Trackon Canada Private Ltd

Anti-Money Laundering

&

Counter Terrorist Financing

Procedures for Compliance Staff

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 Compliance Officer

This document provides procedural guidance for Trackon Canada Private Ltd (Trackon)'s Compliance Officer and any delegates performing tasks on the Compliance Officer's behalf.

2 Staff

For the purposes of this document, references to staff and employees include any other third party companies that perform relevant functions including customer interactions, customer identification, and transaction related functions.

3 AML Compliance Program Updates

The Compliance Officer will update the anti-money laundering (AML) and counter terrorist financing (CTF) compliance program:

- Annually in the fourth quarter of every calendar year;
- Where there are changes to Trackon 's business model;
- Where there are changes to Canadian AML or CTF legislation;
- Following AML Compliance Effectiveness Reviews, which are required every two years in order to address any deficiencies identified by the reviewer;
- Following regulatory reviews to address any deficiencies identified by the regulator; and
- In the event of internal process or performance issues that have been identified by Trackon as requiring remediation.

All program updates will be logged and tracked by the Compliance Officer. Records of program updates will be maintained for a minimum of five years.

The Compliance Officer will communicate relevant changes to staff members in a manner that ensures that all staff are aware of changes and able to perform their roles effectively.

4 AML Compliance Training

The Compliance Officer will ensure that all staff have received sufficient training to be effective in their roles. Minimum standards for training are set out in the AML & CTF Compliance Policy. In instances where staff are performing specialized roles, or where the Compliance Officer has observed performance issues relating to compliance tasks, additional training will be provided.

The Compliance Officer or a delegate will maintain a training plan and records of all training sessions conducted, including training sessions outside of new hire and annual employee training, for a minimum of five years. The Compliance Officer will also maintain records of all external training sessions attended by the Compliance

Officer and/or designates for the purpose of maintaining up to date knowledge of Canadian AML and CTF legislation and best practices.

5 AML Compliance Effectiveness Reviews

The Compliance Officer will ensure that an AML Compliance Effectiveness Review is conducted at least every two years. The resulting report will be signed-off by Senior Management within 30 days of issue. The minimum standards are defined in the AML & CTF Compliance Policy. At a minimum, the following must be completed:

- A review of AML policy and procedure;
- A review of the risk assessment;
- Interviews with the staff to determine their knowledge of the legislative requirements and company's policies and procedures;
- A review of the criteria and process for identifying and reporting attempted suspicious transactions and suspicious transactions;
- A sampling of large cash transactions followed by a review of the reporting of such transactions;
- A test of the record keeping system for compliance with the legislation;
- A test of the client identification procedures for compliance with the legislation;
- A review of the risk assessment.

In addition to ensuring that these standards are met, the Compliance Officer will ensure that all reviewers are sufficiently qualified by requesting a copy of the curriculum vitae (CV) for all reviewers prior to selecting a third-party reviewer.

At minimum, each reviewer must:

- Demonstrate sufficient understanding of the Canadian regulatory context;
- Have sufficient experience in conducting AML Compliance Effectiveness Reviews in Canada; and
- Have maintained up to date training and professional qualifications; including, but not limited to, the Certified Anti-Money Laundering Specialist designation.

Records maintained by the Compliance Officer will include:

- A copy of the final report;
- A record of senior management sign-off on the final report;
- A copy of the agreement between Trackon and the reviewer;
- Copies of the CVs for all reviewers to ensure that each reviewer is sufficiently qualified to perform the review; and
- A record of any updates made to Trackon 's compliance program to address deficiencies identified by the reviewer.

All records relating to AML Compliance Effectiveness Reviews are maintained for a minimum of five years.

6 FINTRAC Registration & Communication

The Compliance Officer will maintain Trackon 's registration with the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) by:

- Ensuring that the renewal of the registration is completed in the time and manner specified by FINTRAC (generally every two years);
- Updating relevant information, including business activity information and key employee information, within 30 days following any changes to Trackon's business activities or key personnel;
- Responding to any FINTRAC requests for clarification regarding the MSB registration within the required timeframes (generally 30 business days); and
- Cancelling the MSB registration with FINTRAC if Trackon ceases to offer MSB services in Canada. This must occur within 30 days after the date Trackon stops offering MSB services.

Updates and renewals of Trackon 's FINTRAC registration is completed using the online money services business (MSB) registry. The Compliance Officer will maintain records of all updates and renewals for five years.

Additional communication with FINTRAC may include examinations, compliance assessment reports, and other information requests. In all cases, the Compliance Officer, or a designate, will act as the liaison with FINTRAC. Records of all FINTRAC communication, including Trackon 's responses, will be maintained for a minimum of five years.

The Compliance Officer will ensure that records that may be required by FINTRAC are stored in a manner that they can be retrieved, and communicated to the regulator, in a timely manner. Generally, Trackon will have 30 calendar days from the date that a request is sent by FINTRAC to assemble and submit information. Where Trackon receives a confirmation from FINTRAC that information has been received, this confirmation will be maintained as part of Trackon 's records of correspondence with FINTRAC.

The Compliance Officer receives regular email updates from FINTRAC, including news releases. Calendar entries are used to track regulatory tasks including updates and renewals.

7 AMF MSB Licensing & Communication[1]

Should Trackon commence business in Quebec, the Compliance Officer will maintain Trackon's MSB licensing with the Quebec Autorité des marchés financiers (AMF) by:

- Ensuring that the renewal of the registration is completed in the time and manner specified by the AMF;
- Updating relevant information, including business activity information and key employee information within 15 calendar days following any changes to Trackon's business activities or key personnel;
- Updating information relating to the previous year's business operations by no later than March 31st of each calendar year.

The Compliance Officer will maintain records of all updates and renewals for a minimum of six years.

Additional communication with the AMF may include examinations, compliance assessment reports, and other information requests. In all cases, the Compliance Officer or his designate will act as the liaison with the AMF. Records of all AMF communication, including Trackon's responses will be maintained for six years.

The Compliance Officer will ensure that records that may be required by the AMF are stored in a manner that they can be retrieved and communicated to the regulator in a timely manner. Where Trackon receives a confirmation from the AMF that information has been received, this confirmation will be maintained as part of Trackon's official records, along with any other official communication to or from the AMF.

8 Ministerial Directives

Under Part 1.1 of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA), which came into force on June 19, 2014, the Minister of Finance may:

- Issue directives that require reporting entities to apply countermeasures to transactions coming from or going to designated foreign jurisdictions or entities; and
- Recommend the introduction of regulations to restrict reporting entities from entering into a financial transaction coming from or going to designated foreign jurisdictions or entities.

These authorities allow the Minister of Finance to take steps to protect Canada's financial system from foreign jurisdictions and foreign entities that are considered to present high risks for facilitating money laundering and terrorist financing.

---

[1] Trackon does not currently conduct business or serve customers in the province of Quebec. This section has been included for educational purposes only or in the event our business model changes.

The Compliance Officer will maintain an awareness of such directives by regularly reviewing FINTRAC's website[2] and subscribing to FINTRAC's mailing list[3].

8.1 Ministerial Directive on the Democratic People's Republic of Korea (DPRK), Also Known as North Korea

This Ministerial Directive requires that all transactions to and from North Korea be treated as high risk, regardless of the amounts of the transactions. In addition, FINTRAC's expectation is that Trackon implements specific measures to mitigate the risk posed by these transactions and document the measures taken.

When conducting these transactions, regardless of the transaction amounts, the measures that are taken to mitigate the risk may include:

- Keeping a record of all transactions to and from North Korea, regardless of the amount.
    - This record must include details such as the customer's name and address, the amount, currency, date and type of transaction.
    - If the customer is a person, their date of birth and the nature of their principal business or their occupation, as applicable; and if the customer is an entity, the nature of their principal business.
    - If the transaction is an electronic funds transfer, recording the ordering customer and the beneficiary, as well as their addresses, the amount, currency and date of transaction.
    - If the ordering customer is a person, their date of birth and the nature of their principal business or their occupation, as applicable; and if the ordering customer is an entity, the nature of their principal business.
- These details must specify whether funds are coming from, or destined to, North Korea;
- Ensuring that the information about the identity of these customers is up to date;
- Exercising customer due diligence, including asking for the:
    - Source of the funds;
    - Purpose of transactions; and
    - Beneficial ownership (if the client is an entity);
- Conducting enhanced ongoing monitoring of the customer and/or the business relationship and/or the account involved in the transaction;
- Keeping records related to all of the above actions; and
- Reporting suspicious transactions (if applicable).

In the case that we suspect, but do not know that a transaction is related to North Korea, the transaction will be treated as high risk. In its Operational Brief[4] on the subject, FINTRAC provides several relevant indicators:

---

[2] http://www.fintrac.gc.ca/obligations/directives-eng.asp
[3] http://www.fintrac.gc.ca/contact-contactez/list-liste-eng.asp

- **Transactions Involving Front or Shell Companies**: North Korean entities and individuals have made use of front and shell companies in various jurisdictions to mask their involvement in the international financial system. Such companies may have the following characteristics:
    - The lack of their own online presence, such as a company website indicating normal business-related information such as products and services, contact information, and physical geographic location.
    - A corporate name which is overly generic, non-descriptive, or easily mistaken with that of another better-known corporate entity. Additionally, the corporate name may be regularly misspelled in different ways.
    - A pattern of sending or receiving international EFTs to or from Canadian businesses that operate in sectors or industries unrelated to each other.
    - Transactional patterns which are exclusively one-directional; e.g., the company only sends but never receives EFTs, or vice versa.
    - Transactional patterns in which the same observed activity (e.g., sending EFTs) and the Canadian recipients remain consistent, but the foreign ordering company changes over time, particularly if the sending companies are from the same jurisdiction or geographic area.
- **Transactions Involving Particular Jurisdictions**: North Korean entities and individuals have been observed using particular jurisdictions from which to access the international financial system. While the jurisdictions discussed below are not an exhaustive list, transactions to or from these areas, in combination with other indicators, should be considered when deciding to report a suspicious transaction report to FINTRAC:
    - Liaoning Province, China shares a land border with North Korea, and both companies and financial institutions in this jurisdiction have been reported to engage in financial activity and other business dealings with North Korean companies and China-based front companies. FINTRAC also notes that there is a substantial amount of Canada-linked EFT reporting to a number of these cities, in particular Dalian, China and Shenyang, China.
    - Jilin Province, China also shares a land border with North Korea, and has been associated with companies employing North Korean guest workers in the food processing and manufacturing sectors. FINTRAC notes that there is also a substantial amount of EFT reporting to Changchun, the capital of Jilin province.
    - Hong Kong has also been associated with North Korean financial activity. While this is not unexpected given Hong Kong's role as a major center of global finance, transactions to or from Hong Kong that display other indicators, particularly those indicating possible use of shell companies, may warrant additional scrutiny.

[4] http://www.fintrac.gc.ca/intel/sintel-eng.asp

While, we do not conduct any transactions with North Korea, nor do any of our transaction have touchpoints with the jurisdiction, where facts, context, and indicators lead the Compliance Officer to believe that a transaction may be related to North Korea, an STR will be submitted to FINTRAC, and the reasons will be noted in the freeform section of the report.

8.2 Ministerial Directive on Financial Transactions Associated with the Islamic Republic of Iran

This Ministerial Directive requires that all transactions to and from Iran be treated as high risk, regardless of the amounts of the transactions. In addition, FINTRAC's expectation is that Trackon implements specific measures to mitigate the risk posed by these transactions and document the measures taken.

When conducting these transactions, regardless of the transaction amounts, the measures that are taken to mitigate the risk may include:

- Treat every financial transaction originating from or bound for Iran, regardless of its amount, as a high risk transaction;
- Verify the identity of any client (person or entity) requesting or benefiting from such a transaction;
- Exercise customer due diligence, including ascertaining the source of funds in any such transaction, the purpose of the transaction and, where appropriate, the beneficial ownership or control of any entity requesting or benefiting from the transaction;
- Keep and retain a record of any such transaction;
- Determine whether there are reasonable grounds to suspect the commission or attempted commission of a money laundering or terrorist financing offence and report all suspicious transactions to FINTRAC;
- Reporting all other reportable transactions (if applicable).

In the case that we suspect, but do not know that a transaction is related to Iran, the transaction will be treated as high risk. In its Guidance[5] on the subject, FINTRAC provides several relevant indicators:

- Payment for products by electronic funds transfers (EFTs) that include an Iranian originating or destination address;
- Receiving Iranian rial as part of a transaction; or
- Accepting bank drafts or other negotiable instruments that include an Iranian rial component.

To be clear, this Ministerial Directive does not apply to transactions where there is no suspicion or explicit connection with Iran and there is no evidence of the transaction originating from or being bound for Iran. A couple of examples were provided in the FINTRAC Guidance:

[5] https://www.fintrac-canafe.gc.ca/obligations/dir-iri-eng

- A client who has previously sent funds to Iran requests an outgoing EFT, where the transaction details do not suggest that this transaction is bound for Iran and you are unable to obtain further details about the transaction destination; or
- The client's identification information is the only suggestion of a connection to Iran (for example, a transaction where the conductor's identification document is an Iranian passport).

While, we do not conduct any transactions with Iran, nor do any of our transaction have touchpoints with the jurisdiction, where facts, context, and indicators lead the Compliance Officer to believe that a transaction may be related to Iran, an STR will be submitted to FINTRAC, and the reasons will be noted in the freeform section of the report.

9 Reporting

Certain types of transactions must be reported to FINTRAC. Reporting to FINTRAC should always be completed by the Compliance Officer, or a designate, which is 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. 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.

Reportable transactions are detected by:

- Trackon 's electronic platforms; and/or
- Trackon employees.

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.

Reports are submitted to FINTRAC electronically using the F2R Reporting system where possible. In all reports with optional fields, these fields should be considered mandatory if Trackon has the information on file.

9.1 Electronic Funds Transfers

Reportable electronic funds transfers (EFTs) include funds or instructions sent out of (outgoing) or into (incoming) Canada for transactions valued at CAD 10,000 or more. These may be either a single transaction, or multiple transactions within the

same 24-hour period[6]. The report type is an Electronic Funds Transfer Report (EFTR) and must be reported where we know the transactions:

- were initiated by the same person or entity;
- were initiated on behalf of the same person or entity (third party); or
- are for the same beneficiary (person or entity); or

Where we receive two or more international EFTs that total CAD 10,000 or more within a static 24-hour window, and we know that the transactions:

- were initiated by the same person or entity; or
- are for the same beneficiary (person or entity).

There are exemptions when it comes to reporting EFTRs, which include when the transaction is conducted by:

- A public body, which is:
    - any department or agent or mandatary of Her Majesty in right of Canada or of a province;
    - an incorporated city or town, village, metropolitan authority, township, district, county, rural municipality or other incorporated municipal body in Canada or an agent or mandatary in Canada of any of them; or
    - an organization that operates a public hospital and that is designated by the Minister of National Revenue as a hospital authority under the Excise Tax Act, or an agent or mandatary of such an organization;
- A Very Large Corporation (VLC) or trust that has minimum net assets of $75 million on its last audited balance sheet, whose shares or units are traded on a Canadian stock exchange or a stock exchange designated under subsection 262(1) of the Income Tax Act and that operates in a country that is a member of the Financial Action Task Force; or
- An administrator of a pension fund that is regulated under federal or provincial legislation.

Trackon uses the last rate provided by the Bank of Canada available at the time of the transaction to determine if the CAD 10,000 or more threshold is met for the transaction to be reportable as an EFT transaction.

If there is no Bank of Canada noon rate published for the currency of the transaction, Trackon uses the actual exchange rate applied when the transaction is processed for determination of whether it is reportable.

Where there is a determination that the EFT is reportable, a report will be submitted to FINTRAC within 5 working days from the date on which the

[6] Trackon uses a 24-hour rolling clock. Any references to a 24-hour period refer to a rolling 24-hour period, and not to a static (calendar day) period.

transaction(s) took place. This will be done manually by the Compliance Officer using FINTRAC Web Reporting (F2R).

Where there is an EFTR valued at CAD 100,000 or more, the Compliance Officer or a designate will ensure that a politically exposed person (PEP) or head of an international organization (HIO) determination has been conducted. Where possible, the source of funds will also be requested and documented. This is discussed in greater detail under the PEP Check section.

These transactions are detected automatically by the IT system. The Compliance Officer reviews transaction related alerts on a regular basis. At the time that these alerts are reviewed, the Compliance Officer will consider whether any additional reporting (STR) is required.

The Compliance Officer will maintain records of:

- All EFTRs filed with FINTRAC;
- All reconciliations conducted to determine whether or not transactions are reportable by Trackon; and
- Records of Politically Exposed Person (PEP) determinations and related information for EFTs valued at CAD 100,000 or more.

All records relating to EFTRs will be maintained for a minimum of five years.

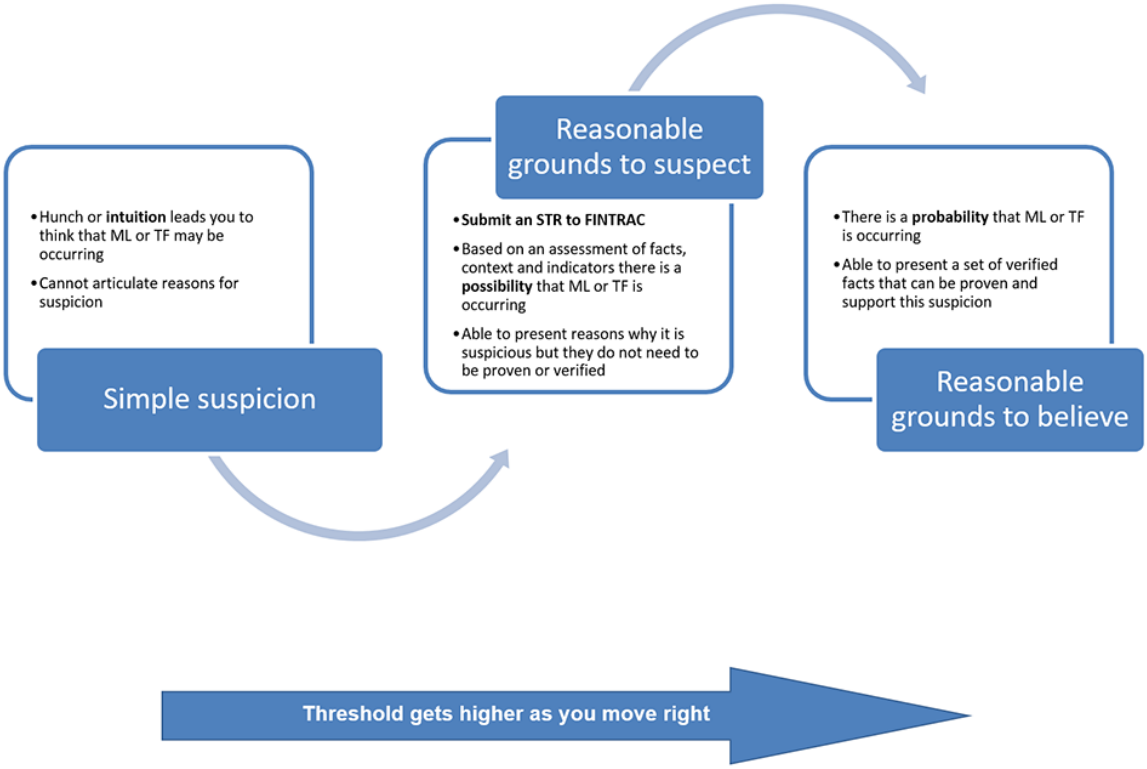
9.2 Suspicious Transactions & Attempted Suspicious Transactions

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 required to establish reasonable grounds to suspect it may be related to money laundering or terrorist financing.

As soon as practicable is a time period that falls in-between immediately and as soon as possible within which a suspicious transaction report (STR) be submitted to FINTRAC. In this context, the report must be completed promptly, taking into account the facts and circumstances of the situation. While some amount of delay is permitted, it must have a reasonable explanation. The completion and submission of the report should take priority over other tasks.

9.2.1 Reasonable Grounds to Suspect

Understanding the differences between the thresholds can help clarify what reasonable grounds to suspect means and how it can be operationalized within your compliance program. See the diagram below for an overview of the different thresholds.



Simple suspicion is a lower threshold than reasonable grounds to suspect and is synonymous with a "gut feeling" or "hunch". In other words, simple suspicion means that we have a feeling that something is unusual or suspicious, but do not have any facts, context or indicators to support that feeling or to reasonably conclude that an ML/TF offence has occurred. Simple suspicion could prompt us to assess related transactions to see if there is any additional information that would support or confirm your suspicion.

Reasonable grounds to suspect is the required threshold to submit an STR to FINTRAC and is a step above simple suspicion, meaning that there is a possibility that an ML/TF offence has occurred. We do not have to verify the facts, context or ML/TF indicators that led to our suspicion, nor do we have to prove that an ML/TF offence has occurred in order to reach reasonable grounds to suspect. Our suspicion must be reasonable and therefore, not biased or prejudiced.

Reaching reasonable grounds to suspect means that we consider the facts, context, and ML/TF indicators related to a financial transaction and, after having reviewed this information, we conclude that there are reasonable grounds to suspect that this particular financial transaction is related to ML/TF. We must be able to demonstrate and articulate our suspicion of ML/TF in such a way that another individual reviewing the same material with similar knowledge, experience, or training would likely reach the same conclusion.

The explanation of our assessment should be included in the narrative portion, Part G, of the STR. Many factors will support our assessment and conclusion that an

ML/TF offence has possibly occurred; they should be included in our report to FINTRAC.

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

If we are in receipt of a production order, by law enforcement, we must perform an assessment of the facts, context, and ML/TF indicators to determine whether we have reasonable grounds to suspect that a particular transaction is related to the commission of ML/TF.

9.2.2 Measures for Establishing Reasonable Grounds to Suspect

In order to submit an STR to FINTRAC, we will need to ensure that we have completed the measures that enable us to reach the reasonable grounds to suspect threshold, meaning that there is a possibility that an ML/TF offence has occurred.

These measures include:

- screening for and identifying suspicious transactions via our IT system;
- assessing the facts and context surrounding the suspicious transaction;
- linking ML/TF indicators to our assessment of the facts and context; and
- explaining our grounds for suspicion in an STR, where we articulate how the facts, context and ML/TF indicators allowed us to reach our grounds for suspicion.

A fact, for the purpose of completing an STR, is defined as an event, action, occurrence or element that exists or is known to have happened or existed — it cannot be an opinion. Facts known to Trackon could also include account details, particular business lines, the client's financial history or information about the individual or entity (for example, that the individual has been convicted of a designated offence or is the subject of a production order, or that an entity is being investigated for fraud or any other indictable offence).

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

Indicators are potential red flags that can initiate suspicion and indicate that something may be unusual without a reasonable explanation. Red flags typically

stem from one or more facts, behaviours, patterns or other factors that identify irregularities related to a client's transactions. These transactions often present inconsistencies with what is expected or considered normal based on the facts and context you know about your client's transactional activities.

9.2.3 Submitting STRs & ASTRs to FINTRAC

When the Compliance Officer has decided that reasonable grounds to suspect have been established, an STR or ASTR must be submitted to FINTRAC as soon as practicable. Trackon has translated this to mean without delay. The STR or ASTR to be submitted will include the following information (if available):

- Who are the parties to the transaction?
    - List the conductor, beneficiary and holders of all accounts involved in the transaction.
    - Take reasonable measures to identify the conductor of the transaction. This means that you are expected to ask the client for this information unless you think doing so will tip them off to your suspicion.
    - Provide identifying information on the parties involved in the transaction. This could include the information you recorded to identify the conductor, as well as any information you have on the other parties to the transaction or its recipients.
    - List owners, directors, officers and those with signing authority, when possible. If the transaction involves a business, you could include information on the ownership, control and structure of the business in the STR.
    - Provide clear information about each individual or entity's role in each of the financial transactions described. It is important to know who is sending and receiving the funds and this may be relevant in Part G of the STR.
    - Explain the relationships among the individuals or entities (if known). This is very helpful to FINTRAC when trying to establish networks of individuals or entities suspected of being involved in the commission or attempted commission of a money laundering (ML) or terrorist financing (TF) offence.
- When was the transaction(s) completed/attempted? If it was not completed, why not?
    - Provide the facts, context and ML or TF indicators regarding the transaction.
- What are the financial instruments or mechanisms used to conduct the transaction?
- Where did this transaction take place?
- Why the transaction(s) or attempted transaction(s) are related to the commission or attempted commission of an ML or TF offence?
    - State the ML or TF indicators used to support your suspicion.

    - State the suspected criminal offence related to ML or TF, if known.
- How did the transaction take place?

Suspicious or attempted suspicious transactions do not have a minimum dollar threshold and may relate to any of Trackon 's business activities. Reports are not limited to the business activities that define Trackon as a regulated entity in Canada.

For example, if a prospective customer calls and asks whether or not Trackon would be willing to send funds to another country without them going through the identification requirements associated with the platform, this should be reported as an attempted suspicious transaction.

Employees are to report this type of transaction using the Unusual Transaction Form (Internal), which is submitted to the Compliance Officer on the same day that the transaction takes place.

The Compliance Officer will emphasize the following to all staff:

- It is important not to let the customer know that they are suspicious. It is against the law to deliberately "tip off" a customer about a potential investigation. Trackon and all staff 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 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).

These transactions are detected automatically by the IT system. The Compliance Officer reviews transaction related alerts on a regular basis. At the time that these alerts are reviewed, the Compliance Officer will consider whether any additional reporting (i.e. EFTR) is required.

The Compliance Officer will maintain records of:

- All STRs and ASTRs filed with FINTRAC;
- All internal unusual transaction reports, including reports filed for transactions that were not reported to FINTRAC;
- All technology-based transaction monitoring alerts related to unusual transactions;
- A record of the reason that transactions escalated (via staff or via a transaction monitoring system) were not reported to FINTRAC, including the analysis that was conducted and the basis for each decision; and

- Records of any follow-up activity, including but not limited to updates to customer risk scores, additional transaction monitoring and the closing of customer accounts.

These records are currently maintained in electronic format and include the original transaction information and Compliance Officer decisions related to reporting.

Where an STR or ASTR is reported, the customer's risk rating will be manually changed to high risk. Where a customer is not considered high risk subsequent to the filing of an STR or ASTR, the rationale must be documented.

All records relating to STRs and ASTRs will be maintained for a minimum of five years.

9.3 Terrorist Property

Terrorist Property Reports (TPRs) are completed if Trackon is in possession of funds or property that belong to a terrorist (either an individual or an organization). Generally, Trackon would become aware of terrorist property via list screening that is conducted. This process involves matching our client information against publicly available lists published by the United Nations Security Council (UNSC)[7], which is a consolidated list of known terrorists and sanctioned individuals and organizations. This process is described under list screening.

It is also possible for staff to become aware through conversations with our customers that illegal activity may be taking place. In these cases, staff are instructed to escalate these reports to the Compliance Officer immediately. The Compliance Officer conducts an investigation to determine whether or not reports or the freezing of property is required. Staff use the Unusual Transaction Report (Internal) for this purpose.

TPRs are submitted immediately to FINTRAC as well as to the Royal Canadian Mounted Police (RCMP) and the Canadian Security Intelligence Service (CSIS). All TPRs are submitted via fax and copies of the faxed confirmations are maintained. TPRs are submitted to:

- FINTRAC, fax: 866-226-2346
- RCMP, Anti-Terrorist Financing Team, unclassified fax: 613-825-7030
- CSIS Financing Unit, unclassified fax: 613-369-2303

The Compliance Officer will maintain records of:

- All TPRs filed;
- Fax confirmations for all TPRs sent to FINTRAC, CSIS and/or RCMP;
- All internal unusual transaction reports related to TPRs, including reports filed for transactions that were not reported;

[7] https://www.un.org/securitycouncil/content/un-sc-consolidated-list

- A record of the reason that transactions escalated (via staff or via a transaction monitoring system) were not reported, including the analysis that was conducted and the basis for each decision; and
- Records of any follow-up activity, including but not limited to updates to customer risk scores, additional transaction monitoring and the closing of customer accounts.

In the case that terrorist property is suspected, but the customer does not match any lists, an ASTR or STR will be submitted to FINTRAC.

All records relating to TPRs will be maintained for a minimum of five years.

9.4 Multiple Reports

More than one report may be required for a single transaction. The Compliance Officer will ensure that all applicable report types are filed.

For example: If a customer conducts a transaction by wiring CAD 15,000 and the transaction is considered to be suspicious (for instance, if the customer provides identification documentation that appears false) then multiple reports would be required, including two of the following:

- EFTR, and
- STR/ASTR.

All reports must be completed in full and filed on time. The completion of one report does not negate or change the requirement to complete any other report type.

9.5 Responding to Law Enforcement Requests

There may be exceptional times when Trackon is required to disclose personal information, without an individual's consent, in order to comply with a subpoena, warrant, court order or other law enforcement request. Similarly, Trackon may disclose personal information without consent to a government institution or an investigative body for a purpose such as national security, national defence or the deterrence of terrorism, law enforcement, or in relation to a suspected money-laundering offence[8].

If Trackon receives a request from law enforcement the Compliance Officer must be notified immediately.

A request has to be in writing: In order to understand the request, the Compliance Officer will request a subpoena, Court Order, or other evidence, if it has not been provided. This documentation protects the company and Compliance Officer in the request for information and the release of information under Canadian privacy law.

[8] https://www.priv.gc.ca/en/privacy-topics/accessing-personal-information/obligations-for-organizations/02_05_d_54_ati_02/

The person requesting information should be identified and the date of the request should be recorded. The request should be analyzed, and clarification should be sought from the law enforcement officer if necessary before any information is disclosed. Exemptions under PIPEDA should also be analyzed by the Privacy Officer if applicable to the request[9].

Once the supporting evidence is received and the information request is understood, Trackon will comply with the information request in a format reasonable to the request such as having the individual review records in the office or providing paper copies of information. Trackon will retain copies of any and all information disclosed during this process for a minimum of five years.

It is possible that the individual concerned may request access to information related to this disclosure. If this happens, Trackon must notify the institution to which the information was disclosed. The institution has 30 days to respond.

Trackon may not respond to the individual's access request before either hearing back from the institution or until 30 days has passed since Trackon was notified of it; whichever occurs first.

If the institution objects to the release of the information to the individual based on permissible grounds, Trackon must withhold it. Trackon may not reveal that we communicated with the institution, or that it objected to the disclosure.

10 Voluntary Self-Declaration of Non-Compliance[10]

If Trackon becomes aware of a non-compliance event that leads to an issue in our reporting obligations, a voluntary self-declaration of non-compliance will be made to FINTRAC, in writing, by the Compliance Officer.

The voluntary self-declaration of non-compliance must include the following:

- Our company name and the Compliance Officer's contact information;
- What the issue is, and how was it discovered;
- What type of report, the number of reports impacted or missed, and the time period during which the issue occurred;
- The reason why the reports were not submitted, were late, or incorrect;
- Other related details; and

[9] https://www.priv.gc.ca/en/privacy-topics/accessing-personal-information/obligations-for-organizations/02_05_d_54_ati_02/

[10] When the voluntarily declared non-compliance issue is not a repeated instance of a previously voluntarily disclosed issue, and when this declaration has not been made after a reporting entity has been notified of an upcoming examination, FINTRAC will work with the entity to resolve the issue and will not propose an administrative monetary penalty.

- How the issue will be resolved and when it will be resolved.

The voluntary self-declaration of non-compliance is sent directly to: VSDONC.ADVNC@fintrac-canafe.gc.ca. A record will be retained by the Compliance Officer.

In cases where there are missing reports, the Compliance Officer (or delegate) will submit them without further delay.

11 Customer & Business Relationship Risk Ranking

All of our customers are required to provide know your customer (KYC) information and identification information in order to complete transactions.

We divide our customers into Not High and High risk buckets based on their activities. The parameters for customer risk ranking are described in our Money Laundering and Terrorist Financing Risk Assessment document.

Customer and business relationship risk ranking is conducted on an ongoing basis, taking into consideration the customer's characteristics, the products, services and delivery channels used by the customer, the customer's geography (including the destination of funds) and any other relevant factors.

Records related to customer and business relationship risk ranking, monitoring, due diligence, enhanced motoring, and enhanced due diligence are maintained electronically.

12 Customer & Business Relationship Information Updates

For all active customers (customers that have conducted a transaction within the past year), verification information is updated on a regular schedule, based on customer risk and triggering events.

12.1 Information Updates

Customer information updates refer to the customer's:

- Name;
- Address;
- Email address;
- Telephone number; and
- Occupation or principal business.

Where we have a business relationship with the customers, the nature and purpose of the business relationship must be updated as well.

12.1.1 Inactive Status

Inactive customers (any customer that has not completed a transaction within the past year) are required to update their customer information in order to complete any prescribed transactions.

12.1.2 Not High Risk Customers & Business Relationships

Not High risk customers are required to update their customer information at the point that the identification document has expired. In the case that there is no expiry date for the identification document initially provided, customer information is updated every five years.

12.1.3 High Risk Customers & Business Relationships

High risk customers are required to update their customer information every two years.

If the reason that a customer has been considered high risk relates to doubts about the veracity of any of the information or identification provided to Trackon, additional identification or confirmation of customer identification may be required at the Compliance Officer's discretion.

High risk customers are subject to enhanced 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.

13 Transaction Monitoring

Transactions are monitored for activities that may indicate that money laundering or terrorist financing could be taking place. Currently, Trackon is using ComplyAdvantage[11] for transaction monitoring and has implemented its customized ruleset in order to do so.

The rules in place monitor transactions based on the following parameters:

#	Name	Description	Rule Logic Explained
1	[Payments] - High Velocity outbound	Number of outgoing transactions over a short period is greater than limit	Was the transaction Outbound Has the customer had more than a set [Number] of Outbound transactions in the most recent 7 days?
2	[Payments] -	Sum of outgoing transactions over a	

[11] https://complyadvantage.com/aml-transaction-monitoring/

	High Cumulative Amount - Outbound	short period is greater than a limit	Was the transaction Outbound Has the customer's sum of Outbound transactions in the most recent 7 days been greater than a set [Amount]?
3	[Payments] - Unexpected Value	Transaction value exceeds customer declared limit	Was the customer's expected amount provided (in base currency)? Was the transaction more than a set [Factor] times greater than the customer's expected transacion value?
4	Movement of Funds - Outbound (rename rule and clean up the description)	Sum of incoming transactions similar to sum of outgoing transactions Totals of incoming is 100+/-[Y] precentage of outgoing transactions over the last {time period} Rule logic: compare the sum of outgoing and sum of incoming transactions over a set number of days. and if they are about the same - we need to alert. ""About the same"" can be calculated any way we choose. My suggestion would be to use a factor for this calculation. sum of incoming transactions is 100+/-[FACTOR] percentage of sum of outgoing transactions over the last {time period}. Explanation: So that if factor = 20, for example, then we use (100-20)%, and (100+20)% as the limits: 80% * sum of outgoing <sum of incoming <120% sum of outgoing"	Has the sum of the cusotmer's Outbound transactions withdrawn over the last 30 days, been greater than a set [Amount]? (A condition that is used to exclude cases when more than a set percentages of the deposited sum has been withdrawn, although the withdrawwn sum was of an irrelevant amount) Has the customer's sum of Outobund transactions within the last 30 days been between the set [Percentage_Low] and [Percentage_High]% of the cusotmer's sum of Inbound transactions that have been deposited within the same 30 days?
5	Structuring - Inbound	Significant number of low value incoming transactions just below a threshold	Was the transaction an Inbound transaction? Was the transaction at least of 9,950 (in base currency)?

			Was the transaction less than 10,000 (in base currency)? Has the customer had morethan a set [Number] of Inbound transactions within 7 days, that have each been at least 9,950 but less than 10,000 (in base currency)??
6	Structuring - Outbound	Significant number of low value outgoing transactions just below a threshold	Was the transaction an Outbound transaction? Was the transaction at least of 9,950 (in base currency)? Was the transaction less than 10,000 (in base currency)? Has the customer had morethan a set [Number] of Outbound transactions within 7 days, that have each been at least 9,950 but less than 10,000 (in base currency)??
7	Multiple Customers, One Counterparty (rename these rules)	Transactions to/from multiple customers from/to the same counterparty	Has the counterpatry transacted with more than a set [Number] of custoemrs within the last 30 days? Has this been the first transaction between this customer and counteraprty within the last 30 days?
8	Multiple Counterparties, One Customer	Transactions from multiple counterparties to the same customer	Has the customer transacted with more than a set [Number] of counterparties within the last 30 days? Has this been the first transaction between this customer and counteraprty within the last 30 days?
9	High Cumulative Amount - Outbound -	Significant number of transactions sent to a Counterparty over a short period	Was the transaction an Outbound transaction?

	Counterparty		Has the sum of Outbound transactions that this customer has sent to a single countearprty within 14 days been greater than a set [Amount]?
10	High Velocity - Inbound - Counterparty	High number of transactions received from a Counterparty over a short period	Was the transaction an Inbound transaction? Has the number of Inbound transactions that this customer has received from a single countearprty within 14 days been greater than a set [Number]?

Where an alert is generated either through a technological solution or via staff, the Compliance Officer or a delegate will conduct an investigation and document the results. These records will be maintained for a minimum of five years, regardless of whether or not a report is filed.

Unusual activity is escalated to the Compliance Officer via electronic transaction monitoring alerts in the IT system and manually escalated by staff based on their interaction with customers.

Transaction monitoring alerts are resolved by the Compliance Officer or a designate. Where there is insufficient information present to determine whether or not a transaction is suspicious, additional investigations are conducted. These may include follow-up with Trackon 's customers via phone and email. All investigations are logged electronically. Detailed notes are used to ensure that all process steps are clear. Detailed notes are completed for each alert, whether or not the transaction is deemed to be suspicious.

Where transactions are deemed to be suspicious, the Compliance Officer or a delegate will file an STR or ASTR with FINTRAC as soon as practicable after completing the measures required to establish reasonable grounds to suspect it may be related to money laundering or terrorist financing. Adjustments will also be made to the customer's risk level where required (if the customer has not already been designated as a high risk customer).

In some cases, the transaction may be suspended while Trackon contacts the customer to obtain additional information. Where the transaction is considered to be outside of Trackon 's risk tolerance (as defined by the Compliance Officer) and mitigating documents or information cannot be obtained, the transaction may be rejected by Trackon.

Regardless of whether or not a transaction that has been escalated to the Compliance Officer is deemed to be suspicious and reported to FINTRAC, a record of the investigation steps and rationale for the reporting decision will be maintained for a minimum of five years.

13.1 Enhanced Due Diligence & Enhanced Transaction Monitoring

For high risk customers and business relationships, the Compliance Officer or a delegate will conduct a full review of account activities. Where there is activity that is not consistent with the information on file about the customer and/or the stated purpose of the business relationship, the customer may be contacted for additional information.

Internet-based searches may also be performed at the time that enhanced due diligence is conducted. Specifically, the Compliance Officer or a delegate will make note of any findings related to:

- Money laundering or terrorist financing;
- Financial crime or serious crime;
- Discrepancies between publicly available information and information listed in the customer's profile; and/or
- Any other information that could affect Trackon 's assessment of the customer's risk profile.

Trackon will request additional clarification or information from a customer where there are discrepancies between the customer profile and publicly available information.

All follow up activities are documented, including customer responses for additional information.

All records are maintained electronically, for a minimum of five years.

14 PEP & HIO Checks

As of June 1, 2021, for customers with whom we have entered into a business relationship, or for international EFTs valued at CAD 100,000 or more, we must take reasonable measures to verify whether or not our customer is a politically exposed person (PEP), the head of an international organization (HIO) or the family member or close associate of a domestic PEP (collectively referred to as PEPs for the remainder of this section, unless otherwise specified). Currently, while not required, we conduct such checks at onboarding and periodically throughout the relationship with the customer.

PEPs may be foreign or domestic. The standards that apply will be slightly different, depending on whether the position that the person holds, or has held was within Canada (domestic) or outside of Canada (foreign).

Politically Exposed Foreign Persons (PEFPs), include anyone who holds or has held any of the following offices or positions in or on behalf of a foreign state:

- Head of state or head of government;
- Member of the executive council of government or member of a legislature;
- Deputy minister or equivalent rank;
- Ambassador, or attaché or counsellor of an ambassador;
- Military officer with a rank of general or above;
- President of a state-owned company or a state-owned bank;
- Head of a government agency;
- Judge of a supreme court, constitutional court or other court of last resort;
- Leader or president of a political party represented in a legislature; or
- Holder of any other prescribed office or position.

A person determined to be a foreign PEP, is forever a foreign PEP (even after they no longer hold the position).

Domestic Politically Exposed Persons (PEPs) include anyone that holds or has held one of the offices or positions on behalf of the federal government or a provincial government:

- Governor General, lieutenant governor or head of government;
- Member of the Senate or House of Commons or member of a legislature;
- Deputy minister or equivalent rank;
- Ambassador, or attaché or counsellor of an ambassador;
- Military officer with a rank of general or above;
- President of a corporation that is wholly owned directly by Her Majesty in right of Canada or a province;
- Head of a government agency;
- Judge of an appellate court in a province, the Federal Court of Appeal or the Supreme Court of Canada;
- Leader or president of a political party represented in a legislature; or
- Holder of any other prescribed office or position.

It also includes anyone that holds or has held one of the following offices or positions in a municipal government:

- Mayor.

A person ceases to be a domestic PEP 5 years after they have left office.

The head of an international organization is a person who is either:

- The head of an international organization established by the governments of states; or
- The head of an institution established by an international organization.

If the organization was established by means of a formally signed agreement between the governments of more than one country, then the head of that organization is a HIO. The head of an international organization or the head of an institution established by an international organization is the primary person who leads that organization, (i.e. a president or CEO).

In addition to PEFPs, PEPs and HIOs, we consider prescribed family members of such persons that we know are closely associated, for personal or business reasons, with a politically exposed person or HIO as high risk customers.

Prescribed family members include:

- Mother or father;
- Child;
- Spouse or common-law partner;
- Spouse's or common-law partner's mother or father;
- Brother;
- Sister; and
- Half-brother or half-sister (that is, any other child of the individual's mother or father).

Persons that are closely connected include:

- Business partners with, or who beneficially owns or controls a business with, a PEP or HIO;
- In a romantic relationship with a PEP or HIO, such as a boyfriend, girlfriend or mistress;
- Involved in financial transactions with a PEP or a HIO;
- A prominent member of the same political party or union as a PEP or HIO;
- Serving as a member of the same board as a PEP or HIO; or
- Closely carrying out charitable works with a PEP or HIO.

When an Trackon employee is aware that our customer is a PEFP, PEP, or HIO they will notify the Compliance Officer immediately so that they can perform a risk assessment and adjust the customer's risk ranking accordingly. Foreign PEPs, their family members and close associates are automatically considered a high risk customer.

When a risk assessment is required for a domestic PEP or HIO, the Compliance Officer will conduct a negative media search to determine if the domestic PEP should be considered low or high risk. Record of the risk assessment should be stored electronically.

In the event that a customer is determined to be a PEP or HIO, the Compliance Officer will ensure that Senior Management is aware of the account and has approved the customer or business relationship within 30 days of the PEP or HIO determination.

The Compliance Officer must keep a record after we have determined that a person is a PEFP, a high risk HIO, PEP, family member or close associate of one of these. The record must include:

- The office or position of the PEP or HIO;
- The name of the organization or institution of the PEP or HIO;
- The source of the funds;
- The date of determination;
- The name of the member of senior management who reviewed the transaction or approved keeping the account open; and
- The date the transaction was reviewed.

As a best practice we should also record the nature of the relationship between the client and the PEP or HIO, as applicable.

14.1 Senior Management Sign Off

In the case that we enter into a business relationship with a PEP or HIO, or they conduct an EFT transaction of CAD 100,000 or more, Senior Management must be notified, and sign-off documented within 30 days.

In order to document the decision and related rationale, the Compliance Officer sends an email to a Senior Officer and the Senior Officer responds. The Compliance Officer maintains a record of all such communication.

15 List Screening

We screen our active customer base[12] against publicly available lists of known terrorist individuals, such as the UNSC consolidated lists, the Consolidated Canadian Autonomous Sanctions List, the Public Safety Canada list and the Canadian Sanctions Justice for Victims of Corrupt Foreign Officials Act.

Screening is conducted automatically at the time of onboarding and periodically throughout the relationship with the customer. Where there is a pending alert (possible match), the onboarding cannot be completed.

Potential matches are resolved by the Compliance Officer or a delegate. The investigation of a potential match may require us to obtain additional information or documentation from the customer.

In the event that a list match is deemed to be a true match, the Compliance Officer will freeze the account and send reports to FINTRAC, CSIS and the RCMP.

The Compliance Officer will develop messaging for staff in dealing with the customer to explain the freezing of the accounts and conduct an investigation to

[12] Active customers include all customers that have completed a transaction within the past year.

determine whether there are any other clients affiliated with the listed person or entity.

If our customer is not a listed person or entity, or we are not in possession of property belonging to the customer, an STR or ASTR should still be filed if there are reasonable grounds to suspect terrorist financing and/or terrorist activity.

Records of all investigations, including the rationale for match/no match decisions, must be maintained for at least five years.

16 Record Keeping

Trackon must maintain specific records in order to meet legislative obligations. These records may be maintained either on paper or electronically. The Compliance Officer will ensure that records retention policies and processes are sufficient in:

- Maintaining records required under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and its enacted regulations for at least five years; and
- Storing all official records in a form and manner that allows these records to be retrieved in a timely manner.

The AML & CTF Policy includes a listing of the records that must be maintained.

Generally, if FINTRAC makes a request for any such records, the information must be delivered to them within 30 calendar days.

17 Compliance Program Monitoring and Testing

Trackon should ensure the adequacy, adherence, and effectiveness of day-to-day AML & CTF compliance procedures, using a risk-based approach. Testing should identify any patterns, themes or trends in compliance controls that may indicate weaknesses. Compliance control processes should include verification of key information (including any significant remediation activities stemming from regulatory exams and effectiveness reviews).

This validation is completed on a rotational basis and is undertaken using a risk-based approach. Testing includes both operational and independent oversight AML & CTF compliance controls.

Each year, the Compliance Officer (or designate) will plan and execute such testing, considering risk, business model changes and operational realities. If possible, the testing should be conducted by someone outside of the Compliance department or someone not involved in the task that is being tested.

Where deficiencies are observed, the Compliance Officer (or designate) will ensure remediation action plans are created and tracked. Depending on the nature of the

deficiencies observed, the Compliance Officer may report findings to Senior Management.

18 Appendix: Sample Compliance Officer Quick Reference

This chart has been developed to assist the Compliance Officer in meeting time sensitive requirements. It is not intended to be a full listing of all AML and CTF Compliance Responsibilities.

18.1 AML & CTF Program Maintenance

There are 5 key elements that must all be documented:

1) **Compliance Officer**: a person that is responsible for your compliance program, including communication with your regulators.
2) **Policies & Procedures**: documents that explain what you must do, and how you are meeting these obligations.
3) **Risk Assessment**: a document that describes and quantifies the risk that your business could be used to launder money or finance terrorism, as well as the controls that you have in place to prevent this from happening.
4) **Training**: for all staff that handle customers and/or transactions, this must be delivered regularly (at least annually, and more often if there are changes to Canadian legislation or your business model).
5) **AML Compliance Effectiveness Review**: a review is like an audit for compliance. The review must test all elements of your compliance program, as well as your operations (what you are actually doing). All reviews should include a formal report that describes the methodology and results.

The AML Compliance program should be updated at regular intervals. This chart can be used to help you keep track of upcoming deadlines.

What?	When?	Last Completed	Next Due Date
Trackon Anti-Money Laundering and Counter Terrorist Financing Policy	Annual	August 2021	August 2022
Trackon Anti-Money Laundering and Counter Terrorist Financing Procedures for Compliance Staff	Annual	August 2021	August 2022
Trackon Anti-Money Laundering and Counter Terrorist Financing Procedures for All Staff	Annual	August 2021	August 2022
Trackon Risk Assessment	Annual	August 2021	August 2022
Training Program	Annual	Q4 2020	Q4 2021
AML Compliance Effectiveness Review	Every Two Years	October 2022	October 2024
Management Sign-off on Review	Within 30 days of the review's issue	TBC – based on issue date of first review report.	

18.2 Training

You should keep a log of all AML and CTF Compliance Training (including training sessions that you take to keep your knowledge sharp). This format can be used to keep track of the training that took place within our organization. The content section should include how the training was delivered and what was covered. This can be a brief bullet point summary.

The category section should include the type of training (Annual Staff Training, New Hire Training, Compliance Officer Training, etc.) that was provided.

These records may be shared with reviewers, financial service partners and FINTRAC. They should be kept up to date at all times and go back at least two years.

Content	Delivered by (Person, Role & Organization)	Delivery Method (In person, webinar, phone, etc.)	Plan Date	Completed Date	Date Persons Trained	Type of Training

18.3 Reporting

The reports that you submit to FINTRAC and other agencies must be submitted within certain timeframes. Reports submitted to FINTRAC, with the exception of Terrorist Property Reports (TPRs) can be submitted via FINTRAC's electronic reporting system F2R[13].

Report Type	Applicability	Timing	Reported To	How is it submitted?
Electronic Funds Transfer Report (EFTR)	Applies to Trackon	5 working days from the transaction date	FINTRAC	Electronically via F2R

[13] https://www.fintrac-canafe.gc.ca/reporting-declaration/guide/sys-eng

Report Type	Applicability	Timing	Reported To	How is it submitted?
Suspicious Transaction Report (STR)	Applies to Trackon	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)	Applies to Trackon	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)	Applies to Trackon	Immediately	FINTRAC, RCMP, CSIS	On paper (via fax)

If reports are submitted to FINTRAC via F2R, you will receive an electronic confirmation that the report has been received. Keep a copy (either paper or electronic) for your records.

There are two ways to send a paper report to FINTRAC in such a way as to obtain an acknowledgment of receipt:

1) Fax: 1-866-226-2346; or
2) Registered mail to the following address: Financial Transactions and Reports Analysis Centre of Canada, Section A, 234 Laurier Avenue West, 24th floor, Ottawa ON, K1P 1H7, Canada

You may send your report by regular mail to the FINTRAC address above. However, FINTRAC will not send you any acknowledgement when your paper report has been received[14].

Terrorist Property Reports must also be sent to the Royal Canadian Mounted Police (RCMP) and the Canadian Security Intelligence Service (CSIS) by fax[15]:

[14] https://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/Guide5/5-eng
[15] https://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/Guide5/5-eng

- RCMP, Anti-Terrorist Financing Team, unclassified fax: 613-825-7030
- CSIS Financing Unit, unclassified fax: 613-369-2303

18.4 Record Keeping

It is important to keep records of everything that you are doing to meet your compliance requirements. Certain records are called out specifically within the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFR) and its enacted regulations. These include:

- 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 related to 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)[16];
- 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;

[16] Effective: June 1, 2021.

- 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.

19 Appendix: Sample Compliance Remediation & Update Log

This sample log format can be used to track the remediation of any AML or CTF compliance issues. Issues are generally discovered in five ways:

1) Annual program review;
2) Self-discovery;
3) AML Compliance Effectiveness Review;
4) FINTRAC Examination; or
5) Other (Include all details of compliance issue discovery).

The issues that pose the greatest risk to our company should be considered the highest priority for remediation. Any issues that form part of a formal findings letter from FINTRAC will also be considered the highest priority.

This log is maintained by the Compliance Officer or a designate and can be used to provide updates to Senior Management and the Board of Directors (if applicable).

Reason for Update	**Date of Update**	**Description of the Update**	**Documents Updated**	**Compliance Officer Approval**	**Updated Documents Shared with All Staff**	**Additional Notes (If Applicable)**

The content in this log may be in point form, but should be detailed enough that the issue and the steps taken to fix it are clear to someone that was not involved in the process. The cause of the issue should be included in the description if the cause is known.

This log can also be used by the Compliance Officer to track the updates to the AML Compliance program documents. If the program is reviewed and no significant changes are made to a document, then there should still be a line item that states that the program was reviewed, and no significant changes were made.

This document may be used to evidence to reviewers and regulators that regular program updates have occurred.

20 Appendix: Sample AML Compliance Effectiveness Review Form For Management Sign-Off

The AML Compliance Effectiveness Review Report conducted by (name of the person or company that conducted the review) _____

_____

on (date the final report was issued) _____

has been reviewed by the management team and discussed with the Compliance Officer.

On behalf of the Senior Management Team:

Senior Management Name & Title: _____

Date: _____

Signature: _____

Compliance Officer Name: _____

Date: _____

Signature: _____

The Compliance Officer maintains this document in our official records related to AML Compliance Effectiveness Reviews.

21 Appendix: Sample Training Plan & Log

This log is a sample and does not contain information about Trackon 's actual training sessions.

Content	Delivered by (Person, Role & Organization)	Delivery Method (In person, webinar, phone, etc.)	Plan Date	Completed Date	Date Persons Trained	Type of Training	Notes
• What is money laundering? • What is terrorist financing? • Who is FINTRAC? • Who is the AMF? • What is a MSB? • What are our responsibilities under Canadian law? ○ Compliance Officer ○ AML Program ○ Risk Assessment ○ AML Compliance Effectiveness Review ○ Training ○ Reporting ○ Recordkeeping ○ Identifying Customers (individuals, organizations, face to face, non face to face) ○ Customer and Business Relationship Risk ○ Transaction							

Content	Delivered by (Person, Role & Organization)	Delivery Method (In person, webinar, phone, etc.)	Plan Date	Completed Date	Date Persons Trained	Type of Training	Notes
Monitoring • Who is our Compliance Officer? • What do I do if I believe that money laundering or terrorist financing is taking pace? • What indicators should I look for in our transactions and customer behaviours?							

Compliance Officer- Rishi Dubey

Signature-

Date- 29/07/2022