## Trackon Canada Private Ltd

# Anti-Money Laundering & Counter Terrorist Financing Policy

**Version Number:** 1.1

**Last Updated:** July 2022

**Next Update:** January 2023

**Approved By:** Jaspreet Singh, Compliance Officer

**Senior Officer Approval for Program:** Jaspreet Singh, Director

# Table of Contents

# 1 Policy Statement

## 1.1 Our Commitment

Trackon Canada Private Ltd (Trackon) is committed to preventing, detecting and deterring money laundering and terrorist financing and has a zero-tolerance policy regarding money laundering and terrorist financing. To that end, it is the responsibility of every employee (including contract and part-time employees) to comply with this program and all related Canadian legislation.

While Trackon is committed to having an effective compliance program in place, if we become aware of a non-compliance event, a voluntary disclosure of their non-compliance will be made FINTRAC.

Our procedures for implementing this policy are described in separate documents, as is our Risk Assessment. To be read in addition to this policy, specific procedures have been designed for:

- Compliance Staff; and
- All Staff.

Reading of this policy and our all staff procedure is currently required for all new hires. An attestation confirming that the policy and procedure are read and understood is kept as a training record. There are also separate training materials for staff, which include quizzes designed to test the effectiveness of training.

## 1.2 Compliance Program

Under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and its regulations (Regulations), we are required to have an anti-money laundering (AML) and counter terrorist financing (CTF) program that consists of these five elements:

1) **Written policies and procedures**: these list our responsibilities under the law, and what we are doing to meet them;
2) **A documented Risk Assessment**: a document that describes and assesses the risk that our business could be used to launder money or finance terrorism;
3) **The appointment of a Compliance Officer**: the person who is ultimately responsible to develop and maintain our AML and CTF compliance program;
4) **AML Compliance Effectiveness Reviews**: testing and reporting completed either annually or every two years that assesses how well our compliance program is working; and

5) **Training**: conducted at least annually to ensure that everyone understands his or her roles and responsibilities.

These five elements are discussed in detail later in this policy.

### 1.3 Operational Compliance

In addition to our documented program that consists of the five elements, we are required to operate in a compliant manner. This includes:

- Collecting and recording customer identification information;
- Know your customer (KYC) information;
- Transaction Monitoring and customer risk scoring;
- Reporting certain types of transactions to regulators and government agencies;
- Maintaining appropriate registration and licensing; and
- Keeping records.

The actions described in our procedures for this purpose are required (not optional) in all cases. Any activity that is offside with our AML and CTF procedures should be brought to the attention of the Compliance Officer immediately.

## 2 AML & CTF Basics

Money laundering is the process of taking money obtained by committing a crime and disguising the source to make it appear legitimate. Under the Criminal Code of Canada, it is illegal to launder money or to knowingly assist in laundering money. Under the PCMLTFA and Regulations, as well as legislation applicable in other jurisdictions in which we operate, we must take steps to be sure that our business is not used to launder money and if we suspect that money laundering may be taking place, we must report it.

Terrorist financing is the process of moving funds in order to pay for terrorist activities. Unlike money laundering, the source of the funds is not always criminal, but the intended use of the funds is criminal. Under the Criminal Code of Canada, it is illegal to knowingly assist in the financing of terrorism, including the possession of terrorist funds or property. If we know or suspect that we have terrorist property in our possession, it must be reported immediately.

### 2.1 How Money Laundering & Terrorist Financing Work

Money laundering is described as having three phases by the Financial Action Task Force ('FATF'). These are 'Placement', 'Layering' and 'Integration.'

Terrorist financing, as opposed to money laundering, can occur with legitimate funds. Meaning; funds which are not the proceeds of crime. Legitimate funds

can be transferred and used by those who would commit terrorist activities. In this, it can be said that terrorist financing most often acts in the 'Layering' and 'Integration' phases described by the FATF. However, rather than investing in luxury items, the

funds are used for the commission or support of terrorist activities and/or organizations. These phases are described in detail below:

**Placement**: In the initial - or placement - stage of money laundering, the launderer introduces illegal profits into the financial system. This might be done by breaking up large amounts of cash into less conspicuous smaller sums that are then deposited directly into a bank account, or by purchasing a series of monetary instruments (cheques, money orders, etc.) that are then collected and deposited into accounts at another location.

**Layering**: After the funds have entered the financial system, the second – or layering – stage takes place. In this phase, the launderer engages in a series of conversions or movements of the funds to distance them from their source. The funds might be channeled through the purchase and sales of investment instruments, or the launderer might simply wire the funds through a series of accounts at various banks across the globe. This use of widely scattered accounts for laundering is especially prevalent in those jurisdictions that do not co-operate in anti-money laundering investigations. In some instances, the launderer might disguise the transfers as payments for goods or services, thus giving them a legitimate appearance.

**Integration**: Having successfully processed funds through the first two phases, the launderer then moves them to the third stage – integration – in which the funds re-enter the legitimate economy. The launderer might choose to invest the funds into real estate, luxury assets, or business ventures.

# 3 Canadian Regulatory Background & Requirements

## 3.1 Money Services Businesses

Money Services Businesses (MSBs) are considered reporting entities under the law in Canada. This means that we must comply with certain requirements and answer to our regulator. Our regulators, federally, define MSB activity in the following way:

"You are considered to be a money services business (MSB) if any of the following apply:

You are engaged in the business of providing at least one money services business (MSB) service:

- **Foreign exchange dealing** - conducting transactions where one type of money or currency (like US dollars, Canadian dollars, Euros and so on) is exchanged for another.
- 
- 

- **Money transfer service** - transferring funds from one individual or entity to another using an electronic funds transfer network or any other transfer method such as hawala, hundi, fei ch'ien, and chiti.
- **Cashing or selling money orders, traveller's cheques or anything similar** - this does **not** include cashing cheques made out to a particular individual or entity.
- **Dealing in Virtual Currency** means 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.[1] ”

In Québec, the additional activities that are included in the MSB Act are:

- **Cheque cashing** (including the types of activity that are excluded under the last point of the federal definition); and
- The **operation of automated teller machines**, including the leasing of a commercial space intended as a location for an automated teller machine if the lessor is responsible for keeping the machine supplied with cash.

## 3.2 FINTRAC

The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)[2] is the agency that regulates our industry to ensure that we are meeting our obligations. They have the power to review our documentation and to levy significant penalties if we are not compliant. Individuals that deliberately attempt to circumvent the law may also be charged criminally in addition to monetary penalties.

FINTRAC is also Canada’s financial intelligence unit (FIU). The agency receives reports from reporting entities, like us, about transactions and analyses the data that they receive. This data is used to assist law enforcement investigations into crimes related to money laundering and terrorist financing. It is vital to this process that the information that we submit to FINTRAC is accurate, on time and as complete as possible.

FINTRAC also requires MSBs to maintain an up to date MSB registration. This includes keeping information about our business activities, key persons and banking services relationships up to date. If there are any changes, we need to

[1] https://www.fintrac-canafe.gc.ca/msb-esm/msb-eng
[2] http://www.fintrac.gc.ca/

inform FINTRAC within 30 days. If our business stops operating in Canada, or no longer offers MSB services, we must cancel our MSB registration.

## 3.3 AMF[3]

The Autorité des marchés financiers (AMF)[4] is the body mandated by the government of Québec to regulate the province's financial markets and provide assistance to consumers of financial products and services.

The AMF enforces Québec's Money-Services Business Act (MSB Act) and its enacted regulations. The MSB Act defines MSBs more broadly than the Canadian federal definition and includes provincial licensing and registration requirements.

## 3.4 Provincial Securities Regulators[5]

Provincial bodies, including the Ontario Securities Commission (OSC), regulate securities dealers and derivatives markets. These bodies require reporting from MSBs that conduct foreign exchange transactions that meet the following criteria[6]:

- Settle over a period longer than 2 business days; and/or
- Contain a rollover provision; and/or
- Are conducted for the purpose of financial speculations (i.e. that are not conducted with an expectation of delivery of the physical currency).

These transactions are required to be reported to a local Trade Repository (TR) along with the Legal Entity Identifiers (LEIs) of all entities party to the transaction, the Unique Product Identifier (UPI) describing the type of product sold, and the Unique Transaction Identifier (UTI) attached to the particular transaction reported.

## 3.5 Regulator Examinations & Compliance Assessment Reports

FINTRAC is responsible for ensuring that we (as a reporting entity) are meeting our obligations. To do this, they will periodically request information. We may receive these requests by email, phone or in writing. All requests should be forwarded to the Compliance Officer for handling immediately.

---

[3] Trackon does not currently carry out any business in the province of Quebec. This has been included for educational purposes, or in case our business model changes.
[4] https://www.lautorite.qc.ca/en/index.html
[5] Trackon does not currently conduct transactions that fall under securities requirements. Should we consider these types of activities at any time, the compliance program will be updated to include all relevant requirements before any qualifying products and/or services are offered.
[6] Some exemptions apply. The complete criteria may vary from province to province, despite the existence of standardized guidance at the federal level.

Most requests will be time sensitive. This means that we only have a certain amount of time to reply by law. For most information requests, this is 30 calendar days. If we do not respond to these requests or respond late, we may be subject to penalties.

### 3.6 Ministerial Directives

From time to time, the Minister of Finance will issue additional directives for AML reporting entities. The Compliance Officer will ensure that our policies, procedures and Risk Assessment are updated accordingly. This may include the implementation of new processes in order to comply with directives, and to test the effectiveness of compliance measures.

Currently, there are two ministerial directives pertaining to transactions that originate from or are destined to North Korea (also known as the Democratic People's Republic of Korea, or DPRK) and to the Islamic Republic of Iran (Iran). We do not serve DPRK, Iran or other regions noted in FINTRAC's operational briefs on ministerial directive obligations. As such, no additional mediation steps have been taken in this case.[7]

## 4 Roles & Responsibilities

Everyone has a responsibility to ensure that our AML and CTF compliance program runs smoothly.

- **Senior Management:**
  - Overseeing the AML and CTF Program on a high level;
  - Receiving regular (at least annual) status reports on the AML and CTF Program;
  - Being accessible to the Compliance Officer as needed where AML or CTF related issues arise;
  - Ensuring that the Compliance Officer has the resources to run an effective AML and CTF program;
  - Ensuring that the Compliance Officer is adequately qualified to manage the AML and CTF Program (understand Canadian AML and CTF requirements and the business model); and
  - Signing off on the results of completed AML Compliance Effectiveness Reviews (within 30 days of the issue of the report).

- **Compliance Officer:**
  - Developing and maintaining the AML and CTF Compliance Program and Risk Assessment, which includes regularly reviewing and

[7] http://www.fintrac-canafe.gc.ca/obligations/dir-dprk-eng.asp and https://www.fintrac-canafe.gc.ca/obligations/dir-iri-eng

updating these documents and maintaining a record of all updates;
    - Ensuring that all employees, agents (if applicable) and other relevant parties receive appropriate AML and CTF training at least annually;

    - Reporting to Senior Management and the Board of Directors (if applicable) on the status of the AML Program, including any AML Compliance Effectiveness Reviews (within 30 days of the issue of the report) and regulatory examinations;
    - Overseeing AML Compliance Effectiveness Reviews and ensuring that the reviewer has sufficient knowledge of Canadian AML and CTF requirements and our business to conduct the review;
    - Maintaining complete and accurate records;
    - Maintaining up to date registration with FINTRAC;
    - Maintaining up to date licensing with the AMF;
    - Corresponding with FINTRAC and the AMF;
    - Maintaining up to date knowledge of Canadian AML and CTF requirements as they apply to our business model; and
    - Obtaining appropriate training, including continuing education, in order to develop and maintain knowledge of AML and CTF compliance requirements and industry best practices.

- **All Employees:**
    - Complying with the requirements set out in the AML and CTF program;
    - Reporting certain types of transactions to the Compliance Officer;
    - Keeping up to date and accurate customer records;
    - Obtaining customer identification when required;
    - Completing AML and CTF training when required (at least annually); and
    - Being vigilant in identifying potential money laundering or terrorist financing activities.

The steps that Trackon will take to meet these responsibilities are described in region-specific procedural documents.

If you aren't sure what to do to meet these responsibilities, speak with your manager or the Compliance Officer.

# 5 Canadian AML Compliance Program Components

As an MSB operating in Canada, we are required to have in place a Compliance Program made up the elements described below. Our Canadian AML/CTF program has been designed to conform to the elements required under Canadian legislation.

## 5.1 Policy & Procedures

Our policy statements describe what we are required to do, while our procedures describe how we will meet these obligations. Our procedures should be detailed

enough that someone could read and follow the steps described. This program document includes both policies and procedures.

All staff are required to read this Policy document and our Procedures for All Staff document.

All staff with compliance related duties are required to read the Policy, Risk Assessment, Procedures for All Staff, and Procedures for Compliance Staff.

## 5.2 Risk Assessment

Our company's Risk Assessment is summarized in a separate document. It describes in detail:

- The risk that our activities could make us vulnerable to terrorist financing or money laundering; and
- The controls that we have in place to prevent, detect, and deter money laundering and terrorist financing[8].

The Risk Assessment is reviewed and updated by the Compliance Officer at least every two years, and more often where there are changes to Canadian legislation, the products and services that we offer, or our controls.

## 5.3 Compliance Officer

Senior Management must approve the Compliance Officer's appointment. While the Compliance Officer may or may not be a member of the Senior Management team, the Compliance Officer must always have access to management and the authority to carry out their duties. It is also vital that the Compliance Officer be educated about the ongoing compliance requirements that apply to our business. This is accomplished by attending education and training sessions, checking FINTRAC's website on a regular basis, and signing up for FINTRAC's mailing list[9]. The current Compliance Officer is Jaspreet Singh appointed October of 2020.

The Compliance Officer must be accessible to all staff members who may have questions about anti-money laundering, counter terrorist financing or compliance related processes. In the case of an extended absence, a designate should be in place (and the duties of the designate should be clearly communicated to other staff members in case questions arise). For larger

[8] Our controls are described at a high level in Risk Assessment documentation.
[9] http://www.fintrac.gc.ca/contact-contactez/list-liste-eng.asp

organizations, an assistant Compliance Officer should be appointed to act in the Compliance Officer's absence.

## 5.4 AML Compliance Effectiveness Review

An AML Compliance Effectiveness Review is like an audit that tests our company's AML and CTF program. The review tests two elements: our program documentation

(what we say we're doing) and our operations (what we've actually done during a specific period of time). These reviews must be completed at least once every two years. The results of the review are shared with Senior Management and must be signed off within 30 days of the date that the final report is issued.

The information gathered for these reports is very specific. If you receive a request related to a review, please check to be certain that you are able to provide all of the information that was requested. The review process may also include interviews with staff. If you are interviewed, it is fine to have a copy of our AML and CTF compliance program and other documentation with you, and to refer to these during the interview.

The Compliance Officer will work to correct any issues that are noted in the report. This may include:

- Updating the AML Compliance Program;
- Creating new controls;
- Updating processes;
- Updating customer records; and
- Providing additional staff training on specific topics.

The results of AML Compliance Effectiveness Reviews may also be shared with potential business partners, financial service providers, and FINTRAC. It is a best practice for the Compliance Officer to keep a record of the updates that have been made based on the AML Compliance Effectiveness Review. This can be done in a simple spreadsheet.

## 5.5 Training

Everyone that deals with customers, customer funds or transactions must receive AML and CTF training at least annually. This includes part-time, seasonal and contract employees.

New hires must receive AML and CTF training within their first 30 days on the job, as well as specific role-based training, which includes AML and CTF components, prior to dealing with customers or customer funds independently.

Anyone that is on a leave of absence that causes them to miss regularly scheduled training will complete training within 30 days of their return to work.

AML and CTF Compliance Training will cover (at minimum) these elements:

- What is money laundering?
- What is terrorist financing?
- Who is FINTRAC?
- What is an MSB?
- What are our responsibilities under Canadian law?
    - AML Compliance Program
        - Compliance Officer
        - AML Program
        - Risk Assessment
        - AML Compliance Effectiveness Review
        - Training
    - AML Compliance Operations
        - Reporting
        - Recordkeeping
        - Identifying Customers
        - Customer Risk
        - Transaction Monitoring
- Who is our Compliance Officer?
- What do I do if I believe that money laundering or terrorist financing is taking place?
- What indicators should I look for in our transactions and customer behaviours?
- Compliance Penalties

The completion of this training is mandatory (non-negotiable) and training must be completed within the time frames communicated by the Compliance Officer or their designate. Failure to complete training could expose the company to regulatory penalties. For this reason, it is vital that you contact the Compliance Officer immediately if you believe that you may not be able to compete your scheduled training session. Reading of this policy and our all staff procedure is currently required for all new hires. An attestation confirming that the policy and procedure are read and understood is kept as a training record.

# 6 Operational Compliance

Operational Compliance is everything that we do in order to meet our obligations. This includes identifying our customers in some cases, reporting certain types of transactions to FINTRAC and other agencies, and keeping records.

## 6.1 FINTRAC MSB Registration

We must register as an MSB with FINTRAC before conducting any transactions. The registration must be maintained, and we must:

- Keep registration information up to date;
- Respond to requests for, or to clarify, information in the prescribed form and manner, within 30 days;
- Renew our registration before it expires; and
- Let FINTRAC know if we stop offering MSB services to the public.

All communication with FINTRAC will be handled by the Compliance Officer or a trained delegate.

## 6.2 Reporting

Trackon must report certain transactions to FINTRAC and other agencies, as necessary. FINTRAC provides secure online forms to report these transactions. Reporting to FINTRAC should always be completed by the Compliance Officer or a designate (a person that has been trained to submit reports in the Compliance Officer's absence).

All other employees should use the internal forms included in this program to submit reports to the Compliance Officer. If you aren't sure whether or not you will need to submit a report, speak with the Compliance Officer for clarification. If it is not possible to speak with the Compliance Officer at that time, err on the side of caution by collecting the information that you need to fill out the form(s) and submit the report(s). This includes collecting the customer's identification information.

All reports have specific timelines in which they must be submitted to FINTRAC. All internal reports should be submitted to the Compliance Officer on the same day that the incident or transaction takes place.

Reports submitted by staff members are reviewed as soon as possible. Where there are issues with the reports, such as missing or incomplete information, the Compliance Officer will conduct follow up coaching sessions. The Compliance Officer will also work with the staff member to contact the customer (where possible) in order to obtain any missing or incomplete information.

The Compliance Officer will report all prescribed transactions within the required timeframes via F2R (where possible) or on paper (where electronic submissions are not possible).

| **Report Type** | **Timing** | **Reported To** | **How is it submitted?** |
|---|---|---|---|
| Electronic Funds Transfer Report (EFTR) | 5 working days from the transaction date | FINTRAC | Electronically via F2R |

| Report Type | Timing | Reported To | How is it submitted? |
|---|---|---|---|
| Large Cash Transaction Report (LCTR)[10] | 15 calendar days from the transaction date | FINTRAC | Electronically via F2R |
| Large Virtual Currency Transaction Report (LVCTR)[11] | 5 working days after the day on which the person or entity transfers or receives the amount | FINTRAC | Electronically via F2R |
| Suspicious Transaction Report (STR) | As soon as practicable after completing the measures that enabled a determination that there are reasonable grounds to suspect that the activity could be related to money laundering and/or terrorist financing. | FINTRAC | Electronically via F2R |
| Attempted Suspicious Transaction Report (ASTR) | As soon as practicable after completing the measures that enabled a determination that there are reasonable grounds to suspect that the activity could be related to money laundering and/or terrorist financing. | FINTRAC | Electronically via F2R |
| Terrorist Property Report (TPR) | Immediately | FINTRAC, RCMP, CSIS | On paper (via fax) |

### 6.2.1 Electronic Funds Transfers (EFTs)

Financial entities, money services businesses and casinos have to report incoming and outgoing international EFTs of CAD 10,000 or more in a single transaction. These include the transmission of instructions for a transfer of funds made at the request of a customer through any electronic, magnetic or optical device, telephone instrument or computer.

EFTs of CAD 10,000 or more, including two or more transactions of less than CAD 10,000 that total more than CAD 10,000 conducted by or on behalf of the same person or entity in the same 24-hour period, are detected by our trade software. The static 24-hour period we have chosen for calculating this is between 12:00am – 11:59pm. An alert is generated, and the Compliance Officer resolves the alert and completes FINTRAC reporting.

[10] At the time this document was last updated, Trackon did not accept cash from our customers. This has been included for educational purposes only.

[11] At the time this document was last updated, Trackon did not accept virtual currency from our customers nor conduct transactions in virtual currency. This has been included for educational purposes only.

Electronic funds transfers must be reported to FINTRAC within five (5) business days of the date on which the transaction takes place.

### 6.2.2 Large Cash Transactions[12]

Large Cash Transaction Reports (LCTRs) are submitted when a customer conducts transactions, in cash, valued at CAD 10,000 or more (in any currency or combination of currencies) in the same 24-hour period. This may be in a single transaction or several separate transactions.

When an LCTR is required, the customer's identification must be verified, and identification information must be recorded.

A third party determination must also be made. This means that we must ask the customer if they are completing the transaction(s) on their own behalf or someone else's. If the transactions are being completed to the benefit of someone else, we must obtain information about that person and their relationship to the person conducting the transaction.

Unlike STRs and ASTRs, it is ok to let the customer know that we must fill out an LCTR form and to fill out this form with the customer present.

LCTRs must be submitted to FINTRAC within 15 calendar days.

### 6.2.3 Large Virtual Currency Transactions[13]

As of June 1, 2021, Large Virtual Currency Transaction Reports will have to be submitted to FINTRAC when a customer conducts transactions, in virtual currency, valued at CAD 10,000 or more in the same 24-hour period. This may be in a single transaction or several separate transactions.

Similar to an LCTR, we are required to verify a customer's identification. We must also conduct a third party determination. This means that we must ask the customer if they are completing the transaction(s) on their own behalf or someone else's. If the transactions are being completed to the benefit of someone else, we must obtain information about that person and their relationship to the person conducting the transaction.

Unlike STRs and ASTRs, it is ok to let the customer know that we must fill out an LVCTR form and it is ok to fill out this form with the customer present.

---

[12] At the time this document was last updated, Trackon did not accept cash from our customers. This has been included for educational purposes only.

[13] Effective: June 1, 2021. At the time this document was last updated, Trackon did not accept virtual currency from our customers nor conduct transactions in virtual currency. This has been included for educational purposes only.

Large Virtual Currency Transaction Reports must be submitted to FINTRAC within 5 working days after the day on which the person or entity transfers or receives the amount.

### 6.2.4 Suspicious Transactions & Attempted Suspicious Transactions

Suspicious Transaction Reports (STRs) and Attempted Suspicious Transaction Reports (ASTRs) are submitted to FINTRAC where there are 'reasonable grounds' to suspect that an activity is related to money laundering or terrorist financing. These reports must be submitted whether or not the transaction or activity is completed. ASTRs are used for transactions that are not completed (whether the transaction is declined by Trackon or cancelled by the customer). These reports must be submitted to FINTRAC as soon as practicable after completing the measures that enabled a determination that there are reasonable grounds to suspect that the activity could be related to money laundering and/or terrorist financing.

It is important not to let the customer know that we are suspicious. It is against the law to deliberately "tip off" a customer about a potential investigation. We are, however, protected under Canadian law from any action when we submit a report "in good faith." In most cases, even when a case goes to court, the customer will not know that this report has been filed.

It is important to try to identify customers that conduct or attempt suspicious transactions. The customer may ask us why we need their identification information. In such cases, let the customer know that it is company policy to collect this information. If this information is not used for additional marketing activities, let the customer know that as well (often customers are more concerned about privacy and security issues, and reassuring them may be helpful).

### 6.2.5 Terrorist Property

Terrorist Property Reports (TPRs) are completed if we believe that Trackon may be in possession of funds or property that belong to a terrorist (either an individual or an organization).

These reports should be escalated to the Compliance Officer immediately. In some cases, property or funds must be frozen. Like STRs and ASTRs, the contents of these reports (or the fact that we are filing a report) should not be disclosed to the customer.

These reports are submitted immediately to FINTRAC, as well as to the Canadian Security Intelligence Service (CSIS) and the Royal Canadian Mounted Police (RCMP).

## 6.3 Responding to Law Enforcement Requests

If Trackon receives a request from law enforcement, the Compliance Officer must be notified immediately. Trackon will comply with law enforcement requests, such as court orders, warrants, and subpoenas that are received, so long as there is no breach of privacy legislation.

## 6.4 Record Keeping[14]

In order to pass a FINTRAC review or an AML Compliance Effectiveness Review, we must be able to prove that we've met our obligations. This means that there are things that will need to be recorded (either on paper or electronically). These records must be kept for at least five years (but may be kept for longer) and be in a format that can be retrieved and sorted easily.

Generally, when FINTRAC makes a request, the information must be delivered to them within 30 calendar days. Depending on the type of information requested and the way that the information is stored, the Compliance Officer or a designate may need time to format and organize the information. For this reason, the following information must be stored in a format that can be retrieved and delivered to the Compliance Officer quickly:

- Certain records created in the normal course of business:
    - Records for transactions of CAD 3,000 or more (if you receive CAD 3,000 or more for the issuance of traveller's cheques, money orders or other similar negotiable instruments, or if you cash CAD 3,000 or more in money orders, the name of the issuer must be on the money order);
    - Records for transactions of CAD 3,000, currency exchange transaction tickets including currency used and method of payment;
    - Records of remitting or transmitting funds of CAD 1,000 or more including currency used and method of payment;
    - Records of virtual currency transactions of CAD 1,000 or more;
- Complete customer identification information;
- Complete records for Politically Exposed Persons (PEPs) and Heads of International Organizations (HIOs);
- Large cash transaction records (including a record of the third party determination);
- Large Virtual Currency Transaction records (including a record of the third-party determination)[15];

[14] It is understood that based on our current business model, some of the record keeping items do not apply. They have been provided in the event our business model changes and for educational purposes.

[15] Effective: June 1, 2021.

- Internal unusual transaction forms (whether or not they were reported to FINTRAC by the Compliance Officer) and a record of the Compliance Officer's investigation process, including a rational that describes why the transaction or attempted transaction was or was not reported to FINTRAC;
- A record of the content, date and completion/attendance of any AML or CTF related training sessions, including internal staff training sessions;

- AML Compliance Effectiveness Review reports, including a record of Senior Management sign-off on the final report;
- All FINTRAC correspondence and reporting;
- All AML and CTF program documents, including policies, procedures and our Risk Assessment;
- All customer and business relationship risk ranking documentation;
- All records of enhanced due diligence for higher risk customers and business relationships;
- All records of transaction monitoring for higher risk customers and business relationships;
- Records related to business relationships;
- Copies of signed agreements with our agents and/or service providers; and
- Any "reasonable measures" that have been taken, the date the measures were taken, as well as an explanation where these have not been successful.

## 6.5 Customer Identification

In some cases, we need to identify our customers and record specific information about the customer. This includes:

- Any customer with whom we have an ongoing service agreement;
- Large cash transactions (valued at CAD 10,000 or more in a single transaction or multiple transactions within 24 hours);
- International electronic funds transfers valued at CAD 1,000 or more;
- Virtual currency exchange transactions value at CAD 1,000 or more[16];
- Foreign exchange transactions valued at CAD 3,000 or more; and
- Cashing monetary instruments valued at CAD 3,000 or more.

And, without letting the customer know that we may have suspicions about the nature of their activities, in instances of:

- Suspected money laundering or terrorist financing activity; and
- Terrorist property.

Where it is not possible to identify a customer in the case of suspicious activity or suspected terrorist property, we must keep a record of the reasonable

[16] Effective: June 1, 2021.

measures that we have taken to do so, the date the reasonable measures were taken, as well as the reason that those measure were not successful.

### 6.5.1 Government-Issued Photo Identification Methods for Individuals

Trackon can confirm the identity of a customer, that is an individual, by relying on an identity document where it is "valid, authentic and current." Meaning, we can

confirm identification using acceptable documents, presented in an electronic format, so long as it can be authenticated. The identification document must:

- Be issued by a provincial, territorial or federal government in Canada or an equivalent foreign government;
- Be valid (not expired);
- Bear a unique identifier number (such as a driver's license number);
- Bear the name of the individual being identified; and
- Bear a photo of the individual being identified.

We must also collect and record the following information:

- The customer's full name (no initials, short forms or abbreviations);
- The customer's occupation (this should be as detailed as possible and be full form, without abbreviations or acronyms);
- The nature and purpose of our business relationship with the customer (if applicable);
- The customer's date of birth (if this appears on the identification document, the date of birth that we record must match the document);
- The customer's full home address (post boxes, office addresses and general delivery addresses are not acceptable for this purpose; if the customer wishes to provide a separate mailing address we can collect this as well, but we must always record the full home address);
- The type of document used to identify the customer;
- The place that the identification was issued (this should be a province, territory, or state and a country, not a city);
- The unique identification number (such as the driver's license number);
- The expiry date of the identification provided (if the document has an expiry date; if it does not, please make a note to say that there was no expiry date on the document); and
- The date on which we verified the document.

If a customer has been identified previously and the information in our records is up to date (the identification document used has not expired), and we recognize the customer (either by seeing them or hearing their voice), then we do not need to request identification to complete a transaction.

Types of acceptable documents include but are not limited to:

- Passport;
- Driver's License;
- Permanent resident card.

Further details of identification documentation can be found in our All Staff Procedures document.

### 6.5.2 Other Identification Methods for Individuals

We can also use the below methods to identify our customers.

#### 6.5.2.1 Single Process Method

We may confirm the identity of a customer by referring to their Canadian credit file (Equifax or TransUnion), provided it has been in existence for at least three years, by doing a credit header match. Meaning, we do not have to collect a credit assessment (hard hit) but simply a credit header match (soft hit). This must be completed at the time we are confirming our customer's identity. To be acceptable, the credit file details must match the name, date of birth and address provided by the customer. If any of the information does not match, we will need to use the dual process method to confirm the customer's identification.

When using this method to confirm our customer's identity, we must record the following information:

- The customer's name;
- The name of the Canadian credit bureau holding the credit file (Equifax or Transunion);
- The reference number of the credit file; and
- The date we consulted the credit file.

#### 6.5.2.2 Dual Process Method

Where the single process method provides information that does not match what the customer has provided us, we must use the dual process method. This involves referring to information from reliable and independent sources, and must be valid and the most recent. In order to qualify as reliable, the sources should be well known and considered reputable. Independent means the sources providing the information cannot be us (as the reporting entity) or the customer, and the documents referred to cannot be from the same source. For example, reliable and independent sources can be the federal, provincial, territorial and municipal levels of government, crown corporations, financial entities or utility providers.

Under the dual process method, we can refer to any two of the following options:

- Documents or information from a reliable source that contain the customer's name and date of birth;
- Documents or information from a reliable source that contain the customer's name and address; or
- Documents or information that contain the customer's name and confirms that they have a deposit, credit card or other loan account with a financial entity.

### 6.5.3 Organizations

When our customers who are organizations conduct transactions that require identification, we must collect and record the following information. Some of the information that we collect will be different depending on the type of organization being identified. For all organization types, we must collect:

- Their full legal name (no initials, short forms or abbreviations);
- The organization's structure (incorporated company, trust, partnership, etc.);
- The organization's "principal business" (this should be as detailed as possible and be full form, without abbreviations or acronyms);
- The organization's physical address (post office boxes and general delivery addresses are not acceptable for this purpose; if the customer wishes to provide a separate mailing address, we can collect this as well, but we must always record the full physical address);
- The organization's telephone number; and
- Information about the organization's authorized representatives, Directors and Beneficial Owners.

## 6.6 Business Relationships

We have a business relationship with any customers that are individuals that have conducted two or more transactions that require identification, or any customers that are entities with whom we have entered into an ongoing service agreement. For these customers, we also need to keep a record of the nature of their business relationship with us. Although this will generally seem self-evident (for example, sending money to support family), it is still something that needs to be recorded.

As of June 1, 2021, we will also have to conduct a Politically Exposed Person (PEP) or Head of an International Organization (HIO) determination when we enter into a business relationship with a customer.

We must also monitor business relationships and keep information up to date (including customer identification if the customer is active with us). The Compliance Officer will determine whether or not information about our customers and/or businesses relationships is up to date, and may contact staff for additional information.

When an ongoing service agreement has been established with an entity client, a third party determination must also be made.

### 6.7 Risk Ranking & Transaction Monitoring

Most of our customers are considered not high risk, however, certain customers will be considered higher risk than others. This does not mean that these are "bad" people or that they have committed any crimes. High risk customers are not treated differently when they interact with our staff, but their activities are reviewed more carefully behind the scenes.

High risk customers are subject to regular transaction monitoring and enhanced due diligence. The Compliance Officer or a designate completes these activities. Transaction monitoring involves the review of customer transaction patterns to look for suspicious indicators. Enhanced due diligence involves additional investigation, and in some cases, the Compliance Officer may ask you to collect additional information from the customer, such as details about a specific transaction.

## 7 Penalties for Non-Compliance[17]

Non-compliance with Parts 1 and 1.1 of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act may result in criminal or administrative penalties.

FINTRAC has legislative authority to issue an administrative monetary penalty (AMP) to reporting entities that are in non-compliance with Canada's Proceeds of Crime (Money Laundering) and Terrorist Financing Act and its enacted regulations.

FINTRAC may disclose cases of non-compliance to law enforcement when there is extensive non-compliance or little expectation of immediate or future compliance. Criminal penalties may include the following:

- Failure to report suspicious transactions: up to $2 million and/or 5 years imprisonment;
- Failure to report a large cash transaction or an electronic funds transfer: up to $500,000 for the first offence, $1 million for subsequent offences;
- Failure to meet record keeping requirements: up to $500,000 and/or 5 years imprisonment;
- Failure to provide assistance or provide information during compliance examination: up to $500,000 and/or 5 years imprisonment; or

[17] https://laws-lois.justice.gc.ca/eng/regulations/SOR-2007-292/

- Disclosing the fact that a suspicious transaction report was made, or disclosing the contents of such a report, with the intent to prejudice a criminal investigation: up to 2 years imprisonment.

Non-criminal penalties may be issued 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 intelligence mandate or on the objectives of the Act and its regulations. Categories for violations where AMPs would be administered are assigned the following penalty ranges:

| **Categories of violations** | **Penalty range** |
|---|---|
| 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<br>$1 to $500,000 per violation for an entity |

# 8 Appendix: Definitions & Acronyms[18]

**AMF:** Autorité des marchés financiers

**AML**: Anti-Money Laundering

**Anti-Money Laundering**: actions taken to detect, deter and prevent money laundering from occurring through our business.

**ASTR**: Attempted Suspicious Transaction Report

**Attempted Suspicious Transaction Report**: a report that is filed with FINTRAC when we have reasonable grounds to suspect that a customer's activities may be related to money laundering or terrorist financing when no transaction was completed. This can include transactions that were cancelled by us, or by the customer. FINTRAC reports are filed by the Compliance Officer or designate as soon as practicable after completing the measures that enabled a determination that there are reasonable grounds to suspect that the activity could be related to money laundering and/or terrorist financing. If you suspect that an attempted transaction is related to money laundering or terrorist financing, you must submit an unusual transaction form to the Compliance Officer on the date that the request occurs.

**Autorité des marchés financiers:** The Autorité des marchés financiers is the organisation responsible for financial regulation in the Canadian province of Québec. It regulates the province's financial markets and provides assistance to consumers of financial products and services.

**Counter Terrorist Financing**: actions taken to detect, deter and prevent terrorist financing from occurring through our business.

**CTF**: Counter Terrorist Financing

**Financial Transactions and Reports Analysis Centre of Canada**: Canada's financial intelligence unit and our regulator for AML and CTF. We submit reports to FINTRAC and they have the right to examine us to test our compliance with Canadian requirements. All FINTRAC correspondences and inquiries should be passed immediately to the Compliance Officer.

**FINTRAC**: The Financial Transactions and Reports Analysis Centre of Canada

[18] Additional definitions and acronyms can also be found here: https://github.com/ScryptoNoob/Glossary-of-Acronyms-Definitions/blob/master/AML%20and%20KYC%20Glossary.md

**Large Cash Transaction**: any cash transactions valued at CAD 10,000 or more that take place within the same 24-hour period for the same customer. This may include one or several transactions.

**Large Cash Transaction Report:** a report that is filed with FINTRAC when a large cash transaction has taken place. This report must be filed with FINTRAC within 15 calendar days of the transaction. Staff are required to report large cash transactions to the Compliance Officer on the day that they occur using our internal Large Cash Transaction Reporting form.

**Large Virtual Currency Transaction Report**: a report that is filed with FINTRAC when a large virtual currency transaction has taken place. This report must be filed with FINTRAC within 5 working days after the day on which the person or entity transfers or receives the amount.

**LCTR**: Large Cash Transaction Report

**LVCTR**: Large Virtual Currency Transaction Report

**Money Laundering**: the process of taking money obtained by committing a crime and disguising the source to make it appear legitimate. Under the Criminal Code of Canada, it is illegal to launder money or to knowingly assist in laundering money. Under the PCMLTFA and Regulations, we must take steps to be sure that our business is not used to launder money and if we suspect that money laundering may be taking place, we must report it.

**Money Services Business**: a business that provides services in Canada: foreign exchange, remittance and/or issuing or redeeming monetary instruments. A business may also be considered a money service business in the province of Québec by providing any of the mentioned services and/or cheque cashing and/or the operation of automated teller machines.

**MSB**: Money Services Business

**STR**: Suspicious Transaction Report

**Suspicious Transaction Report**: a report that is filed with FINTRAC when we have reasonable grounds to suspect that a transaction is related to money laundering or terrorist financing. The Compliance Officer files FINTRAC reports as soon as practicable after completing the measures that enabled a determination that there are reasonable grounds to suspect that the activity could be related to money laundering and/or terrorist financing. If you suspect that a transaction is related to money laundering or terrorist financing, you must submit an unusual transaction form to the Compliance Officer on the date that the transaction occurs.

**Terrorism**: is any attempt to influence or intimidate a government or the public at large through violent or illegal means or means that are intended to induce fear or panic.

**Terrorist Financing**: funding any act of terrorism or committing any act or omission that facilitates the funding of terrorism.

**Terrorist Property Report**: A report that is filed with several government bodies, including FINTRAC, when we believe that we may be in possession of property or funds that are owned or controlled by terrorists. The Compliance Officer files these reports immediately. If you suspect that we are in possession of terrorist property or funds, you must submit a Possible Terrorist Property Report to the Compliance Officer on the same day.

**TPR**: Terrorist Property Report

**Unusual Transaction Report**: An internal form that is used to record the details of any transactions (attempted or completed) that are suspected of being related to money laundering or terrorist financing.

**UTR**: Unusual Transaction Report