your assessment. Additional facts or context about the client or their actions may help you reach the reasonable grounds to suspect threshold.

Alert or triggering system

FINTRAC acknowledges that a reporting entity may have developed a system that relies on specific alerts or triggering events to signal when to assess a transaction to determine if an STR should be submitted to FINTRAC. If you rely on such a system, FINTRAC expects that you review the alerts in a timely manner in order to determine if an STR should be submitted. Regardless of how you choose to operationalize these ML/TF indicators, FINTRAC expects that you will be able to demonstrate that you have an effective process to identify, assess and submit STRs to FINTRAC.

General ML/TF indicators

The ML/TF indicators in the following section are applicable to both suspected ML and/or TF. The ability to detect, prevent and deter ML and/or TF begins with properly identifying the person or entity in order to review and report suspicious financial activity.

As a financial entity, you may observe these ML/TF indicators over the course of your business activities with a client. It is important to note that depending on your business activities, some of these ML/TF indicators may not apply.

ML/TF indicators related to identifying the person or entity

The following are examples of ML/TF indicators that you may observe when identifying persons or entities.

- There is an inability to properly identify the client or there are questions surrounding the client's identity.
- When opening an account, the client refuses or tries to avoid providing information required by the financial institution, or provides information that is misleading, vague, or difficult to verify.
- The client refuses to provide information regarding the beneficial owners of an account opened for an entity, or provides information that is false, conflicting, misleading or substantially incorrect.
- The identification document presented by the client cannot be authenticated.
- There are inconsistencies in the identification documents or different identifiers provided by the client, such as name, address, date of birth or phone number.
- Client produces seemingly false information or identification that appears to be counterfeited, altered or inaccurate.
- Client displays a pattern of name variations from one transaction to another or uses aliases.
- Client alters the transaction after being asked for identity documents.
- The client provides only a non-civic address or disguises a post office box as a civic address for the purpose of concealing their physical residence.
- Common identifiers (e.g. addresses, phone numbers, etc.) are used by multiple clients that do not appear to be related.
- Common identifiers (e.g. addresses, phone numbers, etc.) are used by multiple clients conducting similar transactions.
- Use of the same hotel address by one or more clients.
- Transactions involve persons or entities identified by the media, law enforcement and/or intelligence agencies as being linked to criminal activities.
- Attempts to verify the information provided by a new or prospective client are difficult.

ML/TF indicators related to client behaviour

The contextual information acquired through the know your client (KYC) requirements or the behaviour of a client, particularly surrounding a transaction or a pattern of transactions, may lead you to conduct an assessment in order to determine if you are required to submit an STR to FINTRAC. The following are some examples of ML/TF indicators that are linked to contextual behaviour and may be used in conjunction with your assessment and your risk-based approach.

- Client makes statements about involvement in criminal activities.
- Client conducts transactions at different physical locations, or approaches

different tellers.
- Evidence of untruthfulness on behalf of the client (e.g. providing false or misleading information).
- Client exhibits nervous behaviour.
- Client refuses to provide information when required, or is reluctant to provide information.
- Client has a defensive stance to questioning.
- Client presents confusing details about the transaction or knows few details about its purpose.
- Client avoids contact with reporting entity employees.
- Client refuses to identify a source of funds or provides information that is false, misleading, or substantially incorrect.
- Client exhibits a lack of concern about higher than normal transaction costs or fees.
- Client makes enquiries/statements indicating a desire to avoid reporting or tries to persuade the reporting entity not to file/maintain required reports.
- Insufficient explanation for the source of funds.
- Client closes account after an initial deposit is made without a reasonable explanation.

ML/TF indicators surrounding the financial transactions in relation to the person/entity profile

Clearly understanding the expected activity of a person or entity will allow you to assess their financial activity with the proper lens. For example, an entity involved in an industry that is not normally cash-intensive receiving excessive cash deposits or a person conducting financial transactions atypical of their financial profile. The following are some examples of ML/TF indicators surrounding the financial transactions related to the person/entity profile.

- The transactional activity far exceeds the projected activity at the time of the account opening or the beginning of the relationship.
- The transactional activity (level or volume) is inconsistent with the client's apparent financial standing, their usual pattern of activities or occupational information (e.g. student, unemployed, social assistance, etc.).
- The volume of transactional activity exceeds the norm for geographical area.
- The transactional activity is inconsistent with what is expected from a declared business (e.g. business account has no normal business-related activities, such as the payment of payrolls or invoices).
- Client appears to be living beyond their means.
- Large and/or rapid movement of funds not commensurate with the client's financial profile.
- Rounded sum transactions atypical of what would be expected from the client.
- Size or type of transactions atypical of what is expected from the client.

- Opening accounts when the client's address or employment address is outside the local service area without a reasonable explanation.
- There is a sudden change in the client's financial profile, pattern of activity or transactions.
- Client uses notes, monetary instruments, or products and/or services that are unusual for such a client.

ML/TF indicators related to products and services

Accounts can take different forms (e.g. chequing, savings, investment, etc.) and for the purposes of this section, the ML/TF indicators below will aim to address the ML/TF risks linked to different types of accounts held by various reporting entities in Canada. There are many ML/TF indicators related to account activity. Your process to evaluate risk for accounts and any other products and services you provide should be documented as part of your KYC and risk assessment requirements. The following ML/TF indicators will focus on products or services that may be applicable within your business.

- Holding multiple accounts at several financial institutions for no apparent reason.
- Suspected use of a personal account for business purposes, or vice-versa.
- Client appears to have recently established a series of new relationships with different financial entities.
- A product and/or service opened on behalf of a person or entity that is inconsistent based on what you know about that client.
- Frequent use of safety deposit box.
- Accounts used for pass-through activities (e.g. to receive and subsequently send funds to beneficiaries).
- Use of multiple foreign bank accounts for no apparent reason.
- Credit card transactions and payments are exceptionally high for what is expected of the client including an excessive amount of cash advance usage, balance transfer requests or transactions involving luxury items.
- Client frequently makes credit card overpayments and then requests a cash advance.
- Frequent and/or atypical transfers between the client's products and accounts for no apparent reason.
- The same person holds signing authority for accounts held by multiple entities where there is no legal reason or sufficient explanation for such an arrangement.
- Accounts held by multiple entities either headquartered at the same location or having the same directors/signing authorities for no apparent reason.

ML/TF indicators related to change in account activity

Certain changes regarding an account may be indicative of ML/TF for a multitude of reasons including, but not limited to, the use of an account to suddenly

launder or transmit funds, an increase in volume, changes in ownership of an account, etc. Changes in account activity may trigger a need for further assessment of the person or entity holding the account and some examples to consider are listed below.

- A business account has a change in ownership structure with increases in transactional activity and no apparent explanation.
- An inactive account begins to see financial activity (e.g. deposits, wire transfers, withdrawals).
- Accounts that receive relevant periodical deposits and are inactive at other periods without a logical explanation.
- A sudden increase in credit card usage or applications for new credit.
- Abrupt change in account activity.

ML/TF indicators based on atypical transactional activity

There are certain transactions that are outside the normal conduct of your everyday business. These transactions may be indicative of a suspicious transaction, and would require additional assessment. Some examples of ML/TF indicators based on atypical transactional activity are listed below.

- The client has multiple products, atypical of what would be expected.
- A series of complicated transfers of funds that seems to be an attempt to hide the source and intended use of the funds.
- Transactions displaying financial connections between persons or entities that are not usually connected (e.g. a food importer dealing with an automobile parts exporter).
- Transaction is unnecessarily complex for its stated purpose.
- Client presents notes or financial instruments that are packed, transported or wrapped in an uncommon way.
- A client's transactions have no apparent business or economic purpose.
- Transaction is consistent with a publicly known trend in criminal activity.
- Client deposits musty, odd smelling or extremely dirty bills.
- Transaction involves a suspected shell entity (an entity that does not have an economical or logical reason to exist).
- Client frequently exchanges small bills for larger bills.
- Suspicious pattern emerges from a client's transactions (e.g. transactions take place at the same time of day).
- Atypical transfers by a client on an in-and-out basis, or other methods of moving funds quickly, such as a cash deposit followed immediately by a wire transfer of the funds out.
- Funds transferred in and out of an account on the same day or within a relatively short period of time.

ML/TF indicators related to transactions structured below the reporting or identification requirements

Structuring of transactions to avoid reporting or identification requirements is a common method for committing or attempting to commit an ML/TF offence. There are multiple thresholds which trigger reporting/identification requirements by a reporting entity. Some examples of ML/TF indicators which may be indicative of a person or entity attempting to evade identification and/or reporting thresholds are listed below.

- You become aware of the structuring of deposits at multiple branches or institutions.
- Client appears to be structuring amounts to avoid client identification or reporting thresholds.
- Client appears to be collaborating with others to avoid client identification or reporting thresholds.
- The structuring of deposits through multiple branches of the same financial institution or by groups of persons who enter a single branch at the same time.
- Multiple transactions conducted below the reporting threshold within a short period.
- Client makes enquiries that would indicate a desire to avoid reporting.
- Client conducts transactions at different physical locations or with different representatives in an apparent attempt to avoid detection.
- Client exhibits knowledge of reporting thresholds.

ML/TF indicators involving wire transfers (including electronic funds transfers)

In our current global environment, it is increasingly easier to transfer funds to, from or through multiple jurisdictions (municipal, national or international) in a rapid fashion. This presents an increased ML/TF risk as transactions passing through multiple accounts and/or jurisdictions increase the difficulty for reporting entities and law enforcement to trace illicit funds. Examples of these types of transactions which may require further assessment include the following.

- Client is unaware of details surrounding incoming wire transfers, such as the ordering client details, amounts or reasons.
- Client does not appear to know the sender of the wire transfer from whom the wire transfer was received, or the recipient to whom they are sending the wire transfer.
- Client frequents multiple locations utilizing cash, prepaid credit cards or money orders/cheques/drafts to send wire transfers overseas.
- The client sends wire transfers or receives wire transfers to or from multiple beneficiaries that do not correspond to the expected use of the account type or business account.

- Client is accompanied by persons who appear to be instructing the sending or receiving of wire transfers on their behalf.
- Multiple persons are sending wire transfers that are similar in amounts, receiver names, security questions, addresses or destination country.
- Client attempts to specify the routing of an international wire transfer.
- Client conducts wire transfers that do not include theirs or the beneficiary's requisite information.
- Client utilizes structured cash transactions to send wire transfers in an effort to avoid record keeping requirements.
- Funds are deposited or received into several accounts and then consolidated into one before transferring the funds outside the country.
- Immediately after transferred funds have cleared, the client moves funds, to another account or to another person or entity.
- Multiple clients have sent wire transfers over a short period of time to the same recipient.
- Large wire transfers or high volume of wire transfers are conducted or received through the account that does not fit the expected pattern of that account.
- Large and/or frequent wire transfers between senders and receivers with no apparent relationship.
- Client sending to, or receiving wire transfers from, multiple clients.

ML/TF indicators related to transactions that involve non-Canadian jurisdictions

There are certain types of transactions that may be sent or received from jurisdictions outside of Canada where there is higher ML/TF risk due to more permissible laws or the local ML/TF threat environment. The following are examples to consider when making an assessment of the financial transaction conducted by a person/entity through your business.

- Transactions with jurisdictions that are known to produce or transit drugs or precursor chemicals, or are sources of other types of criminality.
- Transactions with jurisdictions that are known to be at a higher risk of ML/TF.
- Transaction/business activity involving locations of concern, which can include jurisdictions where there are ongoing conflicts (and periphery areas), countries with weak ML/TF controls, or countries with highly secretive banking or other transactional laws.
- Transactions involving any countries deemed high risk or non-cooperative by the FATF.
- Client makes frequent overseas transfers, not in line with their financial profile.

Due to the ever-evolving nature of the ML/TF environment, high risk jurisdictions and trends are often subject to change. To ensure that you are referencing accurate information, FINTRAC encourages you to research publicly available

sources on a regular basis to support these ML/TF indicators as part of your STR process. There are multiple sources that identify jurisdictions of concern, including the FATF, which publishes contextual information on high-risk jurisdictions in relation to their risk of ML and TF. You may also observe funds coming from or going to jurisdictions that are reported in the media as locations where terrorists operate/carry out attacks and/or where terrorists have a large support base (state sponsors or private citizens). Identifying high-risk jurisdictions or known trends can also be included as part of your risk-based approach and internal STR process.

ML/TF indicators related to the use of other parties

In the course of a "normal" financial transaction, there are a "normal" number of parties who engage in the transaction, depending on the nature of the transaction at hand. For example, in the instance of depositing cash to a personal bank account, there is generally one party to the transaction: the person who holds the account is depositing into their own account. By contrast, with the deposit of cash to a business account, you can have many different parties, including: persons associated with the business's finance function who hold authority over the account, or an employee who may be charged with depositing the cash.

Transactions that involve parties not typically associated with a transaction can present an elevated risk of ML and/or TF. These additional parties can be used to allow a criminal to avoid being identified or being linked to an asset or account. This section includes examples of how the involvement of other parties may be indicative of the structure of a criminal enterprise. Some examples of such other parties include the use of a third party, nominee or gatekeeper.

Use of third party A third party is any person or entity that instructs someone to act on their behalf for a financial activity or transaction. There are some situations where there is an apparent and discernable rationale for the inclusion of the third party in a transaction and this may not be suspicious. However, you may become suspicious in a situation where the reason for a person or entity acting on behalf of another person or entity does not make sense based on what you know about the client or the third party. Use of third parties is one method that money launderers and terrorist activity financiers use to distance themselves from the proceeds of crime or source of criminally obtained funds. By relying on other parties to conduct transactions they can distance themselves from the transactions that can be directly linked to the suspected ML/TF offence. Some examples of ML/TF indicators related to the use of a third party can be found below.

- Multiple deposits which are made to an account by non-account holders.
- Unrelated parties sending email money transfers or other forms of electronic transfers to the same beneficiary with no apparent relation to the recipient.

- A client conducts a transaction while accompanied, overseen or directed by another party.
- A client makes numerous outgoing payments to unrelated parties shortly after they receive incoming funds.
- Wire transfers, deposits or payments to or from unrelated parties (foreign or domestic).
- Client appears to be or states they are acting on behalf of another party.
- Account is linked to seemingly unconnected parties.

Use of nominee A nominee is a particular type of other party that is authorized to open accounts and conduct transactions on behalf of a person or entity. There are legitimate reasons for relying on a nominee to conduct financial activity of behalf of someone else. However, this type of activity is particularly vulnerable to ML/TF as it is a common method used by criminals to distance themselves from the transactions that could be linked to suspected ML/TF offences. These are some examples of ML/TF indicators relating to the misuse of nominees.

- A person maintains multiple accounts, or maintains accounts in the names of family members or corporate entities with no apparent business or other purpose.
- A person or entity other than the stated account holder conducts the majority of the transaction activity, which seems unnecessary or excessive.
- Client is involved in transactions or account activities that are suspicious, but refuses or is unable to answer questions related to the account or transactions.

Use of gatekeeper A gatekeeper is a person who controls access to the financial system and can act on behalf of a client. Such services can be abused so that criminals have access to the financial system without being identified. Gatekeepers may include lawyers, accountants and other professions which can access the financial system on behalf of a client. While there are many transactions where it is "normal" to have a gatekeeper represent the interests of a client, such an appearance of normalcy can also be utilized to the advantage of criminals to provide the veneer of legitimacy to their transactions. The use of gatekeepers themselves is not an indicator of an ML/TF offence. However, entities should consider the following examples which can indicate misuse of the financial system access provided to gatekeepers.

- Gatekeeper avoids identifying their client or disclosing their client's identity when such identification would be normal during the course of a transaction.
- Gatekeeper is willing to pay higher fees and seeks to conduct the transaction quickly when there is no apparent need for such expediency.
- Gatekeeper is utilizing their account for transactions not typical of their business (e.g. pass through account, excessive amount of cash, payment

to non-clients or parties of transactions).
- Apparent misuse of correspondent accounts by gatekeeper to obscure the origin and/or destination of funds.

Indicators related to TF

In Canada, TF offences make it a crime to knowingly collect or provide property, which can include financial or other related services, for terrorist purposes. This section is focused on examples that are specific to the possible commission of a TF offence. However, please note that the other ML/TF indicators in this guidance may also prove relevant in determining when you have reasonable grounds to suspect the commission of TF, as the methods used by criminals to evade detection of ML are similar.

Indicators specifically related to TF:

The indicators below are some examples of indicators relating to TF.

- Transactions involving certain high-risk jurisdictions such as locations in the midst of or in proximity to, armed conflict where terrorist groups operate or locations which are subject to weaker ML/TF controls.
- An account opened in the name of an entity, a foundation or association, which may be linked or involved with a suspected terrorist organization.
- The use of funds by a non-profit organization is not consistent with the purpose for which it was established.
- Raising donations in an unofficial or unregistered manner.
- Client identified by media or law enforcement as having travelled, attempted or intended to travel to high-risk jurisdictions (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorist activities and organizations.
- Transactions involve persons or entities identified by media and/or sanctions lists as being linked to a terrorist organization or terrorist activities.
- Law enforcement information provided which indicates persons or entities may be linked to a terrorist organization or terrorist activities.
- Client conducted travel-related purchases (e.g. purchase of airline tickets, travel visa, passport, etc.) linked to high-risk jurisdictions (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorist activities and organizations.
- Person or entity's online presence supports violent extremism or radicalization.
- Client donates to a cause that is subject to derogatory information that is publicly available (e.g. crowdfunding initiative, charity, non-profit organization, non-government organization, etc.).

FINTRAC guidance related to the Ministerial Directive on Financial Transactions Associated with the Islamic Republic of Iran issued on July 25, 2020

This guidance explains the requirements of the Ministerial Directive on Financial Transactions Associated with the Islamic Republic of Iran.

1. Why this Ministerial Directive was issued

The Financial Action Task Force issued a statement in February 2020 which expressed its particular and exceptional concerns regarding Iran's failure to address strategic deficiencies in its anti-money laundering and combatting the financing of terrorism regime, and the serious threat this poses to the integrity of the international financial system. The Financial Action Task Force called on its members to apply effective counter-measures to protect their financial sectors from such risks.

As such, Canada's Finance Minister issued this Ministerial Directive to ensure the safety and integrity of Canada's financial system.

This Ministerial Directive includes requirements that:

- enhance existing obligations of the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations; and
- extend the obligations of the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations

2. Who needs to apply this Ministerial Directive

This Ministerial Directive came into effect on July 25, 2020, and is applicable to every person or entity referred to in paragraphs 5(a), (b) and (h) of the Act. The specific persons and entities that are to take action in response to this Ministerial Directive are:

- banks
- credit unions
- financial services cooperatives
- caisses populaires
- authorized foreign banks
- money services businesses

3. Requirements of the Ministerial Directive

Every bank, credit union, financial services cooperative, caisse populaire, authorized foreign bank and money services business must:

- treat **every** financial transaction **originating from or bound for Iran**, regardless of its amount, as a high-risk transaction for the purposes of subsection 9.6(3) of the Act
- verify the identity of any client (person or entity) requesting or benefiting from such a transaction in accordance with Part 3 of the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations
- exercise customer due diligence in relation to any such transaction, including ascertaining the source of funds or virtual currency, the purpose of the transaction and the beneficial ownership or control of any entity requesting or benefiting from the transaction
- keep and retain a record of any such transaction, in accordance with the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations, regardless of the monetary thresholds set out in those Regulations; and
- report all such transactions to the Centre

3.1 Determining that a transaction originated from or is bound for Iran

When determining whether a transaction originates from or is bound for Iran, you need to look at a variety of elements because the circumstances of each transaction are different. You must consider the facts, contexts and indicators of a transaction to determine whether it is subject to the Ministerial Directive. **Transactions originating from or bound for Iran may include, but are not limited to:**

- electronic funds transfers, remittances or other transfers that include an Iranian originating or destination address - this may include transactions where the ordering person or entity, beneficiary, or third party details are Iranian
- the activities of representatives of the Government of Iran (for example, transactions on an Embassy of Iran's bank account in Canada)
- receiving Iranian rial as a deposit to an account or for a virtual currency transaction
- conducting a foreign currency or virtual currency exchange transaction that includes Iranian rial (for example, Canadian dollar to Iranian rial, Iranian rial to US dollar, virtual currency to Iranian rial, etc.); and
- issuing or redeeming bank drafts or other negotiable instruments that include an Iranian rial component

This Ministerial Directive **does not** apply to transactions where there is no suspicion or explicit connection with Iran and there is no evidence of the transaction originating from or being bound for Iran. For example:

- a client who has previously sent funds to Iran requests an outgoing electronic funds transfer, where the transaction details do not suggest that this transaction is bound for Iran and you are unable to obtain further

details about the transaction destination
- the client's identification information is the only suggestion of a connection to Iran (for example, a transaction where the conductor's identification document is an Iranian passport); or
- the details of a person, who is your client in Canada, are Iranian, but there **are no additional details** on the entity involved, or the sender of, or the recipient to, the transaction, to suggest the transaction is associated with Iran

For further clarity, if the details of your client in Canada include an Iranian address and the client requests that funds be sent to a beneficiary in a country other than Iran, where additional facts, context and indicators (for example, beneficiary account details) point to an association with Iran, then this transaction must be considered as **bound for** Iran, and treated accordingly.

Similarly, if the details of your client in Canada include an Iranian address and this client receives funds into their account from a sending account in a country other than Iran, but where additional facts, context and indicators (for example, sending account details), point to an association with Iran, then this transaction must be considered as **originating from** Iran, and treated accordingly.

Alternatively, if the details of your client in Canada include an Iranian address and this client requests that funds be sent to a beneficiary in a country other than Iran, for which additional facts, context and indicators **do not** bring to light an association with Iran, then this transaction is not required to be considered for the purpose of the Ministerial Directive.

Unless the transaction is being carried out by, or benefitting, a representative of the Government of Iran in Canada, then the details of your client in Canada are not likely enough to consider the transaction against the obligations of the Ministerial Directive.

Note: When you have determined that a transaction originated from or was bound for Iran, you must apply the measures outlined in the Ministerial Directive.

3.2 Verifying the identity of every client who requests or benefits from a transaction originating from or bound for Iran

Under this Ministerial Directive, you must take enhanced identification measures that go beyond the identification triggers and requirements prescribed under the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations. Transactions that fall below the reporting threshold amounts typically do not require that you verify the identity of clients. However, under this Ministerial Directive, **you must:**

- verify the identity of **every client** (including those you have a business relationship with) that requests or benefits from such a transaction **in**

any amount in accordance with the methods prescribed in the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations; and
- for transactions that meet the reporting threshold amounts, apply **enhanced measures** to verify the identity of each client, as described in FINTRAC's ongoing monitoring guidance. Enhanced measures could include obtaining additional information on the client (for example, occupation, volume of assets, information available through public databases, Internet, etc.); gathering additional documents, data or information; or taking additional steps to verify the documents obtained, etc.

3.3 Additional measures required

You must treat **all** transactions originating from or bound for Iran as high risk. In addition to verifying the identity of any client requesting or benefiting from such a transaction, under this Ministerial Directive, you must:

- apply customer due diligence measures to these clients for all transactions (**any amount**)
- assess the client information to determine whether there are reasonable grounds to suspect the commission or attempted commission of a money laundering or terrorist activity financing infraction and to report it through a Reporting suspicious transactions to FINTRAC or Terrorist Property Report to FINTRAC
- apply enhanced measures to **every client** who meets the identification threshold (threshold transactions)
- obtain the purpose and the source of funds or virtual currency of any such transaction; and
- obtain the beneficial ownership or control information of any entity requesting or benefiting from such a transaction

Note: It is the reporting entity that owns the relationship with the client that is required to carry out the additional measures outlined in the Ministerial Directive (i.e., verifying the identity of the client, and exercising the customer due diligence measures).

4. Records you must keep and their retention period

4.1 Records of electronic funds and virtual currency transfers of any amount

For an electronic funds or virtual currency transfer **of any amount** originating from or bound for Iran, you must keep:

- the information included in an electronic funds transfer record, and the information included in a record for virtual currency transfers, **even if the transaction is below $ 1,000 CAD or an equivalent amount in virtual currency**:

  - if you are a bank, credit union, financial services cooperative or caisse populaire, you will find your record keeping requirements in the Record keeping requirements for financial entities guidance
  - if you are a money services business, you will find your record keeping requirements in the Record keeping requirements for money services businesses and foreign money services businesses guidance
- the source of funds or virtual currency of the transaction; and
- the purpose of the transaction

4.2 Records of receipt of cash or virtual currency – of any amount

You must keep a record of **every cash or virtual currency transaction (any amount)** that you receive that reflects a connection to Iran (such as cash received for the issuance of negotiable instruments or foreign exchange using Iranian rial). You must record:

- the information included in a large cash or virtual currency transaction record, **even if the transaction is below $10,000 CAD or an equivalent amount in virtual currency**, and the information included in a foreign or virtual currency exchange transaction record, **including the information that is required when a transaction is over $3,000 CAD**:
  - if you are a bank, credit union, financial services cooperative or caisse populaire, you will find your record keeping requirements in the Record keeping requirements for financial entities guidance
  - if you are a money services business, you will find your record keeping requirements in the Record keeping requirements for money services businesses and foreign money services businesses guidance
- the source of funds or virtual currency of the transaction; and
- the purpose of the transaction

4.3 Records of redeeming other negotiable instruments and records for issuing or redeeming transactions – of any amount:

Transactions originating from or bound for Iran also include the redemption of other negotiable instruments (for example, bank drafts, money orders, traveller's cheques, etc.) in any amount. These too will have to reflect a connection with Iran, such as the use of Iranian rial in the transaction, for the Ministerial Directive to be applicable. You must record:

- the information included in a transaction record, **even if the transaction is below $3,000 CAD or an equivalent amount in virtual currency**:

  - if you are a bank, credit union, financial services cooperative or caisse populaire, and a client is redeeming any amount in one or multiple money orders, your record keeping requirements are referenced in the Record keeping requirements for financial entities guidance
  - if you are a money services business, and a client is redeeming money orders in any amount, your record keeping requirements are referenced in the Record keeping requirements for money services businesses and foreign money services businesses guidance
- the source of funds or virtual currency of the transaction; and
- the purpose of the transaction

4.4 Information on records and retention

If you are required by this Ministerial Directive to keep a record of information that is readily available in other records, you do not have to record the same information again. This means that if you keep the required information and can produce it during a FINTRAC examination, you do not need to create a new record to meet the obligations.

You must keep all records applicable to this Ministerial Directive in accordance with their associated record retention requirement, or for at least five years from the date the record was created.

5. Reporting transactions captured under this Ministerial Directive

5.1 Reporting an electronic funds transfer in any amount to FINTRAC:

- SWIFT electronic funds transfers that are under the reporting threshold of $10,000 CAD and **do not** aggregate to $10,000 CAD under the 24-hour rule and **involve** Iranian rial (IRR), **must be reported using the SWIFT Electronic Funds Transfer Report with the following addition**:
  - Insert the prefix **IR2020** before entering your reporting entity's report reference number. For example, if your reporting entity's report reference number is ABCD1234, then your reporting entity's report reference number would be IR2020ABCD1234.
- SWIFT electronic funds transfers that are under the reporting threshold of $10,000 CAD, **do not** aggregate to $10,000 CAD under the 24-hour rule, and **do not** involve Iranian rial (IRR), **must be reported using the Non-SWIFT Electronic Funds Transfer Report with the following addition:**

  - Insert the prefix **IR2020** before entering your reporting entity's report reference number. For example, if your reporting entity's report reference number is ABCD1234, then your reporting entity's report reference number would be IR2020ABCD1234.

Note: These transactions must have an Iranian address in at least one of the fields.

- Non-SWIFT electronic funds transfers that are under the reporting threshold of $10,000 CAD, and **do not** aggregate to $10,000 CAD under the 24-hour rule, must be reported using the Non-SWIFT Electronic Funds Transfer Report **with the following addition**:
  - Insert the prefix **IR2020** before entering your reporting entity's report reference number. For example, if your reporting entity's report reference number is ABCD1234, then your reporting entity's report reference number would be IR2020ABCD1234.
- SWIFT and Non-SWIFT electronic funds transfers of $10,000 CAD or more, and SWIFT and Non-SWIFT electronic funds transfers resulting from aggregated transactions of $10,000 CAD or more captured under the 24-hour rule are to be reported normally:
  - No prefix is required
- Transfers of funds within Canada, of any amount, where it is deemed that the transaction is originating from or bound for Iran, must be reported using the suspicious transaction report as follows:
  - Insert the prefix **IR2020** before entering your reporting entity's report reference number. For example, if your reporting entity's report reference number is ABCD1234, then your reporting entity's report reference number would be IR2020ABCD1234.
  - As applicable Part B1, Item 5 – "other description" – transfer gov't Iran
  - As applicable Part B2, Item 12 – "other description" – transfer, gov't Iran
  - Insert the prefix **IR2020** into the G section of the Suspicious Transaction Report as well.
  - Because the report is related to the Ministerial Directive, **you must** ensure that information provided, such as currency type, or address or disposition details, reflect the connection to Iran.

5.2 Reporting the receipt of any amount of cash to FINTRAC:

- Any cash received (for example, Iranian rial deposited to an account, or Iranian rial received in exchange for virtual currency, CAD, or any other type of currency) that is under the reporting threshold of $10,000 CAD and **does not** aggregate to $10,000 CAD under the 24-hour rule must

be reported using the Large Cash Transaction Report. Select 'IR2020' in the Ministerial Directive field to indicate the transaction is being reported under the Ministerial Directive.

Note: Because the report is related to the Ministerial Directive, **you must** ensure that the information provided reflects a connection to Iran.

- Large cash transactions of $10,000 CAD or more, and large cash transactions that total $10,000 CAD or more when aggregated under the 24-hour rule are to be reported normally.

5.3 Reporting virtual currency transactions using the Large Virtual Currency Transaction Report :

- Any transaction involving the receipt of virtual currency for exchange to Iranian rial that is equivalent to an amount under the reporting threshold of $10,000 CAD must be reported using the Large Virtual Currency Transaction Report. Select 'IR2020' in the Ministerial Directive field to indicate the transaction is being reported under the Ministerial Directive.

  Note: Because the report is related to the Ministerial Directive, **you must** ensure that the information provided reflects a connection to Iran.

- Virtual currency transactions received in an amount equivalent to $10,000 CAD or more, and virtual currency transactions received that fall under the 24-hour rule are to be reported as normal.

5.4 Reporting negotiable instruments and issuing or redeeming transactions:

- Any negotiable instrument, and issuing or redeeming transaction that originates from or is bound for Iran, must be reported using the Reporting suspicious transactions to FINTRAC. In order to identify these transactions, submit the Suspicious Transaction Report with the following additions **when the transactions do not meet the reasonable grounds to suspect** the commission or attempted commission of a money laundering or a terrorist activity financing offence threshold:
  - Insert the prefix **IR2020** before entering your reporting entity's report reference number. For example, if your reporting entity's report reference number is ABCD1234, then your reporting entity's report reference number would be IR2020ABCD1234.
  - Insert the prefix **IR2020** into the G section of the suspicious transaction report as well.
  - Because the report is related to the Ministerial Directive, **you must** ensure that there is a connection to Iran, such as the Iranian rial, or the conductor address is Iranian.

5.5 Reporting suspicious transactions and terrorist property:

- All transactions that are associated with Iran must be treated as high risk and must be monitored for the purpose of determining whether a Suspicious Transaction Report or a Terrorist Property Report must be submitted to FINTRAC.
- For the purpose of this Ministerial Directive, only completed transactions must be reported if the sole reason for reporting is that the transaction is inbound from or outgoing to Iran. Attempted transactions remain reportable in instances where the reporting entity has reasonable grounds to suspect that the transaction is related to the attempted commission of a money laundering or a terrorist activity financing offence.
- See Reporting suspicious transactions to FINTRAC for more information.
- If you have property in **your possession or control** that you **know or believe** is owned or controlled by or on behalf of a listed person or a terrorist group you must submit a Terrorist Property Report to FINTRAC. This includes information about any transaction or proposed transaction relating to that property. See Reporting terrorist property to FINTRAC for more information.

5.6. Reporting timeframes:

- Where the Ministerial Directive reflects an enhancement to a current transaction reporting obligation (for example, the threshold to report has been reduced or eliminated) the timing for reporting that transaction remains that of the obligation being enhanced:
  - Electronic funds transfers must be reported no later than 5 working days after the day the reporting entity knows that the transfer must be reported;
  - Large cash transactions must be reported within 15 days after the transaction.
- Where the Ministerial Directive reflects an extension of reporting obligations to transactions that previously had no reporting obligation, such as the redemption of a negotiable instrument, transfers of funds within Canada, which are to be reported by means of the suspicious transaction reporting form, it is reasonable for the reporting entity to report this as soon as practicable.

Other

Your compliance program's policies and procedures should already include information on how your organization becomes aware of Ministerial Directives issued by the Minister of Finance and information on how your organization will respond. Once a Ministerial Directive has been issued, you must take steps to meet its requirements.

Your policies and procedures must also fully describe how you will make the

determination that a transaction originates from or is bound for Iran and what specific mitigation measures you will take upon making this determination. For example, your policies and procedures could outline that you ask the purpose of a transaction. Similarly, you could research the origin or destination of a transaction to determine if the details about the sender, beneficiary or entities involved in the transaction, indicate that the transaction is originating from or bound for Iran.

Guidance on how to conduct and document your risk assessment can be found in the Risk assessment guidance. You are required to implement certain measures to mitigate the risk of transactions involving jurisdictions that are identified in Ministerial Directives. Examples of these measures can be found in General information on Part 1.1 of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act provided by the Department of Finance Canada.

During a compliance examination, FINTRAC may assess your compliance with any Ministerial Directive in order to verify that you have taken appropriate mitigating measures in relation to related transactions. FINTRAC may also review your overall risk assessment to verify that you have documented and assessed the risk related to your business activities and clients involving these jurisdictions. Failure to comply with the measures of a Ministerial Directive is a very serious offence. The existing administrative monetary penalties regime extends to all Ministerial Directives, and failure to comply with a directive could result in a penalty. Penalties applicable to the breach of a directive can be found in the Proceeds of Crime (Money Laundering) and Terrorist Financing Administrative Monetary Penalties Regulations.