COMPLIANCE PROGRAM FOR ANTI- MONEY LAUNDERING AND COMBATING THE TERRORISM FINANCING

SNOWCAP FINANCIAL LIMITED (BC1484570)
Issued on: June 2024
Next update: January 2025

CONTENTS

I. BACKGROUND INFORMATION

This section provides a high-level summary regarding what money laundering and terrorist financing is, and our obligations under the law. This summary relies on information provided in the Financial Transactions and Reports Analysis Centre Canada's (FINTRAC's) Guideline 1, Background, and the full version of the guideline can be found on FINTRAC's website:

https://fintrac-canafe.canada.ca/intro-eng

Canada actively participates in the global efforts to combat money laundering and the funding of terrorist activities primarily through the national legislative framework known as the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (referred to as "The Act") and its associated regulations. The primary objectives of The Act include:

1. Detecting and deterring money laundering and the financing of terrorist activities effectively.
2. Implementing reporting and compliance requirements on entities engaged in businesses, professions, and activities with a susceptibility to money laundering and terrorist financing.
3. Establishing FINTRAC (the Financial Transactions and Reports Analysis Centre of Canada) as the designated agency responsible for collecting, analyzing, and disseminating information to facilitate the identification and prevention of money laundering and terrorist financing activities within Canada and internationally.

What is money laundering?

Money laundering constitutes a process, encompassing any act or attempted action, through which funds and assets derived from criminal activities are camouflaged to appear as originating from lawful sources. Essentially, it entails the transformation of ill-gotten gains, often referred to as "dirty money," obtained through criminal endeavors, into "clean money" that is challenging to trace back to its criminal origins. This money laundering process is commonly recognized to involve three distinct stages:

1. Placement: The initial stage involves the introduction of unlawfully obtained funds into the legitimate financial system.
2. Layering: Subsequent to placement, layering entails the conversion of these criminal proceeds into alternative forms and the creation of intricate layers of financial transactions. This complexity serves to obstruct the audit trail, concealing the true source and ownership of the funds.
3. Integration: In the final stage, integrated laundered proceeds are reintroduced into the economy, thereby fostering the appearance of legitimacy.

Money laundering begins with the illicit proceeds stemming from a predicate offense. These predicate offenses encompass a broad range of illegal activities, including but not limited to tax evasion, illicit drug trafficking, bribery, fraud, forgery, murder, robbery, counterfeit currency production, stock manipulation, and copyright infringement. It's important to note that a money laundering offense can encompass both property and proceeds derived from illegal activities that occurred outside the jurisdiction of Canada.

Methods of money laundering

There are multiple methods employed in the process of money laundering. Moreover, these techniques are continually evolving, growing in sophistication and intricacy in tandem with technological advancements. Frequently, money launderers utilize nominees, individuals such as trusted family members, close friends, or associates deeply rooted in the community. These nominees are strategically chosen for their ability to operate discreetly, thereby avoiding detection, while simultaneously aiding in the obfuscation of the source and true ownership of funds, as well as facilitating financial transactions.

Another prevalent strategy involves the practice commonly known as "structuring" or "smurfing." This tactic involves multiple inconspicuous individuals making deposits into a central account, often ensuring that these deposits remain below thresholds that would necessitate reporting. The section below provides instructive insights into potential indicators and transaction patterns that warrant vigilance, as they may have connections to money laundering activities.

What is terrorist financing?

Under the purview of Canadian law, the act of financing terrorist activities entails the conscious and deliberate collection or provision of assets, including monetary funds, either directly or indirectly, to individuals or entities involved in acts of terrorism. The primary objective behind such acts of terrorism typically revolves around instilling fear within a populace or exerting coercive pressure on a government to yield to specific demands. To effectively execute their nefarious activities and realize their objectives, terrorists invariably require financial sustenance.

Notably, many of the methodologies commonly employed in the realm of money laundering are also enlisted in the context of terrorist financing. These techniques encompass a range of practices, including but not limited to obfuscating the trail of funds and leveraging third parties to facilitate financial transactions. The imperative for terrorists is to conceal the origin of their funds, making them appear as if they originate from a legitimate source, to transform them into a format that resists easy traceability, rendering them practical for their intended purposes.

Methods of terrorist financing

There exist two primary sources of funding for terrorist activities. The first involves obtaining financial support from countries, organizations, or individuals. The second encompasses revenue-generating activities undertaken by terrorist groups, which may encompass both lawful and unlawful activities.

Terrorist organizations commonly engage in various illicit pursuits, including but not limited to smuggling, fraud, theft, robbery, and narcotics trafficking, to amass financial resources. Additionally, funding for these groups may originate from legitimate sources, such as membership fees, subscription revenues, the sale of publications, earnings from speaking engagements and cultural or social events, as well as solicitation and appeals within communities. It is pertinent to note that fundraising activities may be conducted under the guise

of charitable or relief organizations, potentially misleading donors into believing they are contributing to a legitimate philanthropic cause.

The strategies employed by terrorist groups to acquire resources from illicit origins frequently mirror those utilized by conventional criminal organizations. Consequently, transactions linked to terrorist financing may bear resemblances to those associated with money laundering activities. As such, the implementation of robust and comprehensive anti-money laundering protocols assumes significance in monitoring and scrutinizing the financial operations of terrorists.

Our responsibilities

Every Money Services Business (MSB) operating in Canada is categorized as an entity under the Act and is obligated to adhere to the following requirements:

- Establish a comprehensive compliance program designed to ensure adherence to reporting, record-keeping, and client identification stipulations.
- Adhere to protocols governing client identification and maintain meticulous records related to specific transactions.
- Report suspicious transactions, significant cash transactions, and provide information pertaining to terrorist assets to FINTRAC (Financial Transactions and Reports Analysis Centre of Canada).

The constituent components of a compliance program mandated by the Act encompass the following:

- Designation of a Compliance Officer responsible for overseeing compliance activities.
- Formulation and implementation of written compliance policies and procedures.
- The evaluation and documentation of money laundering and terrorist financing risks associated with the business, accompanied by strategies for risk mitigation.
- Implementation of an ongoing training regimen, particularly if the agent or agency employs individuals or designates others to act on its behalf.
- Formulation of a plan for periodically reviewing the effectiveness of compliance policies and procedures, alongside the risk assessment, with the provision for testing their efficacy at least once every two years.

Penalties for non-compliance

FINTRAC possesses the authority to impose Administrative Monetary Penalties (AMPs) on reporting entities that fail to comply with the provisions of the Act. Violations are categorized under the Act as either minor, serious, or very serious, each carrying distinct ranges of penalties:

- Minor Violation: Fines ranging from $1 to $1,000 per individual violation.
- Serious Violation: Penalties ranging from $1 to $100,000 per individual violation.
- Very Serious Violation: For individuals, fines ranging from $1 to $100,000 per violation, and for entities (e.g., corporations), penalties ranging from $1 to $500,000 per violation. It's important to note that these limits apply to each violation, and multiple violations can cumulatively result in a total amount exceeding these limits.

In instances of extensive non-compliance or when there is a minimal expectation of immediate or future compliance, FINTRAC reserves the right to disclose cases of non-

compliance to law enforcement agencies. Criminal penalties associated with the Act encompass the following:

- Failure to Report Suspicious Transactions: Potential penalties of up to $2 million in fines and/or up to five years of imprisonment.
- Failure to Report a Large Cash Transaction or an Electronic Funds Transfer: Penalties of up to $500,000 for the first offense, escalating to $1 million for subsequent offenses.
- Failure to Meet Record-Keeping Requirements: Penalties of up to $500,000 in fines and/or up to five years of imprisonment.
- Failure to Provide Assistance or Information During Compliance Examination: Penalties of up to $500,000 in fines and/or up to five years of imprisonment.
- Disclosure of a Suspicious Transaction Report or Its Contents with the Intent to Prejudice a Criminal Investigation: Potential imprisonment for up to two years.

It is essential to note that penalties for failure to report do not apply to employees who duly report suspicious transactions to their superiors.

Indicators of suspicious transactions or potential high-risk clients

Below are examples of general and industry-specific indicators that may give rise to reasonable suspicion that a transaction is connected to money laundering or terrorist activity financing. It is important to note that the presence of one or more of these factors does not automatically imply that the transaction is suspicious and should be reported to FINTRAC. Instead, it suggests that a more thorough examination is warranted.

General indicators

The following are several general indicators that may raise suspicions regarding a transaction's potential association with money laundering or terrorist activity financing offenses. It is essential to recognize that it is typically not just one of these factors in isolation but rather a combination of several factors in conjunction with what is customary and reasonable within the context of the transaction or attempted transaction:

- The client confesses to or makes statements acknowledging involvement in criminal activities.
- The client exhibits reluctance or attempts to evade providing required information or submits information that is misleading, ambiguous, or challenging to verify.
- The client presents seemingly counterfeit, altered, or inaccurate documentation.
- The client appears to maintain accounts with multiple financial institutions in a single area without apparent justification.
- The client frequently uses a consistent address while frequently altering the associated name.
- The client displays an unusual level of interest in internal controls and systems.
- The client provides confusing or inconsistent details concerning the transaction.
- The client makes inquiries that suggest an intention to circumvent reporting requirements.
- The client engages in atypical activities relative to their established patterns, whether as an individual or a business entity.
- The client presents obscure or scant information regarding the transaction's purpose.

- The client demonstrates a notable familiarity with matters related to money laundering or terrorist activity financing.
- The client refuses to furnish personal identification documents.
- The client frequently travels to regions designated as high-risk in terms of financial improprieties.

It is important to reiterate that the mere presence of one or more of these indicators should prompt a more comprehensive examination of the transaction, taking into account the broader context and established norms for similar transactions.

Industry specific examples

- The client requests a transaction at a foreign exchange rate that surpasses the publicly posted rate.
- The client expresses a willingness to pay transaction fees that exceed the officially posted fees.
- The client engages in currency exchange and specifically requests the largest possible denomination bills in a foreign currency.
- The client exhibits limited knowledge regarding the address and contact details of the payee, is reluctant to divulge such information, or requests a bearer instrument.
- The client requests a cheque issued in the same currency as the one being cashed.
- The client seeks to convert cash into a cheque, a service not typically offered by your institution.
- The client desires to exchange cash for numerous postal money orders in small denominations, payable to numerous other parties.
- The client initiates transactions with counterparties in locations that deviate from their usual pattern.
- The client instructs that funds are to be picked up by a third party acting on behalf of the payee.
- The client conducts substantial purchases of traveler's cheques, which do not align with their known travel plans.
- The client makes purchases of money orders in substantial quantities.
- The client requests multiple cheques in small amounts, each bearing different names, the cumulative total of which equals the exchange amount.
- The client requests that a cheque or money order be made payable to the bearer.
- The client requests the exchange of a significant quantity of one foreign currency into another foreign currency.
- The client acquires a substantial volume of money orders and modifies the payment type to circumvent reporting requirements.

It is essential to stress that these indicators serve as red flags necessitating a more in-depth assessment of the transaction's circumstances, considering the broader context and the norms applicable to transactions of a similar nature.

II. POLICIES AND PROCEDURES

The policies and procedures below provide the roles and responsibilities and information for identifying reportable transactions and reporting to FINTRAC, record keeping, record retention, ascertaining identity, risk-based approach, and training program.

Reporting to FINTRAC and related record keeping.

There are various types of reports that may be required to be submitted to FINTRAC:

- Suspicious transaction reporting
- Large cash transaction reporting
- Terrorist property reporting
- Electronic funds transfer reporting

Details of how to report, information required when reporting and related records that must be retained are found in the sections below.

Enrolment with FINTRAC's electronic reporting system

The Compliance Officer holds the responsibility of ensuring the Company's enrollment in FINTRAC's electronic reporting system, F2R system, for electronic reporting purposes.

Following successful enrollment, FINTRAC furnishes an identifier number, which must be included in the Company's reports. This identifier number is retained by the Compliance Officer. It is incumbent upon the Compliance Officer to submit all reports to FINTRAC and ensure the completeness and accuracy of the information furnished in a Suspicious Transaction Report (STR).

Contact information for enrollment:

- FINTRAC's Electronic Reporting Enrollment
- Toll-free phone: 1-866-346-8722 (select <4> after choosing your language)
- Address: Financial Transactions and Reports Analysis Centre of Canada, 234 Laurier Avenue West, 24th Floor, Ottawa, ON K1P 1H7, Canada.

Suspicious transactions reporting and record keeping policy

Definition of Suspicious Transactions: Suspicious transactions refer to financial transactions that the Company possesses reasonable grounds to suspect are linked to the perpetration of a money laundering offense or a terrorist activity financing offense. This extends to attempted transactions that the Company has reasonable grounds to suspect are associated with money laundering or terrorist financing offenses.

Requirement: The Company is mandated to promptly report completed or attempted suspicious transactions to FINTRAC as soon as feasibly possible after undertaking appropriate measures to ascertain the suspicion. A comprehensive record of these transactions, including the circumstances leading to the suspicion, must be maintained. The Company must implement measures that enable it to establish reasonable grounds for suspecting that a transaction or attempted transaction is linked to the commission of a money laundering offense or a terrorist activity financing offense. It's crucial to emphasize that there is no minimum threshold amount for reporting a suspicious transaction.

These measures encompass:

- Screening for and Identifying Suspicious Transactions: The Company should have mechanisms in place to screen and identify transactions that appear suspicious.

- Assessing the Facts and Context: A comprehensive assessment of the circumstances and context surrounding the suspicious transaction is imperative.
- Linking Money Laundering/Terrorist Financing Indicators: This entails connecting indicators of money laundering and terrorist financing to the assessment of the facts and context.
- Explaining Grounds for Suspicion in an STR: In the Suspicious Transaction Report (STR), the Company should articulate the rationale for its suspicion. This explanation should elucidate how the facts, context, and money laundering/terrorist financing indicators collectively led to the reasonable grounds for suspicion.

The term "as soon as practicable" should be construed to mean that the Company has concluded the measures necessary to establish reasonable grounds for suspicion.

Subsequently, the development and submission of the STR should be accorded a high priority status to ensure timely reporting.

Procedures dictate that all employees are obligated to promptly report any transactions they suspect to be suspicious to the Compliance Officer as soon as the suspicion arises.

Subsequently, the Compliance Officer assumes responsibility for filing all Suspicious Transaction Reports (STRs) with FINTRAC and informing senior management about the submission of these reports. Copies of the reports submitted, along with the acknowledgments received from FINTRAC, must be securely retained.

The Compliance Officer is required to transmit STRs to FINTRAC electronically. However, in cases where the Compliance Officer lacks the technological capability for electronic

submission, they must opt for a paper-based submission.

There are two available options for electronic reporting, both ensuring the confidentiality and integrity of transmitted data:

1. FINTRAC Web Reporting: https://www.fintrac-canafe.gc.ca/reporting-declaration/Info/f2r-eng
2. Batch File Transfer: https://www.fintrac-canafe.gc.ca/reporting-declaration/Info/batch-lots-eng#how

Information to be contained in suspicious transaction report.

A comprehensive and well-constructed Suspicious Transaction Report (STR) should take into account the following key questions:

- Who Are the Parties to the Transaction? Identify and provide details about the individuals or entities involved in the transaction.
- When Was the Transaction(s) Completed/Attempted? Specify the date and time of the transaction(s). If the transaction was not completed, explain the reasons for its non-completion.
- What Are the Financial Instruments or Mechanisms Used? Describe the financial instruments or mechanisms employed to execute the transaction.
- Where Did This Transaction Take Place? Indicate the location or locations where the transaction(s) occurred.

- Why Are the Transaction(s) Related to ML/TF Offenses? Provide a detailed explanation of why you believe the transaction(s) or attempted transaction(s) are associated with the commission or attempted commission of money laundering (ML) or terrorist financing (TF) offenses. Elaborate on the grounds for your suspicion, including the facts, context, and money laundering/terrorist financing indicators that led to this determination.

Regarding record-keeping requirements, the Company is obligated to maintain a copy of an STR for a minimum period of five years from the date when the report was submitted.

Large cash transaction reporting and record keeping policy.

Requirement: When a Money Services Business (MSB) receives $10,000 CAD or more in cash, whether through a single transaction or multiple transactions within a 24-hour period, the MSB is obligated to submit a report within 15 calendar days. Additionally, if the MSB is aware that two or more cash transactions, each amounting to less than $10,000 CAD, were conducted within a 24-hour period by or on behalf of the same client and cumulatively reach $10,000 or more, these are considered a single large cash transaction.

Policy: The Company has a policy of not accepting cash from clients, and consequently, the Company is not required to submit a large cash transaction report or maintain records related to such transactions.

Procedures: In instances where clients attempt to provide cash as payment for a transaction, alternative payment options are presented. In the event that cash is accepted in error, the following actions will be undertaken:

- The Compliance Officer is responsible for submitting large cash transaction reports within 15 calendar days of the transaction.
- The creation and retention of a large cash transaction record.
- The retention of a copy of the large cash transaction records in a secure location.

Information to Include on a Large Cash Transaction Report: Detailed guidance on the information that needs to be included in a large cash transaction report can be found in FINTRAC's guidelines, specifically, Guideline 7A6 for electronic submissions and Guideline 7B7 for paper submissions.

Record Keeping: The Company must retain large cash transaction records for a minimum period of five years from the date the record was initially created.

Large virtual currency transaction reporting and record keeping policy

Requirement: When MSB receives $10,000 CAD or more in virtual currency, within a 24-hour period MSB must submit a report within 5 working days, when the following criteria is met:

- Payments were conducted by the same person or entity,
- Payments were conducted on behalf of the same person or entity, or
- Payments are for the same beneficiary.

If MSB knows that two or more virtual currency transactions of less than $10,000 CAD each were made within a 24-hour period (that is, 24 consecutive hours), by or on behalf of the same

client, these are considered to be a single large cash transaction if they add up to $10,000 or more.

Exceptions to reporting large virtual currency transactions.

Exceptions to reporting Large Virtual Currency Transactions (LVCTR) apply to the initial receipt of virtual currency. It's important to note that subsequent transactions or activities may still entail reporting obligations, among other responsibilities. Specifically, an LVCTR is not required when MSB receives two or more amounts in virtual currency, each individually equivalent to less than $10,000 but collectively totaling $10,000 or more within 24 consecutive hours, provided that it is known these amounts are designated for a beneficiary falling within one of the following categories:

- A public body.
- A very large corporation or trust.
- An administrator of a pension fund regulated under federal or provincial legislation.

Furthermore, an MSB is not obliged to submit an LVCTR when it receives virtual currency amounting to $10,000 or more in a single transaction if the virtual currency is received as:

- Compensation for validating a transaction recorded in a distributed ledger.
- A nominal amount of virtual currency solely for the purpose of validating another transaction or transferring information.

Additionally, an MSB is exempt from submitting an LVCTR when it receives virtual currency for its own operational purposes. For example, an MSB is not obligated to report the receipt of virtual currency when it is acquired or received as part of its business holdings.

Terrorist property reports

Requirement: If the Company possesses or controls property that it knows or believes is owned or controlled by or on behalf of a terrorist group, the Compliance Officer must promptly report this to FINTRAC. There are two situations that can trigger the requirement to submit a terrorist property report to FINTRAC:

1. *Knowing Ownership or Control by a Terrorist or Terrorist Group*: This applies when the Company is aware that property is owned or controlled by or on behalf of a terrorist or a terrorist group. A terrorist or terrorist group includes any entity whose purposes or activities involve facilitating or carrying out terrorist activities.
2. *Believing Ownership or Control by a Listed Person*: This situation arises when the Company believes that property is owned or controlled by or on behalf of a listed person. A listed person can be an individual, corporation, trust, partnership, fund, or unincorporated association or organization believed to have carried out, attempted to carry out, participated in, or facilitated a terrorist activity. It can also include entities controlled directly or indirectly by, acting on behalf of, at the direction of, or in association with any individual or entity involved in such activities.

Policy: The Company conducts regular screening of its clients against lists (daily basis), and transactions are screened against lists while also being checked against money laundering and terrorist financing indicators (as outlined in Appendix II of this Compliance program).

Any instances of terrorist property within the Company's possession or control are promptly reported to the Compliance Officer.

Procedures: In the event that a report is required, the Compliance Officer follows these steps:

- Submits the report to FINTRAC.
- Notifies the Royal Canadian Mounted Police (RCMP) via unclassified fax at (613) 825-7030.
- Notifies the Canadian Security Intelligence Service (CSIS) Financing Unit via unclassified fax at (613) 369-2303.

Terrorist reports must be submitted to FINTRAC via paper. Reporting forms can be obtained and printed from FINTRAC's website: FINTRAC Reporting Forms. Alternatively, forms can be requested by calling 1-866-346-8722 for faxing or mailing to the Company.

When filing a report, the Compliance Officer follows the guidelines outlined in FINTRAC's Guideline 5 for submitting terrorist property reports.

Electronic funds transfer reporting

Requirement: The Company is mandated to report incoming and outgoing international electronic funds transfers (EFTs) amounting to $10,000 CAD or more to FINTRAC within five working days from the day of transmitting the instructions. These instructions, whether in the form of non-SWIFT or SWIFT MT 103 messages, pertain to the electronic transfer of $10,000 or more outside Canada (outgoing) or from outside Canada (incoming) at the request of a client. This reporting obligation applies in two scenarios:

1. Single Transaction: EFTs of $10,000 CAD or more are transmitted in a single transaction.
2. 24-Hour Rule Situation: EFTs are conducted in two or more transfers, each of which is less than $10,000 CAD but together amount to $10,000 CAD or more, within 24 consecutive hours of each other by or on behalf of the same individual or entity.

Exception to the 24-Hour Rule for EFTs: An exception to the 24-hour rule applies if the Company sends or receives a bundled EFT, which is an EFT with more than one beneficiary. In this case, the 24-hour rule does not apply to any amounts under $10,000 included in a bundled EFT if it was sent at the request of a public body, a very large corporation, or the administrator of a federally or provincially regulated pension fund.

Policy: The Company conducts regular transaction screening on a daily basis.

Procedures: The Compliance Officer holds responsibility for submitting both SWIFT Electronic Funds Transfer Reports and non-SWIFT Electronic Funds Transfer Reports to FINTRAC. These reports must be sent to FINTRAC no later than five working days after the day of the transfer. The "day of the transfer" is defined as follows:

- For incoming EFTs: The day the instructions were transmitted to the Company.
- For outgoing EFTs: The day the Company transmits the instructions regarding the transfer of funds.

When filing an EFT report, the Compliance Officer follows FINTRAC's guidelines, specifically:

- Guideline 8A: Submitting non-SWIFT Electronic Funds Transfer Reports to FINTRAC electronically.
- Guideline 8B: Submitting SWIFT Electronic Funds Transfer Reports to FINTRAC.
- Guideline 8C: Submitting Non-SWIFT Electronic Funds Transfer Reports to FINTRAC by paper.

III. CLIENT INFORMATION RECORD KEEPING

During the establishment of a business relationship and account opening, the Company utilizes applications and forms to gather essential client information. For individual clients, this information collection may encompass, as necessary but not restricted to, elements such as identification, occupation, industry, employment details, address, tax residency, date of birth, source of wealth, intended purpose and usage of products and services, any third-party involvement, and any known political exposure.

For clients structured as legal entities, additional information is obligatory to identify beneficial owners and those in control of the entity, as guided by FINTRAC and detailed below.

Client Information Record

Policy: Client information records are maintained for all clients engaged in a business relationship with the Company.

Procedures: In practice, the Company fulfills its obligation to establish a client information record by completing client applications for payment products and services. These applications capture all requisite information. The data retained in client information records may vary based on the client type (individual or entity) and the nature and volume of the client's transactions. Key components of client information records encompass:

- Client identification details (applicable to both individuals and entities).
- Industry and occupation (pertaining to business types for entities).
- Beneficial ownership information (pertaining to entities).
- Third-party determination and related information.
- Determination of politically exposed persons.
- Information concerning the business relationship, including the purpose and intended use of the products and services.

Specific requirements for each component of the client information record are elucidated in the subsequent section.

Summary chart

Client information record component	When required	Information required to be retained
Client information for individuals – Recorded on applications and forms.	If the Client is establishing a business relationship with the Company or for occasional transaction.	Client information: • Name • Address • Date of birth • Industry and occupation (descriptive)

Client information and beneficial ownership and control records for entities – Recorded on applications, forms and copies retained of supporting documentation from the client.	If the Client is establishing a business relationship with the Company or for occasional transaction.	• Entity name • Address • Incorporation or other identifying number • Jurisdiction of incorporation • Detailed description of the entity's principal business and industry • Signatory information (name, address, date of birth, occupation, identification details including type, identifying number, place of issue, and expiry) Information to Confirm the Existence of an Entity and Beneficial Ownership, Structure, and Control Information: • Copies of documents used to confirm the existence of the entity, such as: o Certificate of corporate status (for corporations) o Notice of assessment issued by municipal, provincial, territorial, or federal government (for corporations) o Partnership agreement (for entities other than corporations) o Articles of association (for entities other than corporations) • Copies of records obtained to confirm information about the individuals who ultimately control the entity, including ownership details. In addition to the previously mentioned client information, the following details are required for entities: • For Corporations: o Names of all directors. • For Trusts: o Names and addresses of trustees, known beneficiaries, and settlors of the trust. • For Entities Other Than Trusts: o Names and addresses of all individuals/entities who directly or indirectly own or control 25% or more of the entity. Moreover, comprehensive information that establishes the ownership, control, and structure of the entity is necessary.

		In cases where it is not possible to obtain this information or its accuracy cannot be confirmed, the Company should record the following: • Name of the most senior managing officer of the entity. • Ascertain their identity. • Treat the client as high risk.
Politically exposed person (PEP) or Head of an International organization (HIO) determination – Recorded on applications and forms.	If the Client is establishing a business relationship with the Company or for occasional transaction.	PEP determination – is client a PEP or HIO (includes close relatives/close associates)? Yes or no recorded-on applications and forms. If yes: • The name, relationship and office/position of the individual who is a PEP and country. • The source of the funds, if known, that were used for the transaction. • The date you determined the individual to be a PEP or HIO. • The name of the member of Senior management who reviewed the transaction. • The date the transaction was reviewed.

What is beneficial ownership and control?

Beneficial ownership pertains to identifying the individuals who ultimately control, either directly or indirectly, 25% or more of the shares or rights of a corporation or entity. The concept of indirect ownership is crucial, as it may necessitate additional documentation to ensure that all beneficial owners are disclosed.

Policy: When verifying the existence of an entity, the Company must take reasonable measures to confirm and maintain records of information related to the entity's beneficial ownership. This information is documented on applications and forms, and copies of all documentation used to obtain or confirm beneficial ownership and control (including those listed in the table above) are retained in the client file. For additional information on confirming the existence of entities, refer to Client Identification Section of this program.

Procedures: The Compliance officer must conduct a thorough search through as many levels of information as necessary to ascertain beneficial ownership. In cases where there is no individual who owns or controls 25% or more of an entity, the Compliance officer must still maintain a record of the information obtained. Reasonable measures to confirm the accuracy of beneficial ownership information include requesting suitable documentation from the client or referring to publicly available records. Documents obtained to confirm the information or the public source (e.g., the website where the Compliance officer found the information) must be retained in the Company's records.

The Company is not required to identify the most senior managing officer when there is no individual who owns or controls 25% or more of an entity. However, as a part of the Company's business practice, the Compliance officer records the names of individuals who hold a managing role or control over a percentage of shares that the Compliance officer deems significant (e.g., 10%), even if it is less than 25%.

If the client refuses to provide beneficial ownership information for a legal entity when a beneficial owner exists, the client must be considered high risk, and additional identification of the most senior managing officer is necessary. It may also be decided not to proceed with doing business with this client without this information.

For further guidance on examples of ownership, control, and structure, refer to FINTRAC's Guidance.

What is a business relationship?

Business relationships are formed when a client opens an account with the Company or, if they do not have an account, after the client has conducted two or more transactions or activities through the Company, requiring identity verification. The Company establishes business relationships with all clients who open accounts and maintains records of the account's purpose and intended use, as well as payment services and products. For occasional transactions, a business relationship is established as soon as possible after the second transaction or activity that requires identity verification, preferably within 30 calendar days after the second transaction or activity.

Policy: The Company creates a business relationship record for all clients who open accounts and records the purpose and intended nature of the business relationship. Ongoing monitoring of business relationships is conducted to:

- Detect transactions that need to be reported as suspicious.
- Maintain client identification and beneficial ownership information, as well as purpose and intended nature records up to date.
- Reassess the client's risk level based on their transactions and activities.
- Determine if the transactions and activities align with the Company's knowledge of the client.
- Maintain records of monitoring measures and obtained information.

Procedures: Once a business relationship is established, the Compliance officer must adhere to the procedures outlined above.

Reasonable measures:

What are reasonable measures? "Reasonable measures" refer to actions the Company takes to fulfill specific AML/CTF obligations. These actions are documented within this program and other internal Company documents. For instance, reasonable measures involve confirming beneficial ownership information, determining whether a client is a politically exposed person (PEP) or high-risk individual or organization (HIO), verifying if the client is acting on the instructions of a third party, and so on, as outlined in the policies and procedures.

When the Company is required to take reasonable measures, the Compliance officer must keep records, even if the reasonable measure is unsuccessful.

It's important to note that reasonable measures should not be confused with mandatory data elements, where information must be obtained before completing a transaction or activity.

Documenting reasonable measures

When the Company takes reasonable measures that prove unsuccessful, it is essential to maintain records of these efforts. Unsuccessful reasonable measures refer to situations where the Company does not obtain a clear response, such as a "yes" or "no," and is unable to reach a conclusive determination. In such cases, the Compliance officer is responsible for documenting specific information:

- The measure(s) taken: Describe the actions or steps that were taken to fulfill AML/CTF obligations, even if they did not lead to a conclusive determination.
- The date on which the measure(s) was taken: Record the date when the reasonable measure(s) was implemented.
- The reason why the measure(s) was unsuccessful: Explain the circumstances or factors that led to the unsuccessful outcome. This may include a client's refusal to provide requested information or other difficulties in obtaining necessary details.

The Company takes into consideration a client's refusal to provide certain information or any inability to obtain specific data as part of the overall assessment of client risk.

Retention: The Compliance officer retains records of all unsuccessful reasonable measures for a minimum of five years from the date they were created. This documentation ensures compliance with AML/CTF regulations and supports the Company's commitment to due diligence and risk assessment.

IV. ASCERTAINING CLIENT IDENTITY

In compliance with the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and associated Regulations, the Company is committed to verifying the identity of individual clients. This process applies to all clients of the Company.

Methods for Individual Identity Verification

The Company employs one of two methods to ascertain the identity of an individual:

1. Single Record Government-Issued Photo Identification Documents Method

- The original, not copies, of the individual's government-issued photo identification must be reviewed in the presence of the client.
- A visual comparison is conducted to confirm the authenticity of the identification document.
- Acceptable government-issued photo identification documents include:
    - Driver's license
    - Passport
    - National identification card
    - Permanent resident card

    - Other similar documents issued by provincial, territorial, or federal governments.
- These documents must display the following elements: a photo of the individual, name, address, date of birth, and an expiry date.
- The document should also include a unique identifying number.
- The name and appearance on the document must match those of the individual being identified.
- Expired identification documents are not acceptable.
- Photo identification documents issued by municipal governments (Canadian or foreign) are not valid for this purpose.

2. Verification Procedures for Government-Issued Photo Identification Documents

- A responsible employee of the Company or the Compliance officer may perform the verification process.
- The authenticity of the government-issued photo identification document is determined in person by inspecting the physical document and its security features (or markers).
- This inspection is conducted in the presence of the individual to ensure that the document is authentic, unaltered, not counterfeit, and current (not expired).
- In cases where the individual is not physically present, technology capable of assessing document authenticity is used.

3. Retention of Verification Records

If the government-issued photo identification document method is utilized, the responsible employee or the Compliance officer is responsible for documenting the following information:

- Individual's name,
- Date of identity verification,
- Type of document used (e.g., driver's license, passport),
- Unique identifying number of the document,
- Jurisdiction (province or state) and country that issued the document, and
- Expiry date of the document (if available on the document).

These records are maintained as part of the Company's compliance with identity verification regulations.

Confirming the existence of entities

The Company is committed to verifying the existence of both corporations and entities other than corporations as required by regulatory obligations. Corporations and entities serve as clients of the Company, and their existence must be confirmed in accordance with specific procedures.

Verification of Corporate Existence

To confirm the existence of a corporation, the Compliance officer relies on the following methods:

- Paper Records: The Compliance officer may refer to paper records or electronic records accessible to the public. These records include:
    - The corporation's certificate of corporate status,
    - Records that must be filed annually under provincial securities legislation,
    - Any other record that attests to the corporation's existence, such as the corporation's published annual report signed by an independent audit firm or a letter/notice of assessment from a municipal, provincial, territorial, or federal government.

Verification of Entity Existence Other Than Corporations

To confirm the existence of an entity other than a corporation, the Compliance officer employs the following methods:

- Paper Records: The Compliance officer may refer to paper records or electronic records accessible to the public. These records include:
    - A partnership agreement
    - Articles of association
    - Any other record that serves as evidence of its existence as a legal entity, such as a trust agreement.

Retention of Confirmation Records

- Records used by the Company to confirm the existence of a corporation or entity can be in paper or electronic format.
- In the case of paper records, the Compliance officer is responsible for keeping a copy of the record.
- For electronic records, the Compliance officer retains the following information:
    - Corporation's registration number (if applicable)
    - Type and source of the record
- Electronic records must originate from a public source. Verbal confirmations (e.g., over the telephone) are not acceptable, and reliance on such methods is prohibited.

Example:

The Company may obtain information about a corporation's name, address, and the names of its directors from public databases like the Corporations Canada database, accessible through Industry Canada's website (http://www.ic.gc.ca). Alternatively, the use of a corporation searching, and registration service is acceptable for confirmation purposes.

Restrictions on the use of personal information

The Company operates in compliance with the Personal Information Protection and Electronic Documents Act (PIPEDA) and, where applicable, similar provincial legislation that safeguards personal information used in Canadian commercial activities. PIPEDA establishes guidelines and principles for the collection, use, and disclosure of personal information by organizations.

Notification of Personal Information Collection

The Company is obligated to inform clients about the collection of their personal information in accordance with PIPEDA and similar provincial laws. Clients are provided with information regarding how their personal information will be utilized and protected.

Exception: Reporting to FINTRAC

There is an exception to the notification requirement when the Company includes clients' personal information in the reports mandated for submission to the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). In such cases, the Company is not obligated to notify clients about the inclusion of their personal information in these reports.

Guidance and Resources

The Office of the Privacy Commissioner of Canada offers further guidance on PIPEDA and its relationship with the Proceeds of Crime (Money Laundering) and Terrorist Financing Act.

They have developed a Question-and-Answer document to assist organizations in understanding their responsibilities under both federal Acts.

For detailed information and guidance, organizations may refer to the resources provided by the Office of the Privacy Commissioner of Canada.

V. RISK BASED APPROACH

Risk assessment is a crucial aspect of anti-money laundering (AML) and counter-terrorist financing (CTF) efforts. It involves evaluating the potential threats and vulnerabilities related to money laundering and terrorist financing that an organization may face. In the context of AML/CTF, risk refers to the likelihood of specific events happening and the extent of damage or loss that may result from those events.

Understanding Risk

- Threats: Threats are individuals, groups, or objects that have the potential to cause harm. In the context of AML/CTF, threats could include criminals, facilitators, their funds, or even terrorist organizations.
- Vulnerabilities: Vulnerabilities are weaknesses or areas within a business that could be exploited by identified threats. In AML/CTF, vulnerabilities might include inadequate internal controls, offering high-risk products or services, and more.
- Impact: Impact refers to the severity of the damage that could occur if the AML/CTF risk materializes. This includes considering the consequences of identified threats and vulnerabilities.

Risk Assessment Purpose

A risk assessment in the context of AML/CTF is an analysis of potential threats and vulnerabilities that could expose a business to money laundering and terrorist financing risks. The complexity of the assessment depends on the size of the business and the specific risk factors associated with its operations.

Types of Risk Assessments

To effectively assess inherent risks, the Compliance officer conducts two types of risk assessments:

1. Business-based Risk Assessment: This assessment considers the Company's products, services, delivery channels, geographical location, and other relevant factors.
2. Relationship-based Risk Assessment: This assessment focuses on the products, services, geographical locations, activities, transaction patterns, and other aspects related to the Company's clients.

These risk assessments should be reviewed at least every two years, as part of program evaluation, or more frequently if there are significant changes in the Company's operations, client base, products, services, or other relevant factors. Resources for Risk Assessment

For more information and guidance on implementing a risk-based approach to AML/CTF, organizations can refer to resources such as FINTRAC's Risk-Based Approach Workbook for MSBs.

How the Company identifies risks

Risk assessments in the context of anti-money laundering (AML) and counter-terrorist financing (CTF) consider various categories to evaluate and mitigate potential risks effectively. These categories are:

1. Products, Services, and Delivery Channels: Different products and services offered by the Company can have varying levels of inherent ML/TF risk. Key attributes of products that contribute to higher risk include features that facilitate high-risk transactions, ease of withdrawals or transfers, and the ability of third parties to conduct transactions using the product.
    a. Delivery Channels: The delivery channel refers to the medium through which products or services are obtained or transactions are conducted. Delivery channels that allow non-face-to-face transactions pose higher risks, as it can be more challenging to verify the identity of clients. This can be exploited to obscure the true identity of a client or beneficial owner.
2. Geographical Risk: The geographical location where the Company conducts its business and where its clients are located can significantly impact overall risk. Factors contributing to higher inherent risk levels include proximity to high-crime areas, client connections to high-risk countries, and the size or nature of the area where the client base resides (e.g., small rural areas vs. large urban areas).
3. Clients and Business Relationships: Understanding the nature of clients and business relationships is crucial. Certain clients or types of business relationships may pose higher inherent risks due to their activities, transaction patterns, or other factors.
4. Other Relevant Factors: Additional factors related to the Company's operational structure, including the number of employees, employee turnover, the number of branches, and the impact of new technology on the industry and the Company's business model, are considered in the risk assessment.
5. Ministerial Directives and Transaction Restrictions: The Company also takes into account any directives or transaction restrictions received from subscribing to

FINTRAC's mailing list communications. These may impact the risk assessment and influence risk mitigation measures.

Additional Resources

For detailed guidance on implementing a risk-based approach to combat money laundering and terrorist financing, organizations can refer to FINTRAC's guidance documents, such as "Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing."

By considering these factors and leveraging available resources, organizations can develop a comprehensive risk assessment that helps identify and address vulnerabilities and threats related to AML and CTF effectively.

How individual clients are risk assessed (initially and ongoing)

Client risk assessment and classification are essential components of an effective anti-money laundering (AML) and counter-terrorist financing (CTF) program. In this context, clients are categorized into three risk groups: Group A (Low Risk), Group B (Medium Risk), and Group C (High Risk). The default risk rating for all clients is low, but this can change based on the presence of specific risk factors. Here's an overview of the risk assessment and classification process:

Default Risk Classification: Low Risk By default, all clients are initially classified as low risk unless specific risk factors are present. These factors can elevate a client's risk rating to medium or high. The key default risk characteristics are:

1. **Politically Exposed Person (PEP)**: Clients who are politically exposed persons are automatically classified as high risk.
2. **Suspicious Transaction or Terrorist Financing Report**: If a suspicious transaction or terrorist financing report has been filed for a client, they are considered high risk.
3. **Identified Terrorist**: Clients identified as terrorists are classified as high risk.
4. **Unable to Obtain Beneficial Ownership Information**: Clients for whom the Company cannot obtain beneficial ownership information are considered high risk.
5. **Client from High-Risk Country**: Clients originating from high-risk countries are automatically classified as high risk.

Potential High-Risk Triggers: Clients may be categorized as high risk if one or more potential high-risk triggers are present. Typically, if three or more triggers are identified, the client should be classified as high risk. However, this may vary based on other factors known about the client's profile, such as the products they hold, tenure with the client, source of funds, etc. Potential high-risk triggers include:

Client Characteristics, Product, Service, Delivery Channel:

- Politically Exposed Person (PEP), Head of International Organization, and Close Associates
- Unknown Source of Funds
- Large Transaction (EFT) Orders to/from High-Risk Foreign Jurisdictions
- Third-Party Involvement Without Justifiable Reason

- High-Risk Occupations (e.g., Cash-Intensive Businesses, Offshore Businesses, Businesses in High-Risk Countries, Online Gambling)
- Unusually Complex Client Business Structure or Transactions
- Non-Face-to-Face Client Identification Without Justifiable Reason

Geography:

- Clients Residing Outside the Local or Normal Client Area
- Clients Residing in Known High-Crime Areas
- Clients with Offshore Business Activities or Connections to High-Risk Countries

Other Suspicious Transaction Indicators:

- Volume, Timing, and Complexity of Transactions Inconsistent with the Client's Activity or Account Purpose,
- Deposits or Transfers of Value Inconsistent with Occupation or Source of Funds,
- Presence of Any Suspicious Transaction Indicators as Outlined in the Program.

Client Risk Assessment Tool: All high-risk client assessments are documented using the Client Risk Assessment Tool located in the program's appendix. Copies of these assessments are retained to demonstrate that clients have been assigned the appropriate risk classification.

By carefully evaluating these risk factors and maintaining accurate records, the Company can effectively assess and mitigate the ML/TF risks associated with its client base.

Risk mitigation

After establishing a business relationship, the Company is required to conduct ongoing monitoring of these relationships and ensure that client information remains up-to-date.

The primary objectives of ongoing monitoring and keeping client information current are as follows:

1. Detect Suspicious Transactions: The Company must use ongoing monitoring to identify any suspicious transactions that require reporting.
2. Reassess Client Risk Levels: Ongoing monitoring allows for the periodic reassessment of the risk associated with a client's transactions and activities.
3. Consistency Checks: The Company must ensure that client transactions and activities align with the information initially obtained about the client, including their risk assessment.
4. Continued Understanding: Ongoing monitoring helps the Company maintain an understanding of the client's activities and transaction patterns.

Ongoing Monitoring for Individuals: During ongoing monitoring for individual clients, the following information should be confirmed or updated as necessary:

- The individual's name
- Address
- Occupation or principal business

Ongoing Monitoring for Entities: During ongoing monitoring for entities, the following information should be confirmed or updated as necessary:

Name of the entity

- Address
- Principal business or occupation
- Names of directors, trustees, etc.
- Beneficial ownership information (information on individuals who ultimately control the entity)

Frequency of Ongoing Monitoring and Updates: The frequency of ongoing monitoring and client information updates depends on the client's risk rating. The following guidelines apply:

Low-Risk and Medium-Risk Clients: Transactions are monitored, reviewed, and assessed as they occur. Client information can be updated during ongoing interactions and communications, such as when conducting new business or subsequent transactions.

High-Risk Clients: For high-risk clients, transactions are monitored, reviewed, and assessed when they occur, and periodic reviews are conducted. Evidence of the periodic review is maintained, and notes are documented in the client file.

Client identification information for high-risk clients is updated regularly, at least annually or more often as necessary. Additional measures may include taking reasonable measures to confirm the information provided by high-risk clients by repeating the identification procedure, either in person or remotely.

By adhering to these ongoing monitoring and client information update procedures, the Company can effectively manage and mitigate risks associated with its client relationships and ensure compliance with anti-money laundering and counter-terrorist financing regulations.

VI. TIMEFRAME FOR KEEPING RECORDS

Record Keeping Requirements

To ensure compliance with record-keeping requirements, the Company is obligated to maintain records in a manner that allows for their provision to FINTRAC within 30 days upon request. Additionally, these records may be subject to judicial orders by law enforcement authorities when conducting investigations related to money laundering or terrorist financing activities.

The Company primarily keeps records in electronic form, with the provision that paper copies can be easily produced if necessary.

The following types of records must be maintained by the Company:

1. Suspicious Transaction Report Records: Records related to filed suspicious transaction reports.
2. Large Cash Transaction Records: Records of large cash transactions, including:
    a. Receipts for $3,000 or more for the issuance of traveler's cheques, money orders, or similar negotiable instruments.
    b. Records for cashing $3,000 or more in money orders.

3. Records for Transactions of $3,000 or More: Records of transactions of $3,000 or more, including:
    a. Receipts for the issuance of traveler's cheques, money orders, or similar negotiable instruments.
    b. Cash transactions of $3,000 or more.
4. Records of Remitting or Transmitting Funds of $1,000 or More: Records related to remitting or transmitting funds of $1,000 or more.
5. Foreign Currency Exchange Records: Records of foreign currency exchange transactions.
6. Internal Memorandum Records: Records of internal memoranda created in the normal course of business.
7. Records About Ongoing Service Agreements: Records pertaining to ongoing service agreements with clients.
8. Reasonable Measures Records: Records related to the reasonable measures taken by the Company.

The Company is required to retain the following records for a minimum of five years from the day the last business transaction was conducted:

- Client Information Records: Including individual client identification information.
- Records to Confirm the Existence of an Entity: Records confirming the existence of legal entities.
- Beneficial Ownership Records: Records related to beneficial ownership information.
- Politically Exposed Foreign Person Determination Records: Records documenting determinations related to politically exposed foreign persons.
- Third-Party Determination Records: Records concerning determinations related to third-party involvement.

Additionally, copies of suspicious transaction reports, large cash transaction reports, and terrorist property reports that the Company has filed must be retained for at least five years following the date of filing.

All other records created by the Company must also be retained for a minimum of five years from the date of their creation.

By adhering to these record-keeping requirements, the Company can fulfill its obligations under anti-money laundering and counter-terrorist financing regulations and provide necessary documentation when requested by FINTRAC or law enforcement agencies.

VII. ONGOING TRAINING PROGRAM

The Company's training program for anti-money laundering and counter-terrorist financing (AML/CTF) compliance is designed to ensure that all individuals within the organization who have specific responsibilities related to clients, client transactions, handling of funds, and compliance regime implementation are adequately trained to understand and fulfill their obligations.

Training Frequency:

- New employees are required to complete AML/CTF training before they begin interacting with clients.
- Ongoing AML/CTF update training is conducted annually or more frequently as needed. Updates are triggered by changes in legislation, the introduction of new products or services, changes in offered services, shifts in geographical focus, or modifications in delivery channels.

Training Method

- Training primarily involves the circulation and review of two key sections of the Compliance program: Section A - Background Information and Section C - Policies and Procedures.
- Optional or additional training may be provided through modules developed by the Compliance officer or external advisors.
- Keeping employees informed about AML/CTF-related matters may involve sharing AML communications and updates from industry associations, relevant news articles, FINTRAC communications, and other pertinent sources.
- The types of training delivered are recorded and tracked using the provided tracking sheet.

Training Facilitation and Tracking:

- The Compliance officer is responsible for facilitating and tracking the completion of all training activities.
- Records of completed training are maintained in the designated section of the Compliance program for reference and verification purposes.

By following this training program, the Company ensures that its employees remain informed and educated about AML/CTF compliance obligations and can effectively carry out their roles in preventing money laundering and terrorist financing activities. Training updates and ongoing education efforts help employees stay current with regulatory changes and industry best practices.

VIII. PROGRAM REVIEW

As part of the Company's commitment to maintaining an effective anti-money laundering and counter-terrorist financing (AML/CTF) compliance program, an annual review of policies and procedures is conducted. The Compliance officer is responsible for overseeing and completing this program review.

Annual Review Frequency:

- The Company's AML/CTF policies and procedures are reviewed on an annual basis as a standard practice.
- However, the review may be conducted more frequently if significant changes or events occur that warrant immediate attention.

Triggers for Early Program Review:

An early program review may be initiated before the one-year period has elapsed if the Company experiences significant changes or events. These changes or

events include:

- Restructuring of the business,
- Legislative or regulatory changes that impact AML/CTF obligations,
- Opening new offices or branches,
- Noticeable demographic shifts in the clientele that may affect risk profiles.

Review Completion and Documentation:

- The Compliance officer is responsible for conducting the program review and ensuring that all policies and procedures are up-to-date and effective.
- The results of the program review, including any identified areas for improvement or updates, are documented.
- The principal of the Company signs the results of the program review within 30 days of its completion.

By conducting an annual review and being prepared to initiate early reviews, when necessary, the Company can ensure that its AML/CTF policies and procedures remain current and aligned with regulatory requirements. This proactive approach helps maintain the program's effectiveness in preventing money laundering and terrorist financing activities.

Compliance Monitoring Procedure

The Company places great importance on ongoing monitoring and transaction analysis as part of its anti-money laundering and counter-terrorist financing (AML/CTF) compliance program. The Compliance officer is responsible for conducting this monitoring and ensuring that it aligns with regulatory requirements.

Purpose of Ongoing Monitoring: The primary purposes of ongoing monitoring are as follows:

1. Transaction Correspondence: To ensure that transactions conducted within the business relationship align with the information previously known about the client, their declared activities, and their risk profile.
2. Detection of Suspicious Activities: To detect any client activities or facts that indicate potential criminal activities, money laundering, or terrorist financing, or relationships with such activities.
3. Risk Assessment Updates: To continually assess changes in the client's activities that may increase the risk associated with the client and the business relationship, necessitating additional or enhanced due diligence measures.
4. Verification of Transaction Purpose: To verify that the purpose and nature of each individual transaction align with the information previously ascertained during the due diligence measures upon establishing the business relationship.

Standard Due Diligence Measures in Ongoing Monitoring: During ongoing monitoring, the Compliance officer conducts the following standard due diligence measures:

- Reviewing transactions conducted during the business relationship to ensure alignment with the Company's knowledge of the client.
- Regularly updating relevant documents, data, or information collected during the initial due diligence process.
- Identifying the source and origin of funds used in a transaction.

Transaction Monitoring Measures: Transaction monitoring measures are divided into two categories:

1. Real-Time Transaction Monitoring: Using IT solutions, such as automatic IT systems (e.g., SumSub, Coinfirm) and internally built IT systems, to screen transactions in real time based on parameters established in the Company's internal risk assessment.
2. Manual Transaction Review: Assigning an employee of the Company the responsibility to manually review transactions.

Review of Transaction Activity: The Compliance Officer conducts a thorough review of transaction activity to ensure compliance. This includes verifying the following:

- Timely and accurate submission of Suspicious Transaction Referrals/Reports to FINTRAC, where appropriate.
- Compliance with information and identification requirements and adherence to identification policies.
- Completion of Transaction Forms and receipts accurately and matching the printed money transfer receipts.
- Compliance with all record-keeping requirements.
- Completion of refresher training for existing employees and successful completion of compliance training by new employees.
- Proper use of separate user IDs and passwords for conducting the Company's money transfer transactions.
- Monitoring daily activity reports, reconciliation of money transfers, and identification and reporting of suspicious activity, where applicable.

Documentation and Evidence: All monitoring activities are thoroughly documented, and evidence of the review is retained for at least five years. The Company may use the Monitoring Log to record monitoring activities.

Ongoing monitoring and transaction analysis are essential components of the Company's commitment to AML/CTF compliance and the prevention of money laundering and terrorist financing activities.

IX. SUSPICIOUS TRANSACTION REPORT PROCEDURE

The Company takes its responsibility for reporting suspicious transactions and maintaining records seriously to combat money laundering and terrorist financing. Here are the key guidelines and considerations:

Reporting Suspicious Transactions:

1. Reasonable Basis for Suspicion: A Suspicious Transaction Report (STR) must be submitted to FINTRAC for any completed or attempted transaction when there is a reasonable basis to suspect that it is related to money laundering or terrorist financing. This includes possible attempts to launder money, structuring transactions to avoid reporting or record-keeping requirements, and terrorist financing activities.
2. Information Gathering: Employees must take reasonable measures to obtain as much information as possible for completing the STR, all while avoiding alerting the client to the report being prepared. If an employee believes that asking additional questions

would tip off the client, they should refrain from doing so. Under no circumstances should an employee inform a client that an STR is being submitted.

3. Review by Compliance Officer: All STRs must be reviewed for completeness and accuracy by the Compliance officer before submission to FINTRAC. The Compliance officer is responsible for ensuring that the report is in compliance with regulatory requirements.
4. Timely Submission: The Compliance officer is responsible for filing the STR directly with FINTRAC electronically within 30 days of identifying the suspicious activity. They also serve as the contact person for FINTRAC if any questions arise regarding the reports.
5. Record Retention: Copies of Suspicious Transaction Referrals/Reports and evidence of submission to FINTRAC, along with all supporting information, must be retained for a period of 5 years.

Indicators for Suspicion: The Company considers a range of indicators to determine whether an STR should be filed. These indicators include but are not limited to:

- A client appearing to live beyond their means.
- Inconsistent business activity with industry averages or financial ratios.
- Frequent changes in bookkeepers or accountants.
- Inability to provide company records.
- Continuous business losses without reasonable explanation.
- Shareholder loans inconsistent with business activity.
- Unusual large payments to subsidiaries or similarly controlled companies.
- Transactions with organizations in countries with inadequate money laundering regulation
- Statements made by the client about involvement in criminal activity.
- Uncommon curiosity about internal systems, controls, or policies.
- Attempts to convince an employee not to complete required documentation.
- Providing false, counterfeit, altered, or inaccurate identification.
- Refusal to produce personal identification documents.
- Attempts to establish identity using false names.
- Transaction details that lack important information or are impossible to verify.
- Brand-new identification documents.
- Transactions lacking economic purpose or consistency.
- Significant activity on previously inactive or dormant accounts.
- Transactions involving countries known for illicit drug production or money laundering.
- Multimillion-dollar deposits from "confidential sources."
- Transactions involving offshore "shell" companies with names similar to legitimate institutions.

Record Keeping: The Company is committed to maintaining proper records for audit trails money laundering investigations. Records include client identification and transaction details, clearly showing the type of identification evidence obtained from the client. Copies of this evidence kept as part of the client's record.

Transaction records include all information necessary for transactions, including payer, payee beneficiaries, amounts, source of funds, form of money, identity of the person conducting transaction, and instructions for the transaction.

These records are securely maintained for a minimum of five years after the last relevant transaction. If there is an ongoing investigation at the end of the five-year period, records are retained until the authorities close the case. The objective is to allow law enforcement authorities to access relevant information without undue delay.