AML/CFT Compliance Program for FINTRAC-Registered MSB

TABLE OF CONTENTS

Instruction 3
Definitions 4
Senior Officer Approval 5
Last Modified . 5

Compliance Policies and Procedures 5
Compliance Officer 5
Risk Assessment 5
Business-Based Risks 6
Relationship-Based Risk (Clients and Business Relationships) 21
Risk Tolerance 21
Risk-Reduction Measures and Key Controls 21
Evaluating Residual Risk 21
Compliance Training Program 22
Plan for the Compliance Program Effectiveness Review 22

Know Your Client (KYC) 24
When to Verify the Identity of Persons and Entities 24
Methods to Verify the Identity of Persons and Entities 26
Business Relationship Requirements 31
Beneficial Ownership Requirements 33

Reporting 35
Suspicious Transaction Reports (STR) 35
Terrorist Property Reports (TPR) 39
Large Cash Transaction Reports (LCTR) 40
Large Virtual Currency Transaction Reports (LVCTR) 40
Electronic Funds Transfer Reports (EFTR) 42
24-hour Rule 43

Record Keeping 44
Large Cash Transaction Records 44
Large Virtual Currency Transaction Records 45
Records of Transactions of CAD 3,000 or More 45
Records of Remitting or Transmitting CAD 1,000 or More 46
Records of Electronic Funds Transfers 46
Records of Virtual Currency Transfers 46
Foreign Currency Exchange Transaction Records 47
Virtual Currency Exchange Transaction Records 47

Internal Memoranda and Service Agreement Records 47
Exceptions for Virtual Currency 48

Travel Rule 48
Ministerial Directives 49

Schedule 1 – Appointment or Reappointment of the Compliance Officer 50
Schedule 2 – Risk Assessment 51
Schedule 3 – Know Your Client (KYC) 53
Schedule 4 – Reporting (ETF and VC Records and Reporting) 57
Schedule 5 – Transaction Records 59
Schedule 6 – Ministerial Directives 64
Schedule 7 – Client Verification Discussion 65

Approved
by the Director of **1523766 B.C. LTD.**

01 of February, 2026

Signed by:
A732E9930CE24C3...

Viktor Postoialkin

1523766 B.C. LTD. (the "**Company**") provides the following business services:

The Company is registered with FINTRAC as a Money Services Business (MSB). For AML/CFT program purposes, the Company maintains policies and controls applicable to MSB activities that may be registrable under Canadian law. In its current operating model, the Company provides digital asset–related services where applicable, and supports fiat-to-virtual asset and virtual asset-to-fiat conversion processes, which may be executed either directly by the Company or by independent, regulated third-party service providers, depending on the specific product configuration, counterparty, and jurisdiction.

The Company supports a culture of compliance and strives to meet all obligations required to operate as a Money Services Business. The Company maintains a proactive compliance culture and promptly addresses any identified deficiencies in accordance with applicable regulatory guidance.[1]

For the avoidance of doubt, the Company may, in limited and controlled circumstances, operationally initiate and execute fiat-to-virtual asset and virtual asset-to-fiat transactions (only on electronic non cash basis).

Where such execution is performed directly by the Company, the Company assumes responsibility for applicable AML/CFT, sanctions, transaction monitoring, reporting, and recordkeeping obligations in accordance with the PCMLTFA and its implementing regulations.

Where execution is performed by third-party service providers, such providers act in their own name and under their own regulatory obligations.

This document's purpose is to meet the compliance policies and procedures requirements for a Money Service Business ("**MSB**"), in accordance with the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and its implementing regulations.

Instructions

These instructions are intended to help the reader understand the methodology and structure of the Compliance Program and Polices. These instructions are for general information purposes only, for use by the Company, and do not constitute legal or other professional advice or an opinion of any kind.

The document is structured with headings to help guide the reader based on topic and action. For example, the main headings are Compliance Polices and Procedures, Risk Assessment, KYC etc. Below each heading are sub-headings that provide more rules and policies (required by law) that must be followed. Generally sub-sub-headings will have "Compliance Controls" – these are generally instructing the reader that something must be recorded or written down (usually in the Schedules) in order to comply with the relevant laws and regulations.

With respect to the Schedules, the tables in each Schedule are largely examples that summarize requirements in table formats. It would be prudent to keep client data in a separate password protected location. Please note: records must be kept in such a manner that they can be accessed (in physical copy also) within 30 days of a request from FINTRAC as stated in the Record Keeping section of this document – for more information about this requirement see the Record Keeping section below.

Definitions

In this document, unless the context otherwise requires:

[1] https://www.fintrac-canafe.gc.ca/guidance-directives/exam-examen/vsdonc/1-eng.

a) "**Compliance Program Effectiveness Review Date**" means a review of the Company's compliance program no less than every two years starting from the Commencement Date.[2] For clarity, if the Commencement date is February 16, 2025, then the review will occur no later than February 16, 2027, February 16, 2029, etc. The Compliance Officer will add a reminder in their calendar (Outlook, Google etc.) for each of the dates.

b) "**Commencement Date**" means ***June 6, 2025*** in which this document comes into force.

c) "**Compliance Officer**" means the person or delegate(s) of the Compliance Officer who are responsible for implementing and enforcing the Compliance Program.[3]

d) "**Compliance Policies and Procedures" or "this document**" means this document, including any Schedules and any supplementary policies or procedures established by the Company from time to time.

e) "**Compliance Program**" means the policies and procedures, risk assessment, ongoing training program and training plan that a Reporting Entity is legally required have pursuant to the relevant laws and regulations and is approved by a Senior Officer.[4]

f) "**Financial Entity**" takes the same meaning as stated in the PCMLTFR.

g) "**HIO**" means head of an international organization.

h) "**Identifier**" means an employee/officer of the Company who is conducting KYC procedures.

i) "**PEP**" means politically exposed person.

j) "**PCMLTFA**" means Proceeds of Crime (Money Laundering) and Terrorist Financing Act.

k) "**PCMLTFR**" means Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations.

l) "**Public Body**" takes the same meaning as stated in the PCMLTFR.

m) "**Reporting Entity or RE**" means the Company.

n) "**Residual Risk**" means the resulting risk after accounting for risk mitigation measures and controls that are in place to address inherent risk. Types of residual risk include:

a. Tolerated risks: These are risks that are accepted without additional mitigation measures.

b. Mitigated risks: These are risks that are reduced by mitigation measures but not eliminated. In practice, the controls put in place may fail from time to time (for example, you do not report a transaction within the prescribed timeframe because your transaction review process has failed).

o) "**Senior Officer**" means an individual as defined in the PCMLTFR.

Certain sections of this document describe statutory obligations that apply only when the corresponding activity is conducted. Where a specific activity is not part of the Company's current operations, the Company treats the relevant section as "not applicable in practice" while retaining it for completeness and future scalability.

See FINTRAC's Guidance Glossary for definitions of other key terms.

Senior Officer Approval

Officer Name	Title	Date
Perpindervir Singh Patrola	Director	June 6, 2025

[2] PCMLTFR, SOR/2002-184, s. 156(3).
[3] PCMLTFR, SOR/2002-184, s. 156(1)(a).
[4] PCMLTFA, S.C. 2000, c 17, s. 9.6(1); PCMLTFR, SOR/2002-184, s. 156(1)(b).

Viktor Postoialkin	Director	November 13, 2025

Last Modified

November 13, 2025- Change in Compliance Officer, Director and Shareholder of the Company

Compliance Policies and Procedures

Compliance Officer

The Compliance Officer is responsible for implementing and enforcing the Compliance Program.[5] Schedule 1 designates the Company's Compliance Officer.[6]

The appointment and reappointment of the Compliance Officer will occur every two years starting on the Compliance Program Effectiveness Review Date, unless otherwise needed. An additional review[7] may be needed in situations such as:

- when there are changes to the business model;
- upon acquiring a new portfolio or set of clients;
- when there are new Ministerial Directives;
- when employees are hired;

The Compliance Officer will:

- have the necessary authority and access to resources in order to implement an effective Compliance Plan and Policies and make any desired changes;
- have knowledge of the Company's business's functions and structure;
- have knowledge of the Company's business sector's money laundering ("**ML**")/Terrorist Financing ("**TF**") risks and vulnerabilities as well as ML/TF trends and typologies; and
- understand the Company's business sector's requirements under the PCMLTFA and associated Regulations.[8]

The Compliance Officer may delegate certain duties to other employees or third parties, as required. However, the Compliance Officer remains responsible for the implementation of the compliance program.[9] While the compliance officer is appointed, it is the Company's responsibility to meet its compliance program requirements under the PCMLTFA and associated regulations[10] as amended or replaced from time to time.[11]

The Compliance Officer must be aware of the FINTRAC assessment manual to understand what happens during a FINTRAC audit.[12]

Risk Assessment[13]

The purpose of the Risk Assessment is to ensure that the Company remains compliant with the relevant legislation and to assess the risks linked to the Company's business activities and clients.

---

[5] PCMLTFR, SOR/2002-184, s. 156(1)(a).

[6] The owner or the operator of the small business can be the compliance officer: https://fintrac-canafe.canada.ca/guidance-directives/compliance-conformite/Guide4/4-eng#s2.

[7] Expectations for Step 6 — Review your RBA, citing PCMLTFR, SOR/2002-184, ss. 156(1)(f) and 156(3).

[8] https://fintrac-canafe.canada.ca/guidance-directives/compliance-conformite/Guide4/4-eng#s2.

[9] Ibid.

[10] As of March 01, 2022, regulations made under the act include: Cross-border Currency and Monetary Instruments Reporting Regulations (SOR/2002-412), Financial Consumer Protection Framework Regulations [Not in force] (SOR/2021-181), Proceeds of Crime (Money Laundering) and Terrorist Financing Administrative Monetary Penalties Regulations (SOR/2007-292), Proceeds of Crime (Money Laundering) and Terrorist Financing Registration Regulations (SOR/2007-121), Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (SOR/2002-184), Proceeds of Crime (Money Laundering) and Terrorist Financing Suspicious Transaction Reporting Regulations (SOR/2001-317).

[11] Ibid.

[12] https://www.fintrac-canafe.gc.ca/guidance-directives/exam-examen/cam/cams-eng#s1.

[13] PCMLTFR, s. 156(1)(c), and PCMLTFA, s. 9.6(2).

The Company follows a risk-based approach (RBA) cycle in order to identify and mitigate ML/TF risks.

RBA Cycle

A two-pronged assessment must be conducted during an RBA cycle exercise: A business-based risk assessment and relationship-based risk assessment (together, the "**Risk Assessments**").[14] The policies and procedures outlined below help to inform an individual who is performing the Risk Assessments as set out in Schedule 2.

Compliance Control

Risk Assessments will be conducted prior to the Commencement Date. The original Risk Assessment should be reviewed for accuracy approximately 6 months after the Commencement Date. After that, Risk Assessments must be conducted at least every two years starting from the Commencement Date. For clarity, if the Commencement Date is June 6, 2025, then the Risk Assessments must occur before December 6, 2025, June 6, 2027, June 6, 2029, etc.

Areas that are identified as high-risk must be outlined in Schedule 2 as either business or relationship-based risks, including mitigation controls for areas that are identified as high-risk as prescribed in the Compliance Control sections.

Business-based risks[15]

The first stage in the risk assessment process involves identifying the business-based risks, as set out below. These risks include: (i) products, services and delivery channels; (ii) geographic risks; (iii) affiliate risks; (iv) new developments and technologies; and (v) any other relevant factor (other than client and relationship risk).

[14] PCMLTFR, SOR/2002-184, s. 156(1)(c)(i).
[15] PCMLTFR, SOR/2002-184, s. 156(1)(c)(i).

Compliance Control

Products, services and delivery channels [16]

The risk assessment must consider all products, services and delivery channels that are provided and used during the course of business.

Compliance Control

The Compliance Officer must assess the products, services and delivery methods before their adoption and record the assessment in the business-based risk assessment table in Schedule 2.

Business-based examples of higher risk indicators and considerations for products, services and delivery channels[17] *The examples below are included for regulatory completeness and may not be applicable to the Company's operating model.*	
Examples of higher risk indicators	**Considerations**
Products and services, such as: ● EFTs, ● electronic cash (for example, stored value cards and payroll cards) ● products offered through the use of intermediaries or agents ● private banking ● mobile applications	Legitimate products and services can be used to mask the illegitimate origins of funds, to move funds to finance terrorist acts or to hide the true identity of the owner or beneficiary of the product or service. Assess the market for your products and services (for example, corporations, individuals, working professionals, wholesale or retail etc.), as this may have an impact on the risk. Do the products or services you provide allow clients to conduct business or transactions with higher risk business segments? Could our clients use the products or services on behalf of third parties? Products and services offered that are based on new developments and technologies such as electronic wallets, mobile payments, or virtual currencies, may be considered higher risk as they can transmit funds quickly and anonymously.
Delivery channels, such as transactions for which an individual is not physically present, including: ● agent network ● online trading	Delivery channels may have a higher inherent risk as the Company may not offer face-to-face transactions, and clients can initiate a business relationship online. This is especially true if the Company chooses to rely on an agent (that may or may not be covered by the PCMLTFA) to verify the identity of your clients. For the purpose of the PCMLTFA, REs are accountable for the activities conducted by their agents.

[16] PCMLTFR, SOR/2002-184, s. 156(1)(c)(ii). https://www.fintrac-canafe.gc.ca/guidance-directives/compliance-conformite/rba/rba-eng.

[17] https://www.fintrac-canafe.gc.ca/guidance-directives/compliance-conformite/rba/rba-eng#a2T1, Annex2, Table 1.

	In addition, new delivery channels (for example, products or services such as virtual currency) may pose inherently higher ML/TF risks due to the anonymous nature of transactions when conducted remotely.

Geography[18]

In conducting a risk assessment, the Compliance Officer must consider the geographic locations applicable to the Company's business.

Compliance Control

The Compliance Officer must assess the geographic locations where the Company is conducting business, including when the Company changes its place of business or where the Company solicits new clients in a different location (i.e., advertising in another province or country), and record the assessment in the business-based risk assessment table in Schedule 2. The Company should also consider the locations of any beneficiaries of its transactions. Among other things, the Compliance Officer may note a greater number of problematic transactions originating from clients located in a particular region in Canada.

Business-based examples of higher risk indicators and considerations for geography[19]	
Examples of higher risk indicators	**Considerations**
Border-crossings: ● air (for example, airports) ● water (for example, ports, marinas) ● land (for example, land border-crossings) ● rail (for example, passenger and cargo)	If the Company's business is near a border-crossing, it may have a higher inherent risk because it may be the first point of entry into the Canadian financial system. This does not mean that the Company should assess all activities and clients as posing a high-risk if the business is located near a border-crossing or major airport. FINTRAC is simply highlighting that such businesses may want to pay closer attention to the fact that their geographical location may impact their business. For example, this could be done through training so that staff better understand the placement stage of ML and its potential impacts.
Geographical location and demographics: ● large city ● rural area	The Company's geographical location may also affect its overall business risks. For example, a rural area where it's known clients could present a lesser risk compared to a large city where new clients and anonymity are more likely. However, the known presence of organized crime would obviously have the reverse effect. Some provincial governments have interactive maps on crime by regions, which may inform your risk assessment, such as Québec (http ://geoegl.msp.gouv.qc.ca/dpop/) (in French

[18] PCMLTFR, s. 156(1)(c)(iii). https://www.fintrac-canafe.gc.ca/guidance-directives/compliance-conformite/rba/rba-eng.

[19] https://www.fintrac-canafe.gc.ca/guidance-directives/compliance-conformite/rba/rba-eng#a2T1, Annex2, Table 2.

	only). Other websites provide good information on crime in Canada, including statistics and trends by province. For example, crimes, by type of violation, and by province and territory: http://www.statcan.gc.ca/tables-tableaux/sum-som/l01/cst01/legal50b-eng.htm.
The business is located in an area known for having a high crime rate	High crime rate areas should be indicated in the overall assessment of the business as they may present higher ML/TF risks. The Company does not need to consider every client from a higher crime area as posing a high-risk. However, the Company should be aware of how these areas can affect client activities. Searching online for crime related statistics in your city or area should result in sources the Company can consult (such as municipal police departments or other databases). For example, the following websites provide information on crime in cities or neighborhoods: ● Vancouver: http://vancouver.ca/police/organization/planning-research-audit/neighbourhood-statistics.html ● Edmonton: http://crimemapping.edmontonpolice.ca/ ● Calgary: http://www.calgary.ca/cps/Pages/Statistics/Calgary-Police-statistical-reports.aspx# ● Winnipeg: https://winnipeg.ca/police/crimestat/viewMap.aspx ● Toronto: http://www.torontopolice.on.ca/statistics/stats.php ● Ottawa: https://www.ottawapolice.ca/en/crime/crime-stats.aspx ● Montreal: https://ville.montreal.qc.ca/vuesurlasecuritepublique/ (in French only) ● Halifax: https://www.halifax.ca/fire-police/police/crime-mapping Please note that statistics such as those found under the links above are not necessarily linked to ML/TF offences. They provide a general idea of where crime occurs in a given city.
Events and patterns	Depending on the clientele, are there events or patterns (either domestic or international) that could affect the business? For example, the Company may be dealing with clients that have a connection to high-risk jurisdictions or with jurisdictions that are dealing with a specific event (such as terrorism, war, etc.). The Company does not need to classify all activities and clients as posing a high-risk in relation to an event, conflict or high-risk jurisdiction. However, the Company should be aware of these circumstances in order to determine whether a transaction becomes unusual or suspicious.
Connection to high-risk countries: ● Special Economic	International conventions and standards may affect mitigation measures aimed at the detection and deterrence of ML/TF. The Company should identify certain countries as posing a high-risk for ML/TF based on (among other things) their level of corruption, the prevalence of crime in their region, the weaknesses of their ML/TF control regime, or the fact that they are listed in the advisories of competent authorities such as the FATF or FINTRAC. If the Company

Measures Act (SEMA) ● FATF list of High-Risk Countries and Non-Cooperative Jurisdictions ● UN Security Council Resolutions ● Freezing Assets of Corrupt Foreign Officials Act (FACFOA) sanctions	and/or the Company's clients have no connection to these countries, the risk will likely be low or non-existent. If the Company transfers funds to or receive funds from a country subject to economic sanctions, embargoes or other measures, the Company should consider that country as high-risk. For example, the Company should be aware of: ● Canadian Economic Sanctions: https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/index.aspx?lang=eng ● High-Risk and Non-Cooperative Jurisdictions: http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/ ● FINTRAC Advisories: https://fintrac-canafe.canada.ca/new-neuf/1-eng ● Security Council Resolutions: https://www.un.org/securitycouncil/content/resolutions ● Freezing Assets of Corrupt Foreign Officials Act sanctions: https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/current-actuelles.aspx?lang=eng

New Developments and Technologies[20]

The Company operates in an industry where technology and modes of delivery are rapidly changing. The Compliance Officer must identify the risks associated with new developments and the adoption of new technologies.

Business-based examples of higher risk indicators and considerations for new developments and technologies[21]	
Examples of higher risk indicators	**Considerations**
● Payment methods ● Methods of communication or identification: ○ Phone ○ Email ○ chat applications ○ electronic information exchange ○ document signing on a cloud server such as DocuSign	The Company's overall inherent risks may be higher if the Company's business adopts new technologies or operates in an environment subject to frequent technological change. New technologies may include systems or software used in your organizations ML/TF mitigation strategy such as a transaction monitoring system or a client onboarding or identification tool. The implementation of new technologies such as mobile payment services could subject the business to a wide range of vulnerabilities that can be exploited for ML. For example, the use of new technologies can result in less face-to-face interaction with customers, allowing more anonymity and possibly increasing ML/TF risks. Therefore, when the Company implements new technology in the business, it is important to

[20] PCMLTFR, s. 156(1)(c)(v). https://www.fintrac-canafe.gc.ca/guidance-directives/compliance-conformite/rba/rba-eng. https://www.fintrac-canafe.gc.ca/guidance-directives/compliance-conformite/rba/rba-eng.

[21] https://www.fintrac-canafe.gc.ca/guidance-directives/compliance-conformite/rba/rba-eng#a2T1, Annex2, Table 4.

	assess the associated ML/TF risks and document and implement appropriate controls to mitigate those risks. **Payment methods** The payment method examples listed in the Indicators column can be used to transfer funds faster and anonymously, which can increase ML/TF risks. If the business offers such products, services and delivery channels, assess them for ML/TF risks. **Methods of communication or identification** The Company's business may communicate with clients through means other than the telephone and email or clients may use new ways to communicate with the Company or identify themselves to the Company. Communications means are evolving continually and can affect your overall inherent risks.
developments	der acquisitions, changes to the Company's business model, or ess restructuring.

Compliance Control
The Compliance Officer must assess the new technology and business development before the adoption of the new technology(s) or business development(s) and record them in a documented risk assessment. Consider the matters covered in the business-based risk assessment table in Schedule 2.

Other Relevant Factors[22]
The regulatory landscape is fluid; therefore, the Compliance Officer will assess, on a continual basis, the relevant laws and regulations associated with the Company's business.

Compliance Control
The Compliance Officer should subscribe to FINTRAC's mailing list and establish an alert system such as Google Alerts for key words such as: "Special Economic Measures Act", "FINTRAC", and "Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)". The purpose of the foregoing is to alert the Compliance Officer to potential, pending and actual changes in relevant legislation, regulations and policies.

This document should be updated to address changes in relevant legislation, regulations and policies.

Business-based examples of higher risk indicators and considerations for other relevant factors[23]	
Examples of higher risk indicators	**Considerations**

[22] PCMLTFR, s. 156(1)(c)(v).
[23] https://www.fintrac-canafe.gc.ca/guidance-directives/compliance-conformite/rba/rba-eng#a2T1, Annex2, Table 5.

● Special Economic Measures Act (SEMA) ● ministerial directives ● regulators ● national risk assessment	Restrictions such as economic sanctions can impact the business by: ● prohibiting trade and other economic activity with a foreign market; ● restricting financial transactions such as foreign investments or acquisitions; or ● leading to the seizure of property situated in Canada. These restrictions may apply to dealings with entire countries, regions, non-state actors (such as terrorist organizations), or designated persons from a target country. As part of the risk assessment, the Compliance Officer must also take into consideration ministerial directives. The Company's sector's regulator may also impose additional measures (for example, provincial, prudential, etc.). The national risk assessment assesses the ML/TF risks in Canada, which may help identify potential links to the business activities.
Trends, typologies and potential threats of ML/TF: ● ML/TF methods used in specific sectors ● ML/TF actors including organized crime groups, terrorist organizations, facilitators, etc. ● corruption and other crimes	Trends and typologies for the Company's respective activity sector may include specific elements of risks that the business should consider. For example: ● FATF Methods and Trends (not available for all activity sectors): http://www.fatf-gafi.org/topics/methodsandtrends/). ● Public Safety Canada — Organized Crime: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cmbtng-rgnzd-crm/index-en.aspx ● Transparency International (rank by country): https://www.transparency.org/country/# Not all elements listed in these trends and typologies will affect the Company, but the Company should be aware of the high-risk indicators that may have an impact on the business.
Business model: ● operational structure ● third party and/or service providers	To determine if risks exist in relation to this element, the Company must consider the business model, the size of the business, and the number of branches and employees. For example: ● A business with hundreds of branches and thousands of employees will present different risks than a business that has one location and two employees. ● A business with a high employee turnover. These examples highlight the fact that the Company's risk assessment should be related to other compliance program elements, such as training. Training should give employees an

	understanding of the reporting, client identification, and record keeping requirements, and an understanding of the penalties for not meeting those requirements. If the Company has numerous branches or a high employee turnover in the future, the training program should address these risks. It is also important to remember that although the use of a third party service provider can be a good business practice, the service provider may need to comply with the Company's obligations under the PCMLTFA and associated Regulations. The Company must consider how service providers are functioning.

Matrix and Rating
The Company may engage in a three-level scoring system, displayed below.

Compliance Control
As the business matures, this scoring system should change and must be reviewed during any reviews of the Compliance Program.

Examples of risk segregation for a business-based risk assessment[24]

Factors	**Low**	**Medium**	**High**
Products & services —Electronic transactions	No electronic transaction services	The Company has some electronic transaction services and offers limited products and services	The Company offers a wide array of electronic transactions services
Products & services —Currency transactions	Few or no large transactions	Medium volume of large transactions	Significant volume of large or structured transactions
Products & services — EFTs	Limited number of funds and transfers of low value for clients and non-clients Limited third-party transactions and no foreign funds transfers	Regular funds transfers and transfers of medium value Few international funds transfers from personal or business accounts with typically low-risk countries	Frequent funds transfers and transfers of high value from personal or business accounts, to or from high-risk jurisdictions and financial secrecy jurisdictions

[24] https://www.fintrac-canafe.gc.ca/guidance-directives/compliance-conformite/rba/rba-eng#a3T6.

Products & services (business model) — International exposure	Few international accounts or very low volume of transactions in international accounts	Some international accounts with unexplained transactions	High number of international accounts with unexplained transactions
Geography (location) —Prevalence of crime	All locations are in an area known to have a low crime rate	One or a few locations are in an area known to have an average crime rate	One or a few locations are in an area known to have a high crime rate and/or criminal organization(s)
Technology	No new technologies are used to conduct the business in terms of products ,services to clients and used to contact clients	Certain areas of the business use new technologies to contact clients but products, services and payment methods do not use new technologies	The majority of products, services, delivery channels, payment methods and client contact methods use new technologies.

Rating and <u>likelihood</u> of the ML/TF risk[25]

Rating	**Likelihood of ML/TF risk**
High	High probability that the risk is present
Medium	Reasonable probability that the risk is present
Low	Unlikely that the risk is present

Rating and <u>impact</u> of the ML/TF risk[26]

Rating	**Likelihood of ML/TF risk**
High	The risk has severe consequences

[25] https://www.fintrac-canafe.gc.ca/guidance-directives/compliance-conformite/rba/rba-eng#annex4.
[26] https://www.fintrac-canafe.gc.ca/guidance-directives/compliance-conformite/rba/rba-eng#annex4.

Medium	The risk has moderate consequences
Low	The risk has minor or no consequences

Relationship-based risk (clients and business relationships)[27]

Compliance Control

After the Company completes its business-based risk assessment, it can focus on the risks presented by clients and business relationships. To conduct a relationship-based risk assessment, the Company must identify the inherent risks of ML/TF for its clients. T

It is important to compare the clients' expected activity to the clients' actual activity, and determine whether the actual activity reflects elevated, or different risks than the expected risks. A risk rating methodology is often a helpful tool to assess relationship-based risks.

The matters below should be considered as part of the risk assessment.

Products, services and delivery channels[28]

The Compliance Officer must review the clients' use of products, services and delivery channels for ML/TF.

Compliance Control

In the relationship-based risk assessment, the Compliance Officer considers the products, services and delivery channels that clients are using and the impact they have on the clients' overall risk. Some helpful considerations are provided in Schedule 2.

Products will have a higher inherent risk when there is client anonymity or when the source of funds is unknown. The assessment focuses on risks relevant to the Company's services and excludes correspondent banking, payment execution, and fund transmission activities to the extent such activities are not performed by the Company. Delivery channels will have either to face-to-face or online interactions with clients. Celivery channels that feature little or no face-to-face interaction allow for increased risk in the form of client anonymity and in many cases, transactional speed.

Where possible, it is advisable that the Compliance Officer complete a review of products and services with the employees who handle them to ensure the completeness of the risk assessment.

Relationship-based examples of higher risk indicators and considerations for products, service and delivery channels[29]	
Examples of higher risk indicators	**Considerations**
Clients that use some products and services offered through non-face-to-face channels or	Non-face-to-face transactions can make it more difficult to verify the identity of clients. Using intermediaries or agents may increase inherent risks, because intermediaries or agents may lack adequate supervision

[27] PCMLTFR, SOR/2002-184, s. 156(1)(c)(i).
[28] https://www.fintrac-canafe.gc.ca/guidance-directives/compliance-conformite/rba/rba-eng.
[29] https://www.fintrac-canafe.gc.ca/guidance-directives/compliance-conformite/rba/rba-eng#a2T1, Annex2, Table 9.

use intermediaries, agents or introducers.	if they are not subject to anti-money laundering and anti-terrorist financing (AML/ATF) laws or measures. It is important to note that under the PCMLTFA, the Company is accountable for the activities conducted by all its agents. As a result, the Company must ensure that they meet all compliance obligations on an ongoing basis. Furthermore, the Company should have due diligence processes in place (such as background checks and ongoing monitoring) to lessen the risk of agent network being used for ML/TF purposes.

Geography[30]

The business-based risks above identify risks based on the Company's location. The relationship-based risk assesses where the client or client's business is located.

Compliance Control

The Compliance Officer must assess the geographic locations of the Company's clients and record the assessment in relationship-based risk assessment table in Schedule 2. The Compliance Officer should also be aware of any Ministerial Directives relating to clients' geographical location.

Relationship-based examples of higher risk indicators and considerations for geography[31]	
Examples of higher risk indicators	**Considerations**
The client's proximity to the Company's location	A client that conducts business or transactions away from their home branch or address without reasonable explanation. For example, a client conducts transactions at different branches across a broad geographical area over one day and this does not appear to be practical.
The client is a non-resident	Identifying non-resident clients may prove to be more difficult if they are not present and as such, could raise the inherent level of risk.
The client has offshore business activities or interests	Is there a legitimate reason for the client to have offshore interests? Offshore activities may be used by a person to add a layer of complexity to transactions, thus raising the overall risk of ML/TF.
The client's connection to high-risk countries	Take the client's connection to high-risk countries into account as some countries have weaker or inadequate AML/ATF standards, insufficient regulatory supervision or present a greater risk for crime, corruption or TF.

[30] PCMLTFR, SOR/2002-184, s. 156(1)(c)(iii). https://www.fintrac-canafe.gc.ca/guidance-directives/compliance-conformite/rba/rba-eng.

[31] https://www.fintrac-canafe.gc.ca/guidance-directives/compliance-conformite/rba/rba-eng#a2T1, Annex2, Table 10.

Impacts of new developments and technologies[32]

The business-based risks above identify risks based on the Company's introduction of new developments and technologies in your business model prior to implementing them. In the relationship-based risk assessment, the Compliance Officer must examine the potential impacts that new developments (putting in place a new service/activity/location) and technologies (introducing a new technology) could have on the Company's clients, affiliates, and anyone with whom the Company has a business relationship. Further, new developments and technologies can increase risk, as they may provide another layer of anonymity.

Compliance Control

The Compliance Officer must assess the new technology and development before the adoption of the new technology(s) or development(s) and record them in relationship-based risk assessment table in Schedule 2.

Relationship-based examples of higher risk indicators and considerations for new developments and technologies[33]	
Examples of higher risk indicators	**Considerations**
Changing payment methods	A client that conducts business or transactions away from their home branch or address without reasonable explanation. For example, one of the clients conducts transactions at different branches across a broad geographical area over one day and this does not appear to be practical.
A new service or activity that offers transaction anonymity	It is important to assess the impact that a new service or activity can have on the behaviour of the clients who may use it to distance themselves from a transaction.

Client characteristics and patterns of activity or transactions[34]

Periodically throughout the client relationship, the Compliance Officer should consider the purpose and intended nature of the relationship. Doing so will help understand the clients' activities and transaction patterns, in order to determine their level of ML/TF risk.

Compliance Control

The Compliance Officer should holistically assess new client records, risk assessments, and transaction records for higher risk indicators and the rationale for client characteristics and patterns of activity. It may be helpful to review the relationship-based risk assessment table in Schedule 2.

Note also that many financial institutions use automated systems to identify unusual patterns or transactions, among other things, and the Company may adopt such systems if deemed appropriate and effective.

Relationship-based examples of higher risk indicators and rationale for client characteristics and patterns of activity[35]

[32] PCMLTFR, SOR/2002-184, s. 156(1)(c)(v). https://www.fintrac-canafe.gc.ca/guidance-directives/compliance-conformite/rba/rba-eng.

[33] https://www.fintrac-canafe.gc.ca/guidance-directives/compliance-conformite/rba/rba-eng#a2T1, Annex2, Table 11.

[34] PCMLTFR, SOR/2002-184, ss. 123.1, 156(1)(c)(v).

[35] https://www.fintrac-canafe.gc.ca/guidance-directives/compliance-conformite/rba/rba-eng#a2T1, Annex2, Table 12.

Examples of higher risk indicators	Considerations
The client is in possession or control of property that the Company knows/believes is owned or controlled by or on behalf of a terrorist or a terrorist group	The Company is required to send a terrorist property report to FINTRAC if the Company has property in its possession or control that the Company knows/believes is owned or controlled by or on behalf of a terrorist or a terrorist group. This includes information about transactions or proposed transactions relating to that property. After filing a terrorist property report, the client automatically becomes high-risk.
The client is a foreign PEP Politically exposed person ("**PEP**")	A foreign PEP is an individual who is or has been entrusted with a prominent function. Because of their position and the influence they may hold, a foreign PEP, their family members and their close associates are vulnerable to ML/TF and other offences such as corruption. As a business, the Company must consider a foreign PEP, their family members and their close associates as a high-risk client.
The entity has a complex structure that conceals the identity of beneficial owners	When it is not possible to obtain or confirm the ownership and control information of a corporation or an entity, the Company is required to verify the identity of the most senior managing officer of the entity and treat the entity as high-risk, and apply the prescribed special measures as stated in the Proceeds of Crime Money Laundering and Terrorist Financing Regulations. For more information, please consult FINTRAC's Beneficial ownership requirements guidance. It is important to note that when it is not possible to obtain the information on beneficial ownership, there may be other information or indicators that would make this relationship pose a higher risk.

Relationship-based examples of additional higher risk indicators and related considerations[36]	
Examples of higher risk indicators	**Considerations**
STR was previously filed or considered	Suspicious transactions (or attempted transactions) are financial transactions for which the Company have reasonable grounds to suspect they are related to the commission or attempted commission of an ML/TF offence. For more information about STRs and ML/TF indicators, see FINTRAC's STR guidance. Clients that are the conductors of suspicious transactions that have been reported should be assessed as posing a higher risk.
Transactions involving third parties	Transactions involving third parties may indicate high-risk when the link between the third party and the client is not obvious.

[36] https://www.fintrac-canafe.gc.ca/guidance-directives/compliance-conformite/rba/rba-eng#a2T1, Annex2, Table 12.

The account activity does not match the client profile	Account activity that does not match the client profile may indicate a higher risk of ML/TF. The Company may face situations where it has submitted several large cash transaction reports to FINTRAC about a client with an occupation that does not match this type of activity (for example, student, unemployed, etc.).
The client's business generates cash for transactions not normally cash intensive *These examples are included for regulatory completeness and are not representative of the Company's client base or services.*	The fact that there is no legitimate reason for the business to generate cash represents a higher risk of ML/TF.
The client's business is a cash-intensive business (such as a bar, a club, etc.)	Certain types of business, especially those that are cash-intensive may have a higher inherent risk for ML/TF because legitimate money can be co-mingled with illegitimate money. For example, clients that own white label ATMs.
The client offers online gambling	Industry intelligence, including reports from the Royal Canadian Mounted Police, indicates that due to the nature of the business, the gambling sector is susceptible to ML activity. Additionally, the FATF has indicated that internet payment systems are an emerging risk in the gambling industry. Internet payment systems are used to conduct transactions related to online gambling, these two factors make the online gambling industry inherently higher risk. As well, higher inherent risk may exist if the online gambling activities are not managed by provincial lottery and gaming corporations.
The client's business structure (or transactions) seems unusually or unnecessarily complex	An unnecessarily complex business structure or complex client transactions (compared to what the Company normally sees in a similar circumstance) may indicate that the client is trying to hide transactions or suspicious activities.
The client is an RE under the PCMLTFA that is not otherwise regulated	Some reporting entities that are not federally or provincially regulated (other than under the PCMLTFA) may present higher risks of ML/TF. In addition, some may have cash intensive businesses that can also increase the overall risks of ML/TF.
The client is an intermediary or a gatekeeper (such as a lawyer or accountant) holding accounts for others unknown to the Company	Accountants, lawyers and other professionals sometimes hold co-mingled funds accounts for which beneficial ownership may be difficult to verify. This does not mean that all clients with these occupations are high-risk. Be aware of the risks that exist for these occupations and determine if the activities of the clients are in line with what one would expect and with the intended purpose of the account (for example a personal, business or trust account).
The client is an unregistered charity	Individuals and organizations can misuse charities in ML schemes or to finance or support terrorist activity. It is important to be aware of the risks in relation to charities and to apply due

	diligence by confirming if a charity is registered with the Canada Revenue Agency
Domestic PEPs and heads of international organizations (HIOs)	Corruption is the misuse of public power for private benefit. Internationally, as well as in Canada, it is important to understand that the possibility for corruption exists and that domestic PEPs or HIOs can be vulnerable to carrying out or being used for ML/TF offences. Once the Company has determined that a person is a domestic PEP, a HIO or a family member or close associate of them, the Company must determine if the person poses a higher risk for committing an ML/TF offence. If the assessment is high-risk, then the Company must treat the person as a high-risk client. For more information, please consult the PEP and HIO guidance for your sector (if applicable).

Matrix and Rating

The clients must be assessed on an individual basis. If the Company starts scaling and the number of clients increase, the Compliance Officer should consider grouping clients risk assessments based on metrics such as incomes, occupations and portfolios, or those who conduct similar types of transactions.

Risk Tolerance

If a risk is deemed high-risk, the Compliance Officer must weigh the overall regulatory risk, reputational risk, legal risk, or financial risk of said high-risk before approving it.

Risk-reduction Measures and Key Controls

In addition to the ongoing monitoring of business and client relationships including keeping a record of the measures and information obtained through this monitoring, [37] the Compliance Officer will use special measures to mitigate high-risk clients.[38]

Compliance Control

For your high-risk clients and business relationships, the Compliance Officer must: [39]

1. Conduct enhanced monitoring of these clients and business relationships.
2. Take enhanced measures to verify their identity and/or keep client information up to date.

The Compliance Officer must document points “1” and “2”. A sample recordkeeping table for these matters is set out in Schedule 2.

Evaluating Residual Risk

The Compliance Officer must ensure the residual risk is never greater than the Company’s risk tolerance. The Compliance Officer should also ensure the Company’s risk measures and controls sufficiently mitigate high-risk situations or high-risk posed by clients.

[37] PCMLTFR, SOR/2002-184, ss. 123.1, 146(1), 157 and PCMLTFA, S.C. 2000, c 17, s. 9.6(3).
[38] PCMLTFR, SOR/2002-184, s. 157 and PCMLTFA, S.C. 2000, c 17, s. 9.6(3).
[39] PCMLTFR, SOR/2002-184, s. 157 and PCMLTFA, S.C. 2000, c 17, s. 9.6(3).

The following are examples of possible Residual Risk Assessment Charts that may be used by the MSB to evaluate the Residual Risk:

Residual Risk Assessment Chart					
Residual Risk Rating		Control Assessment			
		Excellent	Adequate	Poor	Control /Not Tested
herent Risk Rating (IRR)	High	Low	Medium	High	High
	Medium	Low	Low	Medium	Medium
	Low	Low	Low	Low	Low

Residual Risk Assessment Chart					
Residual Risk Rating		Impact of Risk			
		Low (1)	Medium (2)	High (3)	ery High (4)
elihood of Risk	ery High (4)	4	8	12	16
	High (3)	3	6	9	12
	Medium (2)	2	4	6	8
	Low (1)	1	2	3	4

Risk Score	
Very High	9-16
High	7-9
Medium	4-6
Low	0-3

Compliance Control

The Compliance Officer must conduct a residual risk assessment for each initial client at onboarding and on a periodic bases, depending on the client's then-current residual risk rating. The higher the then-current risk rating, the more frequently the updated risk assessment should occur.

Compliance Training Program

Sole proprietors do not need a training program.[40]

All of the Company's employees, agents or other individuals authorized to act on behalf of compliance officer, need either a compliance training program to be created for their training or have courses provided to them to teach them the compliance program, as required by law.[41]

[40] PCMLTFR, SOR/2002-184, s. 156(d). See also https://fintrac-canafe.canada.ca/guidance-directives/compliance-conformite/Guide4/4-eng#s2: "**Note: If you are a sole proprietor with no employees, agents or other individuals authorized to act on your behalf, you are not required to have a training program nor are you required to have a training plan in place for yourself."

[41] Ibid.

The Company will provide general AML training to its officers, employees and appointed agents to ensure awareness of the AML laws and regulations and this Policy. The training will include, at a minimum:

- how to identify potential signs of money laundering and to determine the appropriate corrective measure;
- what duties and responsibilities the officers, employees and appointed agents have in the Company's compliance efforts and how to perform such duties and responsibilities;
- escalation procedures;
- the Company's recordkeeping requirements; and
- disciplinary consequences for non-compliance with this Policy (up to and including termination).

Training is provided to all relevant staff on a regular basis, but at least annually. The content of training materials is approved by the Compliance Officer. Completion of training is mandatory for all employees and failure to complete training will be reported to the Compliance Officer.

Additional training may be provided by the Compliance Officer or other relevant staff, internally or externally where deemed appropriate. Additional training will be recorded in an internal training register which will contain details of the content of training provided, the attendees and where relevant any results or scores taken from tests or feedback.

Plan for the Compliance Program Effectiveness Review[42]

The Compliance Officer must review the Compliance Program on the Compliance Program Effectiveness Review Date.[43]

The following must be analyzed and tested during a Compliance Program Effectiveness Review:

- interviews with those handling transactions to evaluate their knowledge of policies and procedures and related record keeping client identification and reporting requirements;
- a review of a sample of records to assess whether client identification policies and procedures are being followed;
- a review of agreements with agents or mandataries, as applicable, as well as a review of a sample of the information that agents or mandataries referred to in order to verify the identity of persons, to assess whether client identification policies and procedures are being followed;
- a review of transactions to assess whether suspicious transactions were reported to FINTRAC;
- a review of large cash transactions to assess whether they were reported to FINTRAC with accurate information and within the prescribed timelines;
- a review of electronic funds transfers to assess whether reportable transfers were reported to FINTRAC with accurate information and within the prescribed timelines (applicable to RE sectors that have EFT obligations);
- a review of a sample of client records to see whether the risk assessment was applied in accordance with your risk assessment process;
- a review of a sample of client records to see whether the frequency of ongoing monitoring is adequate and carried out in accordance with the client's risk level assessment;
- a review of a sample of high-risk client records to confirm that enhanced mitigation measures were taken;

[42] PCMLTFR, SOR/2002-184, s. 156(1)(f).
[43] PCMLTFR, SOR/2002-184, s. 156(1)(b).

- a review of a sample of records to confirm that proper record keeping procedures are being followed;
- a review of the risk assessment to confirm that it reflects current operations; and
- a review of policies and procedures to ensure that they are up to date and reflect the current legislative requirements and that they reflect current business practices. [44]

The Compliance Officer must use their best judgement to determine if an interim review is needed based on changes to the business model or significant changes in client relationships. For example, adding employees (trigging a need for a compliance training plan) or servicing new types of clients (e.g., a high-net-worth client from a different jurisdiction).

Compliance Control

The Compliance Program review must be carried out every two years (at minimum) and the results documented by an internal or external auditor, or by the Compliance Officer.[45] **As part of best practices, the Company should engage an external auditor in Canada to conduct its Compliance Program review every two years, at minimum**.

The Compliance Officer must ensure the following is documented:

- the date the review was conducted, the period that was covered by the review and the person or entity who performed the review;
- the results of the tests that were performed; and
- the conclusions, including deficiencies, recommendations and action plans, if any.[46]

The Compliance Officer must report, in writing, the following to a senior officer of the Company no later than 30 days after the completion of the effectiveness review:[47]

- the findings of the review (for example, deficiencies, recommendations, action plans);
- any updates made to the policies and procedures during the reporting period (the period covered by the two-year review) that were not made as a result of the review itself; and
- the status of the implementation of the updates made to your policies and procedures.[48]

[44] 7. What are the requirements related to my two-year effectiveness review and plan?
[45] PCMLTFR, SOR/2002-184, s. 156(3).
[46] 7. What are the requirements related to my two-year effectiveness review and plan?
[47] PCMLTFR, SOR/2002-184, s. 156(4).
[48] 7. What are the requirements related to my two-year effectiveness review and plan?

Know Your Client ("**KYC**")

When to Verify the Identity of Persons and Entities

The Company must verify the identity of clients where required under the PCMLTFA and applicable to the Company's operating model, including in connection with the following (only for services provided by the Company):

1. Large cash transactions;[49]

(Not permitted under the Company's operating model; included solely to reflect statutory requirements applicable to MSBs under the PCMLTFA.)

2. Large virtual currency ("**VC**") transactions;[50]
3. Suspicious transactions;[51]
4. Issuing or redeeming traveler's cheques, money orders, or similar negotiable instruments of $3,000 or more.[52]
5. Transmitting $1,000 or more in funds by means other than an electronic funds transfer (EFT);[53]

(Included to reflect statutory MSB recordkeeping requirements, where applicable.)

6. Initiating an EFT of $1,000 or more;[54]

(Included to reflect statutory MSB recordkeeping requirements, where applicable..)

7. Foreign currency exchange transactions of $3,000 or more;[55]
8. Transferring VC in an amount equivalent to $1,000 or more;[56]
9. Exchanging VC in an amount equivalent to $1,000 or more;[57]
10. Remitting funds in the amount of $1,000 or more to a beneficiary, by means other than an EFT;[58]
11. Remitting funds to the beneficiary of an international EFT of $1,000 or more;[59]
12. Remitting VC to a beneficiary in an amount equivalent to $1,000 or more; and[60]
13. Information records.[61]

(together, the "**Required Verification Transactions" or "RVT**")

Below are descriptions of particular RVTs, for ease of reference.

1. Large Cash Transactions

Not permitted under the Company's operating model. The Company does not receive, handle, or authorize the receipt of cash. This section is included solely to reflect statutory MSB requirements under the PCMLTFA[62]

---

[49] Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFR), SOR/2002-184, ss. 84(a), 105(7)(a), 109(4)(a) and 112(3)(a).
[50] PCMLTFR, SOR/2002-184, ss. 84(b), 105(7)(a), 109(4)(a) and 112(3)(a).
[51] PCMLTFR, SOR/2002-184, ss. 85(1), 105(7)(c), 109(4)(b) and 112(3)(b).
[52] PCMLTFR, SOR/2002-184, ss. 95(1)(a) and 105(7)(a).
[53] PCMLTFR, SOR/2002-184, ss. 95(1)(a.1) and 105(7)(a).
[54] PCMLTFR, SOR/2002-184, ss. 95(1)(b) and 105(7)(a).
[55] PCMLTFR, SOR/2002-184, ss. 95(1)(c) and 105(7)(a).
[56] PCMLTFR, SOR/2002-184, ss. 95(1)(d) and 105(7)(a).
[57] PCMLTFR, SOR/2002-184, ss. 95(1)(e) and 105(7)(a).
[58] PCMLTFR, SOR/2002-184, ss. 95(1)(e.1) and 105(7)(a).
[59] PCMLTFR, SOR/2002-184, ss. 95(1)(f) and 105(7)(a).
[60] PCMLTFR, SOR/2002-184, ss. 95(1)(f) and 105(7)(a).
[61] PCMLTFR, SOR/2002-184, ss. 95(3), 95(4), 109(4)(g) and 112(3)(g).
[62] PCMLTFR, SOR/2002-184, s. 126.

Exceptions
The Company does not have to verify the identity of a person or entity that conducts a large cash transaction if:

- money is received from a Financial Entity or Public Body, or someone acting on their behalf;[63]
- the amount is deposited to a business account or is deposited in an automated banking machine (including a quick drop or night deposit).[64]

(Not applicable to the Company, as cash transactions are not conducted.)

2. Large VC transactions
FINTRAC requires the Company to verify the identity of every person or entity from which it receives VC in an amount equivalent to $10,000 or more when the transaction takes place. This includes a situation where the Company is deemed to have received VC because it authorized another person or entity to receive the VC on its behalf.[65] This obligation is subject to the 24-hour rule.[66]

Exceptions
The Company does not have to verify the identity of a person or entity that conducts a large VC transaction if:

- VC is received from a Financial Entity or Public Body, or someone acting on their behalf;[67]
- when the Company transfers or receives VC as compensation for the validation of a transaction that is recorded in a distributed ledger or the Company exchanges, transfers or receives a nominal amount of VC for the sole purpose of validating another transaction or a transfer of information – the Company does not need to keep a large VC transaction record and do not need to verify identity.

Applicable only to the extent required by regulation and only where VC-related activity occurs within the Company's services.

3. Suspicious Transactions
The Company must take reasonable measures to verify the identity of every person or entity that conducts or attempts to conduct a suspicious transaction, regardless of the transaction amount, and including transactions that would normally be exempt from client identification requirements, before sending a Suspicious Transaction Report (STR) where required under the PCMLTFA and applicable to the Company's operations.[68]

Exceptions
The Company does not have to take reasonable measures to verify the identity of the person or entity that conducts or attempts to conduct a suspicious transaction if:

- the Company has already verified the identity of the person or entity as required and have no doubts about the identification information;[69]or
- the Company believes that verifying the identity of the person or entity would inform them that a Suspicious Transaction Report will be submitted.[70]

---

[63] PCMLTFR, SOR/2002-184, ss. 31 and 84(a).
[64] PCMLTFR, SOR/2002-184, s. 84(a).
[65] PCMLTFR, SOR/2002-184, 141(2), 143(2)
[66] PCMLTFR, SOR/2002-184, s. 126.
[67] PCMLTFR, SOR/2002-184, ss. 31 and 84(a).
[68] PCMLTFR, SOR/2002-184, ss. 85(1), 105(7)(c), 109(4)(b) and 112(3)(b).
[69] PCMLTFR, SOR/2002-184, ss. 155(1), 155(2) or 155(3).
[70] PCMLTFR, SOR/2002-184, s. 85(2).

4. Information records

The Company must verify the identity of a corporation or other entity 30 days after the day on which the information record is created for:[71]

- an ongoing service agreement related to virtual asset services supported by the Company, where applicable;
- a service agreement to exchange or transfer VC.

Exceptions

The Company does not have to verify the identity of a corporation or other entity when creating an information record if the entity is:

- a Public Body;[72]
- a corporation 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; [73]or
- a subsidiary of a public body or corporation or trust, whose financial statements are consolidated with the financial statements of the public body, corporation or trust.[74]

Compliance Control

The Company must keep a record of new clients, including the client's name, address, telephone number, occupation or nature of principal business, and date of birth for an individual. It must also keep a record of the purpose and intended nature of each business relationship. A helpful summary of the records to maintain that can also serve as a template, is set out in Schedule 3.[75] The Company can use the tables in Schedule 3 or record the information in another format.

If the Identifier is unable to verify the identity of a new client, then the Company will not open an account for the new client or otherwise transact with the new client above the applicable thresholds, until their identity can be verified.[76]

Methods to Verify the Identity of Persons and Entities

Identifying a Person

The Company applies the "government-issued photo identification method" to verify clients that are individuals.[77]

The Identifier must follow the Verification Checklist table in Schedule 3 to ensure the government-issued photo identification meets the legislative requirements and FINTRAC's guidance.

When identifying a person, it is important to check that the government-issued photo identification document is *authentic*, *valid* and *current*[78] by viewing the document in person and in the presence of the person being identified:

---

[71] PCMLTFR, SOR/2002-184, ss. 95(3), 95(4), 109(4)(g) and 112(3)(g).
[72] PCMLTFR, SOR/2002-184, s. 95(5)(a).
[73] PCMLTFR, SOR/2002-184, s. 95(5)(b).
[74] PCMLTFR, SOR/2002-184, s. 95(5)(c).
[75] PCMLTFR, SOR/2002-184, ss. 123.1(b), 138, 145.
[76] PCMLTFA, S.C. 2000, c 17, s. 9.2.
[77] PCMLTFR, SOR/2002-184, s. 105(1)(a). a. Government-issued photo identification method.
[78] PCMLTFR, SOR/2002-184, s. 105(5).

- Look for security features on the document to determine it is *authentic* (e.g., BC driver's licence has a 'ghost' image with your year of birth on the right-hand side that can be felt by touch.).
- Ensure the document is *valid* (unaltered, not counterfeit, not severely damaged).
- Determine if the document is *current* (not expired and will not expire in the next 6 months).

When viewing a government-issued photo identification document in person is not possible, the Identifier must utilize the process outlined in Schedule 7 (Client Verification Discussion), section C - **Sample Procedure For Verifying Clients Not Physically Present** - to ensure the identification document is authentic, valid and current, and to ensure the "selfie" or live video representation of the client matches the provided identification document. *Schedule 7 also includes a more comprehensive discussion of client verification, as required by FINTRAC.*

Compliance Control
The Identifier must record the type of document used to identify the individual. For manual processes, the Company can use applicable (Person) table in Schedule 3.

Identifying a Corporation
The Company applies the "confirmation of existence method" to identify corporations and entities.

The Identifier must receive the certificate of incorporation of the company seeking the Company's services. Regarding other entities, the Identifier must receive a copy of a partnership agreement, articles of association, or the most recent version of any other record that confirms its existence and contains its name and address.

When identifying a corporation or other entity, the Identifier must check that the certificate of incorporation[79] or entity[80] is *authentic*, *valid* and *current*. The same principles as identifying a person apply to authentic, valid and current.

Compliance Control
The Identifier must record the type of document used to identify the corporation or entity. For manual processes, the Company can use applicable (Corporation) table in Schedule 3.

Business Relationship Requirements

Entering into a Business Relationship
Determining when a business relationship is established is a sector-specific exercise, in which the rules are different for the different RE sectors.[81] For MSBs, a business relationship is established when (i) the MSB (the Company) must identify a person or entity twice with a 5-year period; and (ii) an entity enters into a service agreement with the Company in respect of its MSB business)

To determine whether the company must identify a person or entity a second time in a 5-year period, the Company must determine when the requirement to verify the client is triggered for the second time. This may occur, for example, when a client's first transaction is a large VC transaction, and two months later, the client's second interaction triggers an additional verification requirement under applicable AML rules (for example, a reportable virtual asset-related activity). Although the Company may not need to reperform the identity verification process at this time (see below), it does need to carry out the additional obligations that apply when a business relationship is established.

[79] PCMLTFR, SOR/2002-184, s. 109(2).
[80] PCMLTFR, SOR/2002-184, s. 112(2).
[81] 1. What is a business relationship?

There may be situations where a business relationship is formed by virtue of suspicious transaction reporting (STR) to FINTRAC.[82] In this case, the Identifier must identify the person or entity conducting the suspicious transaction. The identifier must be aware not to "alert" the person or entity conducting the suspicious transaction.

There is no need to re-verify the identity of a client if:

- it has already been done via the prescribed methods outlined in the Compliance Program and Procedures and Regulations;
- you have kept the associated records; and
- you have no doubts about the information used.

Time

The Identifier must determine whether the Company has entered into a business relationship no more than 30 days after (i) the service agreement-based account is open; or (ii) verifying the client's identity.[83] There are no exceptions to this rule.

End of the Business Relationship

A business relationship ends five years after the day on which a client closes their last account with the Company.

A Non-account-based business relationship ends when a period of at least five years has passed since the day of the last transaction that required the Company to verify the identity of the client.

Compliance Control

If there is a need to identify a person or entity by virtue of entering into a business relationship or through a STR, the Identifier must add the information in the respective table in Schedule 3.

The Identifier must also record the purpose and intended nature of the business relationship.[84] If this information is already recorded, there is no need to record it again,[85] but the Identifier must note that the information has been recorded and where the record is kept. For manual processes, the Identifier can add the information using the Business Relationship Record table in3.

Beneficial Ownership Requirements

The Identifier must take reasonable steps to determine if a client is using techniques to conceal beneficial ownership of money.[86] Identifying the beneficial owners of a corporation or other entity helps prevent money laundering and terrorist activity financing schemes.

Beneficial owners are the individuals who directly or indirectly own or control 25% or more of a corporation or an entity other than a corporation.[87] Some examples of entities include corporations, trusts and partnerships.

The beneficial ownership information must be confirmed when it is first obtained by the Identifier and during ongoing monitoring of the Company's business relationships.

The Identifier must obtain and confirm the accuracy of the following for each entity:

---

[82] PCMLTFR, SOR/2002-184 s. 85.
[83] 4. How much time do I have to determine if I have entered into a business relationship with a client?
[84] PCMLTFR, SOR/2002-184, s. 145.
[85] PCMLTFR, SOR/2002-184, s. 153.
[86] PCMLTFR, SOR/2002-184, s. 138(1).
[87] PCMLTFR, SOR/2002-184, s. 138(1).

Entity	Requirements	Examples of supporting documents to establish accuracy of information
Corporations	the names of all directors of the corporation and the names and addresses of all persons who directly or indirectly own or control 25% or more of the shares of the corporation[88]	● minute book; ● securities register; ● shareholders register; ● articles of incorporation; ● annual returns; ● certificate of corporate status; ● shareholder agreements; or ● board of directors' meeting records of decision
Trusts	the names and addresses of all trustees and all known beneficiaries and settlors of the trust[89]	● Trust Deed
Widely held or publicly traded trusts	the names of all trustees of the trust and the names and addresses of all persons who directly or indirectly own or control 25% or more of the units of the trust[90]	● Trust Deed
Entities other than corporations or trusts (e.g., Partnerships)	the names and addresses of all persons who directly or indirectly own or control 25% or more of the entity[91]	● partnership agreements
Non-for-profits	charity registered with the Canada Revenue Agency under the Income Tax Act or an organization, other than one referred to above, that solicits charitable donations from the public.	● Constitution and Bylaws
		Other reasonable measures can include: ● asking the client to provide supporting official documentation; ● conducting an open-source search; or ● consulting commercially available information

The Identifier must obtain information establishing the ownership, control and structure of the entity, including reasonable steps to confirm the accuracy of the documents obtained and in the course of ongoing monitoring of the Company's business relationship with the client.[92]

[88] PCMLTFR, SOR/2002-184, s. 138(1)(a).
[89] PCMLTFR, SOR/2002-184, s. 138(1)(b).
[90] PCMLTFR, SOR/2002-184, s. 138(1)(a.1).
[91] PCMLTFR, SOR/2002-184, s. 138(1)(c).
[92] PCMLTFR, SOR/2002-184, s. 138(2).

Records must be kept of the measures taken to determine the beneficial interest in an entity.[93]

Compliance Control
An example of beneficial ownership Records is set out in a table in Schedule 3, though in many cases this information may be recorded in an application form submitted by the client to the Company.

The Company must keep these records for at least five years from the day the last business transaction is conducted.[94]

Third Party Determination Requirements
A third party is someone who conducts a transaction on behalf of another individual.

You must take reasonable measures to make a third-party determination when you are required to:

Triggering Event	**Triggering Event Description**	**Requirement**
Large Cash Transaction Report or large cash transaction record	Receive cash in an amount of $10,000 or more, and are required to submit a Large Cash Transaction Report (LCTR) to FINTRAC or to keep a large cash transaction record	Take reasonable measures to determine whether the person that gave you the cash is acting on behalf of a third party[95] and subject to the 24-rule[96]
Large Virtual Currency Transaction Report or large virtual currency transaction record	Receive an amount of virtual currency (VC) equivalent to $10,000 or more, and are required to submit a Large Virtual Currency Transaction Report (LVCTR) to FINTRAC or to keep a large virtual currency transaction record	Take reasonable measures to determine whether the person from whom you receive the VC is acting on behalf of a third party.[97]
Information record	MSB/FMSBs must keep an information record for certain transactions or activities; most commonly, after entering into a service agreement with another businesses.	At the time the Identifier creates the information record, the Identifier must take reasonable measures to determine whether the person or entity for which the information record is kept on, is acting on behalf of a third party.[98]

Compliance Control
In determining if a third party relationship exists, the Identifier must document the required information. An example is set out in the Third Party Information table in Schedule 3.[99]

[93] PCMLTFR, SOR/2002-184, s. 138(3).
[94] PCMLTFR, SOR/2002-184, s. 148(1)(b).
[95] PCMLTFR, SOR/2002-184, s. 134(1).
[96] PCMLTFR, SOR/2002-184, s. 126.
[97] PCMLTFR, SOR/2002-184, s. 134(1).
[98] PCMLTFR, SOR/2002-184, s. 136(1).
[99] CMLTFR, SOR/2002-184, ss. 134(2), 135(2), 136(2), 137(2).

If the Identifier cannot make a definitive third party determination, but suspects that a third party is involved, then the Identifier must record the required information. An example is set out in the Third Party Information table in Schedule 3.

The information contained in both tables must be kept for at least five years from the date the third party determination record was created.[100]

Politically exposed persons (PEP) and heads of international organizations (HIO) requirements
Foreign and domestic PEPs and HIOs are vulnerable to corruption and the potential targets of criminals who could exploit their status and use them, knowingly or unknowingly, to carry out ML or TF offences. Family members and close associates of PEPs and HIOs are also potential targets. Therefore, it is important for an Identifier to note when a PEP or HIO has engaged the Company for services.

A **domestic PEP** is a person who currently holds, or has held within the last 5 years,[101] a specific office or position in or on behalf of the Canadian federal government, a Canadian provincial (or territorial) government, or a Canadian municipal government. Specifically, the person has held the office or position of:

- 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
- mayor, reeve or other similar chief officer of a municipal or local government.[102]

A person ceases to be a domestic PEP 5 years after they have left office or 5 years after they are deceased.[103] The Company must mitigate a domestic PEP risk until the PEP ceases to be domestic PEP.

The Identifier must also be aware of any **foreign PEPs**. A foreign PEP is a person who holds or has held one of the following offices or positions in or on behalf of a foreign state:

- head of state or head of government;
- member of the executive council of government or member of a legislature;
- deputy minister or equivalent rank;
- ambassador, or attaché or counsellor of an ambassador;
- military officer with a rank of general or above;
- president of a state-owned company or a state-owned bank;
- head of a government agency;
- judge of a supreme court, constitutional court or other court of last resort; or
- leader or president of a political party represented in a legislature.[104]

---

[100] PCMLTFR, SOR/2002-184, s. 148(1)(c).
[101] PCMLTFR, SOR/2002-184, s. 2(2).
[102] PCMLTFA, S.C. 2000, c 17, s. 9.3(3).
[103] PCMLTFR, SOR/2002-184, s. 2(2).
[104] PCMLTFA, S.C. 2000, c 17, s. 9.3(3).

The Company must forever treat as a PEP a person identified as a foreign PEP, including deceased foreign PEPs. After determining an individual is a foreign PEP, there is no need to make that determination again.[105]

A HIO is a person who currently holds or has held within the last 5 years the specific office or position of "head" (i.e., CEO or President) of an international organization and the international organization that they head or were head of is either:[106]

- an international organization established by the governments of states;
- an institution of an organization referred to in 1 above; or
- an international sports organization.[107]

A person ceases to be a HIO 5 years after they are no longer the head of the organization or institution or 5 years after they are deceased.[108] The Company must mitigate this risk until the HIO ceases to be HIO (no longer hold the respective position for the organization). Examples of international organizations include (non-exhaustive):

- United Nations organizations;
- Association of Southeast Asian Nations organizations;
- North Atlantic Treaty Organization (NATO).[109]

The Identifier must determine if an individual is a **family member** of a PEP or HIO. These family members are:

- their spouse or common-law partner, including ex-spouse or partner;
- their biological or adoptive child(ren), not stepchildren;
- their mother(s) or father(s);
- the mother(s) or father(s) of their spouse or common-law partner (mother-in-law or father-in-law); and
- the child(ren) of their mother or father (sibling(s)).[110]

The Company must forever treat as a PEP a person identified as a family member of a foreign PEP, including deceased a family member of a foreign PEPs. After determining an individual is a family member of a foreign PEP, there is no need to make that determination again.[111]

A person ceases to be a family member of a domestic PEP or HIO 5 years after the domestic PEP or HIO has left office or 5 years after they are deceased. The Company must mitigate continue to mitigate the risks associated with the family members of domestic PEPs or HIOs during that time.

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

- are the business partners of, or who beneficially own or control a business with, a PEP or HIO;
- are in a romantic relationship with a PEP or HIO;
- are involved in financial transactions with a PEP or a HIO;

---

[105] PCMLTFR, SOR/2002-184, s. 155(4).
[106] PCMLTFA, S.C. 2000, c 17, s. 9.3(3).
[107] PCMLTFA, S.C. 2000, c 17, s. 9.3(3).
[108] PCMLTFR, SOR/2002-184, s. 2(2).

[109] https://fintrac-canafe.canada.ca/guidance-directives/client-clientele/pep/pep-eng#annex1.
[110] PCMLTFR, SOR/2002-184, s. 2(1).
[111] PCMLTFR, SOR/2002-184, s. 155(4).

- serve as prominent members of the same political party or union as a PEP or HIO;
- serve as a member of the same board as a PEP or HIO;
- carry out charitable works closely with a PEP or HIO; or
- are listed as joint on a policy where one of the holders may be a PEP or HIO.[112]

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

As a best practice, a senior manager at the Company (Compliance Officer, CEO, sole proprietor), will analyze and review this type of transaction to determine if such accounts should stay open.

Compliance Control
The Identifier and a member of senior management must record and make determinations about a PEP or HIO. An example of the recordkeeping measure is set out in the PEP and HIO table in Schedule 3. The trigger for the determination includes:

Business relationships

- entering into a business relationship;[113]
- conducting periodic monitoring of your business relationships;[114]
- detecting a fact about your existing business relationships that indicates a PEP or HIO connection;[115]

Transactions

- initiation of an international electronic funds transfer (EFT) in the amount of $100,000 or more in the course of providing services in Canada;[116]
- final receipt of an international EFT in the amount of $100,000 or more in the course of providing services in Canada for remittance to a beneficiary;[117]
- transfer of an amount of VC equivalent to $100,000 or more in the course of providing services in Canada;[118]
- receipt of an amount of VC equivalent to $100,000 or more in the course of providing services in Canada for remittance to a beneficiary.[119]

Detail of the above are described below.

Business relationships

For foreign[120] and domestic[121] PEPs and HIO (including close family and associates[122]) the Identifier must do the following and keep a record (a sample record is set out in the PEP and HIO table in Schedule 3):

- establish the person's source of wealth; and

---

[112] PCMLTFR, SOR/2002-184, s. 120(1).
[113] PCMLTFR, SOR/2002-184, ss. 120(3) and 120.1(1).
[114] PCMLTFR, SOR/2002-184, ss. 120(4) and 120.1(2).
[115] PCMLTFR, SOR/2002-184, ss. 120(5) and 120.1(4).
[116] PCMLTFR, SOR/2002-184, ss. 120(1)(a) and 120(2)(a).
[117] PCMLTFR, SOR/2002-184, ss. 120(1)(b) and 120(2)(b).
[118] PCMLTFR, SOR/2002-184, ss. 120(1)(c) and 120(2)(c).
[119] PCMLTFR, SOR/2002-184, s. 120(1)(d) and 120(2)(d).
[120] PCMLTFR, SOR/2002-184, ss. 122.1(1) and 157 and PCMLTFA, S.C. 2000, c 17, s. 9.6(3).
[121] PCMLTFR, SOR/2002-184, ss. 122.1(3) and 157 and PCMLTFA, S.C. 2000, c 17, s. 9.6(2).
[122] PCMLTFR, SOR/2002-184, ss. 122.1(3) and 157 and PCMLTFA, S.C. 2000, c 17, s. 9.6(2).

- take enhanced measures, including taking additional measures to verify the person's identity, conducting enhanced ongoing monitoring of the business relationship, and taking any other enhanced measures to mitigate the risks posed by the person.

The source of wealth for any PEP or HIO or close family member of PEP or HIO must be determined no later than 30 days after the individual enters a business relationship with the Company.[123]

Transactions

For transactions relating to initiating an international EFT in an amount of $100,000 or more,[124] transferring an amount of VC equivalent to $100,000 or more,[125] Final receipt to a beneficiary of an international EFT in the amount of $100,000 or more, and receiving an international EFT or an amount of VC equivalent to $100,000 or more for a beneficiary,[126] relating to a foreign PEP or family member or close associate of a foreign PEP, the Identifier must keep a record of the following (a sample record is set out in the PEP and HIO table in Schedule 3):

- the source of the funds/VC used for the transaction and to establish the source of the person's wealth; and
- the name of the member of senior management who reviewed the transaction, and the date of that review (if applicable).

For transactions relating to initiating an international EFT in an amount of $100,000 or more,[127] transferring an amount of VC equivalent to $100,000 or more,[128] Final receipt to a beneficiary of an international EFT in the amount of $100,000 or more and receiving an international EFT or an amount of VC equivalent to $100,000 or more for a beneficiary,[129] relating to domestic PEPs or HIOs, the Identifier must keep a record of the following (a sample record is set out in the PEP and HIO table in Schedule 3):

- establish the source of the funds/VC used for the transaction and the source of the person's wealth; and
- the name of the member of senior management who reviewed the transaction, and the date of that review (if applicable).

Any recorded transaction records must be kept for 5 years form the day on which they last business transaction was conducted.[130]

As an MSB (when providing services to people located in Canada), for the applicable transactions referred to above, the Identifier has 30 days after the day on which the transaction is conducted to:[131]

- take reasonable measures to make a PEP, HIO, family member or close associate determination, and if you determine the person is a PEP, HIO, or close associate or family member of a PEP or HIO, determine the source of the funds or source of the VC used for the transaction and determine the person's source of wealth, and ensure that a member of senior management reviews the transaction; or

[123] PCMLTFR, SOR/2002-184, s. 122.1(5).
[124] PCMLTFR, SOR/2002-184, s. 122(1).
[125] PCMLTFR, SOR/2002-184, s. 122(2).
[126] PCMLTFR, SOR/2002-184, s. 122(3).
[127] PCMLTFR, SOR/2002-184, s. 122(5) and PCMLTFA, S.C. 2000, c 17, s. 9.6(2).
[128] PCMLTFR, SOR/2002-184, s. 122(6) and PCMLTFA, S.C. 2000, c 17, s. 9.6(2).
[129] PCMLTFR, SOR/2002-184, s. 122(7) and PCMLTFA, S.C. 2000, c 17, s. 9.6(2).
[130] PCMLTFR, SOR/2002-184, s. 148 (1)(b).
[131] PCMLTFR, SOR/2002-184, s. 122(9).

- take reasonable measures to make a PEP, HIO, family member or close associate determination and if you determine the person is a PEP, HIO, or close associate or family member of a PEP or HIO, ensure that a member of senior management reviews the transaction.

Any individual who is identified as a PEP or HIO, and any PEP or HIO controlled entity, must be treated as high-risk.

Ongoing Monitoring Requirements
In addition to the ongoing monitoring requirements and other prescribed requirements already set out in this Program, there must be ongoing monitoring and ongoing monitoring for high-risk clients to:[132]

- detect any suspicious transactions that the Company is required to report to FINTRAC;
- keep client identification information, beneficial ownership information, and the purpose and intended nature of the business relationship record up to date;
- reassess the level of risk associated with each client's transactions and activities; and
- determine whether transactions or activities are consistent with the client information the Company obtained and its risk assessment of the client.

Compliance Control
Ongoing monitoring must be taken when a high-risk client is identified. The high-risk client information is in Schedule 2 and most of the high-risk clients will be identified during the risk assessment.

A record must be kept of the measures taken when conducting ongoing monitoring (an example is provided in Schedule 3).[133] Any suspicious patterns or activity must be recorded (an example is provided in Schedule 2).

Ongoing monitoring records must be retained for at least five years from the date the record was created.[134]

Reporting

As an MSB, the Company must submit reports to FINTRAC for suspicious transactions, terrorist property, large cash transactions, large virtual currency transactions and electronic funds transfers.

Suspicious transaction reports ("**STR**")

The Compliance Officer must submit a STR to FINTRAC if there are reasonable grounds to suspect that a financial transaction that occurs *or* is attempted in the course of their activities is related to the commission or the attempted commission of an ML/TF offence.

In order to submit an STR to FINTRAC, the Compliance Officer will need to establish there are reasonable grounds to suspect the transaction is related to the commission of an ML/TF offence. Relevant measures include:

- screening for and identifying suspicious transactions;
- assessing the facts and context surrounding the suspicious transaction;
- linking ML/TF indicators to the assessment of the facts and context; and
- explaining your grounds for suspicion in an STR, where you articulate how the facts, context and ML/TF indicators allowed you to reach your reasonable grounds for suspicion.

[132] PCMLTFR, SOR/2002-184, s. 123.1.
[133] PCMLTFR, SOR/2002-184, s. 146(1).
[134] PCMLTFR, SOR/2002-184, s. 148(1)(c).

FINTRAC has compiled data on various ML/TF indicators based on industry and service. By way of example, please see a few ML/TF indicators for VC below:

- Client portfolio only consists of privacy coins or has a high value in privacy coins.
- Client transfers Bitcoin in large volumes in exchange for privacy coins.
- Client is unwilling or unable to provide information about the source of privacy coins they once held or currently have.[135]

See more examples for VC and MSB/FMSB generally.

Commonly cited examples of ML/TF indicators involving customers may include, but are not limited to:

- A customer who refuses or is hesitant to provide complete or accurate documentation or information.
- Customers who engage in repeated small transactions rather than a single larger transaction
- Customers who struggle to fill up forms that are required to complete a transaction (repeatedly misspelling their address, for example)
- Any indication that a client is trying to "structure" transactions to avoid reporting or recordkeeping requirements, including, for example, by attempting to make multiple purchases below amounts that would require reporting. This often involves making multiple cash payments each below $10,000 but that together total more than $10,000.
- Identification documents that appear fraudulent or unusual, or in which the description of the individual does not match the individual's appearance (e.g., different age, height, eye color, or sex).
- A customer who provides different information or presents different identification documents for separate transactions.
- Unusual payment methods, such as the use of large amounts of cash, multiple or sequentially numbered money orders, traveler's checks, or cashier's checks, or payment from third parties.
- Direct requests from a customer not to file required reports with the government or otherwise keep records.
- Purchases that appear unusual for a particular customer or type of customer.
- Customers who significantly change their behavior, including, for example, the number of transactions or the size and frequency of such transactions.
- Purchases or sales that are not in conformity with standard industry practice.
- Customers who engage in transactions with cash using musty bills that have an unusual or chemical-like odor.
- Customers who pay for items using money orders or traveler's checks without relevant entries on the face of the instrument or with unusual symbols, stamps, or written annotations (such as initials) that appear either on the face or on the back of the instrument.

Employees should also be alert to ML/TF indicators involving the behavior of other employees. Examples of red flags involving employee behavior may include, but are not limited to:

- Employees who demonstrate a lifestyle that cannot be supported by their salary.
- Employees who are reluctant to take vacations or leave the store.
- Employees who are associated with unusually large numbers of transactions or transactions in unusually large amounts.
- Employees who engage in excessive speculation, trading or holding of digital assets

[135] https://fintrac-canafe.canada.ca/guidance-directives/guidance-directives-eng#s3.

FINTRAC will evaluate the quality of the STRs, so it is important that they are treated with care. FINTRAC may review:

- previously submitted STRs, including their quality, timing and volume;
- the nature of the original transaction;
- the size of the Company's business and business model;
- internal processes and procedures;
- the complexity of the transactions;
- the number of relevant transactions identified in the STR;
- the nature of the indicators and grounds for suspicion;
- the facts of the case;
- the overall number of transactions in your assessment; and
- other relevant considerations.[136]

It is important for the Identifier to take reasonable measures to identify the conductor of the transaction[137] unless asking the client for this information will tip them off to the suspicion of ML/TF.[138]
STR must be retained for at least five years from the date the STR was sent to FINTRAC.

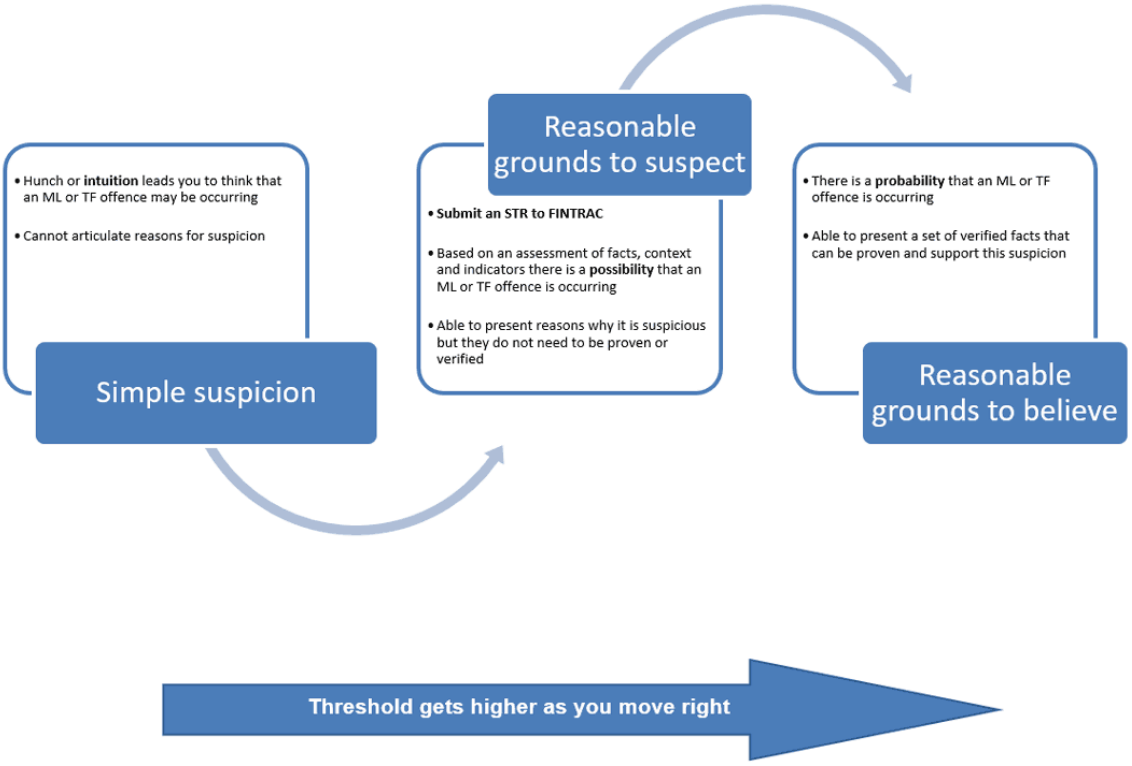
The person or entity that is the subject of the STR may never be told or 'tipped off' about the STR. Doing so could prejudice a criminal investigation, even if an actual investigation has begun.[139]

Please note: FINTRAC will assess how the Company reports suspicious transactions and expects the compliance controls listed in the Compliance Plan and Polices to be followed and applied diligently. Therefore, it is important for the Compliance Officer to regularly review ongoing monitoring process, risk assessments, and transactions.

No employee or officer of the Company should be hesitant or reluctant to file a STR. the Company supports a culture of compliance and strives to meet all obligations required to operate as an MSB. There will be no criminal or civil proceedings against an individual or entity for submitting an STR in good faith or providing FINTRAC with information about a suspicious report regarding ML/TF.[140]

FINTRAC's threshold suspicious reporting diagram[141]

[136] https://fintrac-canafe.canada.ca/guidance-directives/transaction-operation/Guide2/2-eng.
[137] PCMLTFR, SOR/2002-184, s. 85(1).
[138] PCMLTFR, SOR/2002-184, s. 85(2).
[139] PCMLTFA, S.C. 2000, c. 17, s. 8.
[140] PCMLTFA, S.C. 2000, c. 17, s. 10.
[141] https://fintrac-canafe.canada.ca/guidance-directives/transaction-operation/Guide2/2-eng.



Compliance Control

A STR must be submitted as soon as practicable. FINTRAC describes 'as soon as practicable' as:

A time period that falls in-between immediately and as soon as possible, within which a suspicious transaction report (STR) must be submitted to FINTRAC. The completion and submission of the STR should take priority over other tasks. In this context, the report must be completed promptly, taking into account the facts and circumstances of the situation. While some delay is permitted, it must have a reasonable explanation.[142]

Therefore, the Compliance Office must make the proper determinations immediately after discovering the suspicious transaction. The key requirements for the STR are outlined in STR table in Schedule 4.

The Compliance Officer must keep a copy of the STR sent to FINTRAC.[143] The record must be kept for at least five years after the day the STR was submitted.[144]

Terrorist Property Reports ("**TPR**")

The TPR is a report that the Company must submit for property that is owned or controlled by or on behalf of a terrorist or terrorist group, or the Company has reason to believe is owned or controlled by or on behalf of a person listed under the Regulations.[145] The Compliance Officer should be aware that the TPR is triggered by section 83.1 of the Criminal Code or section 8 of the Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism (RIUNRST). The Compliance Officer should also be

[142] https://fintrac-canafe.canada.ca/guidance-directives/glossary-glossaire/1-eng#asap. Proceeds of Crime (Money Laundering) and Terrorist Financing Suspicious Transaction Reporting Regulations (PCMLTFSTRR), SOR/2001-317, s. 9(2).

[143] Proceeds of Crime (Money Laundering) and Terrorist Financing Suspicious Transaction Reporting Regulations (PCMLTFSTRR), SOR/2001-317, s. 12.1 (1).

[144] Ibid.

[145] Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism, SOR/2001-360.

aware of the Listed Terrorist Entities. The latter two pieces of legislation are outside of FINTRAC's mandate; however, the Compliance officer should read and understand their basic requirements.

FINTRAC provides examples of property for the purpose of a TPR:

- cash;
- casino products and tokens;
- virtual currency (VC);
- accounts (for example, personal or business accounts, Registered Retirement Savings Plans (RRSP), Tax-Free Savings Accounts (TFSA));
- prepaid payment products and prepaid payment product accounts;
- securities (for example, stocks, bonds or mutual funds);
- jewellery, precious metals or precious stones;
- real estate, including an instrument that gives title or right to a property (for example, a deed); and
- insurance policies.[146]

The Company is concerned with VC, but also any of the above being used to convert to VC. The Compliance Officer must be aware of any suspicious property being used to barter for VC.

It is important to note that TPR differs from STR because a transaction or attempted transaction does not have to occur to submit a TPR – it is the mere existence of the property that establishes the requirement.

The Compliance Officer must submit a TPR to FINTRAC immediately once the requirements to make a disclosure under the Criminal Code or the Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism are triggered.[147] No criminal or civil proceedings will be carried out against a person or an entity for submitting a TPR to FINTRAC in good faith.[148]

Compliance Control

The Compliance Officer must make the proper determinations immediately after discovering the terrorist property. The key requirements for the STR are outlined in the TPR table in Schedule 4.

The Company must keep a copy of any TPR submitted to FINTRAC for a period of at least five years from the day the report is sent.[149] The copy of the report may be kept in a machine-readable or electronic format if a paper copy can be readily produced from it.[150]

Large Cash Transaction Reports ("**LCTR**")

The Company will utilize the LCTR Requirements via electronic reporting. FINTRAC provides instructions on how to report electronically here.

LCTR's must be sent to FINTRAC if $10,000 or more is received in cash for a single transaction. One report must be submitted for each individual transaction. If there are multiple transaction that amount to $10,000 or more with 24hrs, then the Compliance Officer must report the transaction to FINTRAC. The exception to this rule pertains to public bodies and Financial Entities such as:

- a bank (that is, one that is listed in Schedule I or II of the Bank Act) or an authorized foreign bank with respect to its operations in Canada;
- a credit union or a caisse populaire;

---

[146] https://fintrac-canafe.canada.ca/guidance-directives/transaction-operation/Guide5/5-eng#s3.
[147] PCMLTFA, S.C. 2000, c. 17, s. 7.1(1) and PCMLTFSTRR, SOR/2001-317, s. 10(2).
[148] PCMLTFA, S.C. 2000, c. 17, s. 10.
[149] PCMLTFSTRR, SOR/2001-317, s. 12.1(1).
[150] PCMLTFSTRR, SOR/2001-317, s. 12.1(2).

- a financial services cooperative (in the province of Quebec) or a credit union central (in all other provinces);
- a trust and loan company; or
- an agent of the Crown that accepts deposit liabilities.[151]

If the amount is in a foreign currency, the rate provided by the Bank of Canada must be used to determine if the foreign currency is over or under the $10,000 Canadian Dollar threshold.[152]

The Company does not receive or handle cash. This section is included solely to reflect statutory MSB reporting requirements.

Compliance Control

The Compliance Office must keep a copy of the LCTR sent to FINTRAC.[153] The record must be kept for at least five years from the day it was created.[154]

Large Virtual Currency Transaction Reports ("**LVCTR**")

The Compliance Officer must report the receipt of virtual currency in an amount equivalent to $10,000 or more in a single transaction and must submit an LVCTR to FINTRAC.[155] The Compliance Officer must also submit an LVCTR to FINTRAC in accordance with the 24-hour rule when the Company receives two or more amounts of virtual currency, that total $10,000 or more within a consecutive 24-hour window, and it's known that the transactions meet one of the following:[156]

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

The Company will use its then-current market prices to determine the value of the virtual currency in a given transaction, to determine if it meets the $10,000 and over reporting threshold.[157] If the Company does not have a market price, it will use and make a record of the market price published by Coinbase or another reputable provider of cryptocurrency services in Canada.

LVCTR can have 1-99 transactions. If there are more transactions, then the reports can be submitted with titles like this:

- Report 1 (LVCTR999-01): Transactions 1 to 99;
- Report 2 (LVCTR999-02): Transactions 100 to 198; and
- Report 3 (LVCTR999-03): Transactions 199 to 250.[158]

The Compliance Officer must submit an LVCTR to FINTRAC within five working days after the day the Company receives the amount.[159]

A record must be kept when the Compliance Officer submits an LVCTR to FINTRAC.

---

[151] https://fintrac-canafe.canada.ca/guidance-directives/transaction-operation/Guide7A/lctr-eng#s2-4.
[152] https://fintrac-canafe.canada.ca/guidance-directives/transaction-operation/Guide7A/lctr-eng#s2-4.
[153] PCMLTFR, SOR/2002-184, s. 144.
[154] PCMLTFR, SOR/2002-184, s. 148(1)(c).
[155] PCMLTFR, SOR/2002-184, ss. 7(1)(d), 19, 26, 30(1)(f), 33(1)(f), 40, 49, 55, 61, 67, 70(1)(d), and 79.
[156] PCMLTFR, SOR/2002-184, s. 129(1).
[157] PCMLTFR, SOR/2002-184, s. 125.
[158] https://fintrac-canafe.canada.ca/guidance-directives/transaction-operation/lvctr/lvctr-eng#s1.
[159] PCMLTFR, SOR/2002-184, s. 132(2).

LVCTR Exceptions

The following exceptions refer to the initial receipt of virtual currency, but any further transaction or activity may have reporting obligations, in addition to other obligations.

the Company is not required to submit an LVCTR if it receives two or more amounts in virtual currency that are each individually equivalent to less than $10,000, but together total $10,000 or more within 24 consecutive hours, when it's known the amounts are for a beneficiary that is:[160]

- a public body;
- a very large corporation or trust; or
- an administrator of a pension fund that is regulated under federal or provincial legislation.

The Company does not need to submit an LVCTR for the receipt of virtual currency in an amount equivalent to $10,000 or more in a single transaction if the virtual currency is received as:[161]

- compensation for the validation of a transaction that is recorded in a distributed ledger (a digital ledger that is maintained by multiple persons or entities and that can only be modified by a consensus of those persons or entities.); or
- a nominal amount of virtual currency for the sole purpose of validating another transaction or a transfer of information.

The Company is not required to submit an LVCTR if it receives virtual currency for its own operational purposes. For example, there is no need to report the receipt of virtual currency when it is received or purchased as holdings for the Company's business.

Compliance Control

FINTRAC has detailed instruction on how to gather and submit information relating to LVCTR which can be found at Annex 1: Field instructions to complete an LVCTR. The Compliance Officer must submit the LCVTR within 5 working days after receiving the amount.

The Compliance Officer must keep a copy of the LVCTR sent to FINTRAC.[162] The record must be kept for at least five years from the day it was created.[163] The appropriate records must be obtained and kept pursuant to what is stipulated by FINTRAC at the time the report is made.[164]

Electronic Funds Transfer Reports ("**EFTR**")

The Company must report EFTs that are $10,000 or more sent outside of Canada and coming from outside of Canada.[165] These transactions are subject to the 24-hr rule. These transactions include SWIFT MT 103 message transactions.

The above includes:

- the initiation, at the request of a person or entity, of an international electronic funds transfer of $10,000 or more in a single transaction, together with the information set out in Schedule 2 of the PCMLTFR if the electronic funds transfer is sent or is to be sent from one country to another;[166]

---

[160] PCMLTFR, SOR/2002-184, s. 129(2).
[161] PCMLTFR, SOR/2002-184, ss. 151(1) and (2).
[162] PCMLTFR, SOR/2002-184, s. 144.
[163] PCMLTFR, SOR/2002-184, s. 148(1)(c).
[164] PCMLTFR, SOR/2002-184, 30 (1)(f).
[165] PCMLTFR, SOR/2002-184, s. 30 (1).
[166] PCMLTFR, SOR/2002-184, s. 33 (1)(b).

- the final receipt of an international electronic funds transfer of $10,000 or more in a single transaction, together with the information set out in Schedule 3 of the PCMLTFR if the electronic funds transfer was sent from one country to another and the beneficiary is in Canada;[167]
- the initiation, at the request of a person or entity, of an international electronic funds transfer of $10,000 or more in a single transaction, together with the information set out in Schedule 2 of the PCMLTFR, if the Money Services Business also finally receives or is to finally receive the electronic funds transfer;[168]
- the final receipt of an international electronic funds transfer of $10,000 or more in a single transaction, together with the information set out in Schedule 3 of the PCMLTFR, if the Company also initiated the electronic funds transfer and the beneficiary is in Canada.[169]

- Guideline 8A: Submitting non-SWIFT Electronic Funds Transfer Reports to FINTRAC electronically;
- Guideline 8B: Submitting SWIFT Electronic Funds Transfer Reports to FINTRAC;

The Company will not report via paper, however, the link on guidance is below:
- Guideline 8C: Submitting non-SWIFT Electronic Funds Transfer Reports to FINTRAC by paper.

Compliance Control

The Compliance Officer must keep a copy of the EFTR sent to FINTRAC.[170] The record must be kept for at least five years from the day it was created.[171] The Compliance Officer must submit the EFTR within 5 working days after the transaction occurs. The appropriate records must be obtained and kept pursuant to what is stipulated by FINTRAC at the time the report is made.

24-hour rule

The 24-hour rule is a requirement to aggregate multiple transactions when they total $10,000 or more within a consecutive 24-hour window and the transactions are:

a) conducted by the same person or entity;
b) conducted on behalf of the same person or entity (third party), or
c) for the same beneficiary (person or entity).[172]

Some examples include:

- several transactions in amounts under $10,000 that total $10,000 or more;
- one transaction of $10,000 or more;
- several transactions in amounts under $10,000 and one or more transactions of $10,000 or more; or
- two or more transactions of $10,000 or more.[173]

The Company must report large virtual currency[174] and large cash transactions to FINTRAC in accordance with the 24-hour rule when:

---

[167] PCMLTFR, SOR/2002-184, s. 33 (1)(c).
[168] PCMLTFR, SOR/2002-184, s. 33 (1)(d).
[169] PCMLTFR, SOR/2002-184, s. 33 (1)(e).
[170] PCMLTFR, SOR/2002-184, s. 144.
[171] PCMLTFR, SOR/2002-184, s. 148(1)(c).
[172] PCMLTFR, SOR/2002-184, ss. 126, 127, 128, 129, and 130.
[173] https://fintrac-canafe.canada.ca/guidance-directives/transaction-operation/24hour/1-eng#annex3.
[174] PCMLTFR, SOR/2002-184, ss.129(1)(a) to (c).

- two or more amounts are received in VC/cash totalling $10,000 or more within a static 24-hour window, and they know that those transactions:

a) were conducted by the same person or entity;

b) were conducted on behalf of the same person or entity (third party); or

c) are for the same beneficiary (person or entity).

The Compliance Officer must be aware of certain exceptions (PCMLTFR, SOR/2002-184, ss. 129(2)(a) to (c)) to VC transactions totalling $10,000 or more.

the Company must report electronic funds transfers to FINTRAC in accordance with the 24-hour rule when they: [175]

- initiate two or more international EFTs (An electronic funds transfer other than for the transfer of funds within Canada) that total $10,000 or more within a static 24-hour window, and they know that the transactions:[176]

a) were initiated by the same person or entity;

b) were initiated on behalf of the same person or entity (third party);

c) or are for the same beneficiary (person or entity); or

- finally receive two or more international EFTs that total $10,000 or more within a static 24-hour window, and they know that the transactions:[177]

a) were initiated by the same person or entity; or

b) are for the same beneficiary (person or entity).

The Compliance Officer must be aware of certain exceptions (PCMLTFR, SOR/2002-184, ss. 127(2)(a) to (c) and 128(2)(a) to (c)) to international EFTs and EFTs totalling $10,000 or more. However, based on the Company's clients, it is unlikely that these exceptions will apply; therefore, this Compliance Plan and Policies are silent to further instruction.

The Company will use a static 24hr-window of 09:00 am to 08:59 am each day for the purposes of counting aggregate transactions (totalling 23:59 hours). Therefore, the Compliance Officer must ensure that when a person or entity has transmitted a total of $10,000 or more within that window, a large transaction has occurred and must report it to FINTRAC. For example, the Company receives $5,000 from A at 09:01am Monday, $6,000 at 07:00am Tuesday and $1,000 at 9:00am Tuesday. Only the $5,000 at 09:01am Monday and $6,000 at 07:00am Tuesday would count toward the static 24-window. FINTRAC provides other examples at annex 3 here.

Compliance Control

Record keeping requirements will be addressed under the "Record Keeping" heading.

[175] PCMLTFR, SOR/2002-184, s. 126.
[176] PCMLTFR, SOR/2002-184, ss.127(1)(a) to (c).
[177] PCMLTFR, SOR/2002-184, ss.128(1)(a) to (b).

Record Keeping

The recordkeeping scenarios below reflect statutory requirements applicable to MSBs generally and apply only where the corresponding activity is conducted.

This Compliance Plan and Policies has various requirements to keep records; however, the list below pertains to transaction records. The Company must keep records for the following:

1. Reports – a copy of every report sent to FINTRAC (already addressed above)
1.1. Suspicious Transaction Reports
1.2. Terrorist Property Reports
1.3. Large Cash Transaction Reports
1.4. Large Virtual Currency Transaction Reports
1.5. Electronic Funds Transfer Reports
2. Large virtual currency transaction records
3. Records of transactions of $3,000 or more
4. Records of remitting and transmitting $1,000 or more in funds by means other than an electronic funds transfer
5. Records of electronic funds transfers of $1,000 or more
6. Records of virtual currency transfers equivalent to $1,000 or more
7. Foreign currency exchange transaction tickets
8. Virtual currency exchange transaction tickets
9. Created or received internal memorandums about MSB/FMSB services,
10. Service agreement records

The Compliance Officer must ensure that the records are kept in such a manner that they can be accessed within 30 days of a request from FINTRAC.[178] A record (or a copy) may be kept in a machine-readable or electronic form, so long as a paper copy can easily be produced.[179]

2. Large cash transaction records

As an MSB, the Company must keep a large cash transaction record when it receives $10,000 or more in cash.[180]

*If the Company authorizes a person or an entity to receive funds on its behalf, and that person or entity receives $10,000 or more in cash in accordance with the authorization, the Company is deemed to have received the amount when it is received by the person or entity and must keep a large cash transaction record.[181]

Compliance Control

The Compliance Officer must ensure that large cash transactions are recorded. For manual processes, an example can be found in the Large Cash Transaction table in Schedule 5.

[178] PCMLTFR, SOR/2002-184, s. 149.
[179] PCMLTFR, SOR/2002-184, s. 147.
[180] PCMLTFR, SOR/2002-184, ss. 1(2) and 31.
[181] PCMLTFR, SOR/2002-184, s. 142(1) and 142(2).

Retention

The Company must retain records for at least five years from the date the large cash transaction record was created.[182]

3. Large virtual currency transaction records

As an MSB, the Company must keep a large virtual currency transaction record when it receives $10,000 or more in VC.[183]

*If the Company authorizes a person or an entity to receive funds on its behalf, and that person or entity receives $10,000 or more in VC in accordance with the authorization, the Company is deemed to have received the amount when it is received by the person or entity and must keep a large VC transaction record.[184]

Compliance Control

The Compliance Officer must ensure that large VC transactions are recorded. For manual processes, an example can be found in the Large Virtual Currency Transaction table in Schedule 5.

Retention

The Company must retain records for at least five years from the date the large virtual currency transaction record was created.[185]

4. Records of Transactions of $3,000 or more

Issuance of traveller's cheques, money orders or other similar negotiable instruments

When the Company receives an amount of $3,000 or more as consideration for the issuance of traveller's cheques, money orders or similar negotiable instruments from a person or entity other than another financial entity or a person who is acting on behalf of a client that is a financial entity, a record must be kept.[186] See the Issuance of Money Orders table in Schedule 5.

Redemption of money orders

When the Company redeems one or more money orders for a total value of $3,000 or more in funds or in an equivalent amount of VC at the request of a person or entity, a record must be kept.[187] See the Redemption of Money Orders table in Schedule 5.

Compliance Control

The Compliance Officer must ensure that the issuance or redemption of money orders for a total value of $3,000 or more in funds or in an equivalent amount of VC at the request of a person or entity are recorded. For manual processes, an example can be found in the Issuance of Money Orders table or the Redemption of Money Orders table in Schedule 5, as applicable.

Retention

The Company must retain records for at least five years from the date the record for a transaction of $3,000 or more was created.[188]

---

[182] PCMLTFR, SOR/2002-184, s. 148(1)(c).
[183] PCMLTFR, SOR/2002-184, ss. 1(2) and 32.
[184] PCMLTFR, SOR/2002-184, s. 143(1) and 143(2).
[185] PCMLTFR, SOR/2002-184, s. 148(1)(c).
[186] PCMLTFR, SOR/2002-184, s. 36(b).
[187] PCMLTFR, SOR/2002-184, s. 36(c).
[188] PCMLTFR, SOR/2002-184, s. 148(1)(c).

5. Records of remitting and transmitting $1,000 or more in funds by means other than an electronic funds transfer (e.g., Hawala)

Not applicable at this time.

6. Records of electronic funds transfers of $1,000 or more

Initiating an electronic funds transfer of $1,000 or more

When the Company initiates, at the request of a person or an entity, an electronic funds transfer (EFT) of $1,000 or more, the Company must record it.[189]

Sending an international EFT of $1,000 or more

When the Company sends, as an intermediary, an international EFT of $1,000 or more that was initiated by another reporting entity, the Company must record it.[190]

Final receipt of an international EFT of $1,000 or more

When the Company is the final recipient of an international EFT of $1,000 or more, the Company must record it.[191]

Compliance Control

The Compliance Officer must ensure that EFTs of $1,000 or more are recorded. (Although this information is typically recorded in a company's operational ledgers, an example for manual record keeping is provided in a table in Schedule 5.)

Retention

the Company must retain records for at least five years from the date the record for EFTs of $1,000 or more.[192]

7. Records of virtual currency transfers in amounts equivalent to $1,000 or more

VC transfer in an amount equivalent to $1,000

When the Company transfers VC in an amount equivalent to $1,000 or more at the request of a person or entity, the Company must record it.[193]

Receipt of VC in an amount equivalent to $1,000 or more for remittance to a beneficiary

When the Company receives VC in an amount equivalent to $1,000 or more for remittance to a beneficiary, the Company must record it.[194]

Compliance Control

The Compliance Officer must ensure that virtual currency transfers in amounts equivalent to $1,000 or more are recorded. (Although this information is typically recorded in a company's operational ledgers, an example for manual record keeping is provided in a table in Schedule 5.)

Retention

the Company must retain records for at least five years from the date the VC transfer or VC receipt record was created.[195]

---

[189] PCMLTFR, SOR/2002-184, s. 36(d).
[190] PCMLTFR, SOR/2002-184, s. 36(e).
[191] PCMLTFR, SOR/2002-184, s. 36(f).
[192] PCMLTFR, SOR/2002-184, s. 148(1)(c).
[193] PCMLTFR, SOR/2002-184, s. 36(g).
[194] PCMLTFR, SOR/2002-184, s. 36(h).
[195] PCMLTFR, SOR/2002-184, s. 148(1)(c).

8. Foreign currency exchange transaction tickets

The Company must keep foreign currency exchange transaction tickets, which may take the form of an entry in a transaction register, for every foreign currency exchange transaction the Company conducts, regardless of the amount.[196]

Compliance Control

The Compliance Officer must ensure that foreign exchange transaction tickets are recorded. (Although this information is typically recorded in a company's operational ledgers, an example for manual record keeping is provided in a table in Schedule 5.)

Retention

The Company must retain records for at least five years from the date the foreign exchange transaction record was created.[197]

9. VC exchange transaction tickets

The Company must keep VC exchange transaction tickets, which may take the form of an entry in a transaction register, for every VC exchange transaction the Company conducts, regardless of the amount. [198]

Compliance Control

The Compliance Officer must ensure that VC exchange transaction tickets are recorded. For manual processes, an example can be found in the VC exchange transaction tickets table in Schedule 5.

Retention

The Company must retain records for at least five years from the date the VC exchange transaction record was created.[199]

10. Created or received internal memorandums about MSB/FMSB services

Compliance Control

The Company must keep a record of every internal memorandum (i.e. any memo, note, message or similar communication) that it creates or receives in the normal course of business regarding MSB/FMSB services you provide to clients.[200]

Retention

The Company must retain records for at least five years from the date the internal memorandum record was created.[201]

11. Service agreement records

If the Company enters into an agreement with an entity to provide an MSB service covered under section 5(h) of the PCMLTFA, a record must be kept of it.[202]

Compliance Control

The Compliance Officer must ensure that records of service agreements are maintained. For manual processes, see the Service agreement table in Schedule 5.

---

[196] PCMLTFR, SOR/2002-184, ss. 1(2) and 36(i)
[197] PCMLTFR, SOR/2002-184, s. 148(1)(c).
[198] PCMLTFR, SOR/2002-184, ss. 1(2) and 36(j).
[199] PCMLTFR, SOR/2002-184, s. 148(1)(c).
[200] PCMLTFR, SOR/2002-184, s. 36(a).
[201] PCMLTFR, SOR/2002-184, s. 148(1)(c).
[202] PCMLTFR, SOR/2002-184, s. 37.

Retention
the Company must retain records for at least five years from the day the last transaction was conducted.[203]

Exceptions for VC

With respect to a transfer or receipt of VC as compensation for the validation of a transaction that is recorded in a distributed ledger OR an exchange, transfer or receipt of a nominal amount of VC for the sole purpose of validating another transaction or a transfer of information, the Company does not need to keep a record of:

- large VC transactions;
- transfers of $1,000 or more in VC at the request of a person or entity;
- receipt of $1,000 or more in VC for remittance to a beneficiary; or
- VC exchange transaction tickets.[204]

Travel Rule

The Company must ensure that the travel rule is met with every EFT or VC transfer. The travel rule is the requirement to ensure that specific information (listed below) is included with the information sent or received in an EFT or a VC transfer.[205] Information received under the travel rule cannot be removed from a transfer.[206]

Please note: the Travel Rule is not a separate record keeping requirement, rather, it is a rule to keep compliance with the legislation.

The required travel rule information for EFTs is:

- the name, address and account number or other reference number (if any) of the person or entity who requested the transfer (originator information);
- the name and address of the beneficiary; and
- if applicable, the beneficiary's account number or other reference number.[207]

The required travel rule information for VC transfers is:

- the name, address and the account number or other reference number (if any) of the person or entity who requested the transfer (originator information); and
- the name, address and the account number or other reference number (if any) of the beneficiary.[208]

What to do if the Company receives an EFT or VC that does not have the required information?
The Compliance Officer must take reasonable measures to obtain the missing information.[209] The Compliance Officer must consider the following:[210]

1. Does the name and address suggest anything suspicious (e.g., the name sounds fake, previously flagged client, high-risk location like Iran, North Korea or other regions)?
a. If yes, suspend the transaction and try and verify the transaction through established KYC procedures in this Program and contact the sending institution to verify the transaction.
b. If the issue persists, consider rejecting the transaction.

---

[203] PCMLTFR, SOR/2002-184, s. 148(1)(c).
[204] PCMLTFR, SOR/2002-184, ss. 151(1)(a) and (b).
[205] PCMLTFA, S.C. 2000, c 17, s. 9.5 and PCMLTFR, SOR/2002-184, ss. 124 and 124.1.
[206] PCMLTFA, S.C. 2000, c 17, s. 9.5.
[207] PCMLTFA, S.C. 2000, c 17, s. 9.5 and PCMLTFR, SOR/2002-184, s. 124(3).
[208] PCMLTFR, SOR/2002-184, s. 124.1(1)(a).
[209] PCMLTFA, S.C. 2000, c 17, s. 9.5(b) and PCMLTFR, SOR/2002-184, s. 124.1(1)(b).
[210] PCMLTFA, S.C. 2000, c 17, ss. 9.5(c) and 9.6(2) and PCMLTFR, SOR/2002-184 ss. 124(4) and 124.1(2).

Compliance Control

For EFTs/VCs, the Company must ensure travel rule information is included when and if EFTs/VC transfers are initiated[211] and when or if EFTs/VC transfers are received either as an intermediary or as the final recipient where applicable to the Company's activities.[212]

Ministerial Directives

In order for the Company to stay compliant with the relevant laws and regulations, the Compliance Officer must be up to date with the Ministerial Directives and transaction restrictions. Further, during an audit of the Company, FINTRAC has the right to examine records to ensure compliance with Ministerial Directives.[213]

FINTRAC will send the Company updates when there are changes to Ministerial Directives.

Directives will be reviewed at least every three years from the day they take effect.

The standard measures in the Directive vary from directive to directive. Therefore, the Compliance Officer must utilize the FINTRAC guidance related to the Ministerial Directives. Links to the latter can be found in Schedule 6.

Compliance Control

The Compliance Officer must update the Ministerial Directives table in Schedule 6 as and when updates are provided from FINTRAC.

[211] PCMLTFA, S.C. 2000, c 17, s. 9.5(a) and PCMLTFR, SOR/2002-184, s. 124(1).
[212] PCMLTFA, S.C. 2000, c 17, s. 9.5(b) and PCMLTFR, SOR/2002-184, s. 124(1).
[213] PCMLTFA, S.C. 2000, c 17, 11.42 (1).

This Schedules is maintained for regulatory completeness and future scalability and can not indicate that the Company currently performs all listed activities.

Schedule 1 – Appointment or Reappointment of the Compliance Officer

Compliance Officer Name	**Start of Appointment [d/m/y]**	**End of Appointment [d/m/y]**
Perpindervir Singh Patrola	4/6/2025	13/11/2025
Radim Pesak	13/11/2025	

Schedule 2 – Risk Assessment

Business-based risk assessment table[214]

Business relationships and/or high-risk clients Identify all the risk factors that apply to your business (including, products, services and delivery channels, geography, new developments and technologies, foreign and domestic affiliates and other relevant factors)	**Risk rating** Assess each risk factor (for example, low, medium or high).	**Rationale** Explain why you assigned a particular risk rating to each risk factor.	**Date (d/m/y)**

Relationship-based risk assessment table[215]

Business relationships and/or high-risk clients Identify all business relationships and/or high-risk clients (individually or as groups).	**Risk rating** Rate each business relationship and/or client (or group of clients) (for example, low, medium or high risk).	**Rationale** Explain why you assigned that particular rating to each business relationship and/or client (or group of clients).	**Date (d/m/y)**

Residual Risk Assessment table

Risk Rating	**Risk Rating Description**	**Residual Risk rating**	**Rationale**	**Date (d/m/y)**

[214] PCMLTFR, SOR/2002-184, s. 156(2).
[215] Ibid.

High Risk Monitoring table

Enhanced Monitoring (y/n)	Date (d/m/y)	What activity was flagged?	Enhanced Monitoring Action	Enhanced KYC of High-Risk Client	Notes

Schedule 3 – KYC

New Client Repository (person) – Government-Issued Photo Identification Method[216]

Person's name	Date of Verification	Type of ID document	Document number	Province or state and country that issued the document (if Iran or North Korea flag and see the Ministerial Directives section)	Expiry date (if applicable)	In-Person (y/n)	Where is it stored (copy saved in a computer file folder)	Notes

Verification Checklist table – Government-Issued Photo Identification Method

Requirements	(y/n)	Was this information recorded (y/n)
Authentic, valid and current		
Virtual verification process completed (if applicable)		
Be issued by a federal, provincial or territorial government (or by a foreign government if it is equivalent to a Canadian document)		
Indicate the person's name		
Include a photo of the person		
Includes a unique identifying number		
Matches the name and appearance of the person being identified		

New Client Repository (Corporation) table – Confirmation of Existence Method[217]

Corporation or Entity	Documents provided (y/n)	Where is it stored (copy saved in a computer file folder)

[216] PCMLTFR, SOR/2002-184, s. 108(a).
[217] PCMLTFR, SOR/2002-184, ss. 109(5) and 112(4).

KYC Verification table

Verification Trigger (e.g., large cash transaction)	Was Verification Conducted (y/n)	Description of transaction, include the person and purpose

Business Relationship Record table

Purpose and intended nature of the business relationship	Business dealings with the client	Types of transactions and activities that the client may conduct (helps for identifying suspicious transactions)	Is this information recorded elsewhere? If so, where?

Beneficial Ownership Records tables

Names of all directors of the corporation	Names and addresses of all persons who directly or indirectly own or control 25% or more of the shares of the corporation	Information establishing the ownership, control and structure of the corporation

Trust[218]	
Names and addresses of all trustees, known beneficiaries and known settlors of the trust	Information establishing the ownership, control and structure of the trust
[Example - Trustee: Sam Smith of Parliament Buildings, Victoria BC V8V 1X4 Canada]	

Widely Held or Publicly Traded Trust[219]		
Names and of all trustees,	The names and addresses of all s who directly or indirectly own or 25% or more of the units of the trust	Information establishing the ownership, control and structure of the trust

Entity other than a corporation or trust[220]

[218] PCMLTFR, SOR/2002-184, ss. 138(1)(b) and (d).
[219] PCMLTFR, SOR/2002-184, ss. 138(1)(a.1) and (d).
[220] PCMLTFR, SOR/2002-184, ss. 138(1)(c) and (d).

The names and addresses of all persons who directly or indirectly own or control 25% or more of the entity	Information establishing the ownership, control and structure of the entity

Not-for-profit organization[221]	
A charity registered with the Canada Revenue Agency under the Income Tax Act	An organization, other than a registered charity, that solicits charitable donations from the public

Third Party Information table

Person						
Name	Address	Telephone number	Date of birth	Occupation	Nature of the Business (sole proprietor only)	Relationship between the third and person or entity
					y	

	Corporation or another entity						
Name	Address	Telephone number	Nature of its principal business	Registration or incorporation number	Jurisdiction (province or state)	Country of issue of that number	Relationship between the third and person or entity

[221] PCMLTFR, SOR/2002-184, s. 138(5).

Suspected Third Party Information table

Why you suspect that the person or entity is acting on behalf of a third party[222]	When you receive cash in an amount of $10,000 or more, and are required to submit an LCTR to FINTRAC or to keep a large cash transaction record— whether according to the person who gave you the cash, they are acting on their own behalf only[223]	When you receive an amount of VC equivalent to $10,000 or more, and are required to submit an LVCTR to FINTRAC or to keep a large virtual currency transaction record—whether according to the person from whom you received the VC, they are acting on their own behalf only;[224]	When you open an account and are required to keep a signature card or an account operating agreement— whether according to a person who is authorized to act in respect of the account, the account will only be used by or on behalf of an account holder[225]	When you create an information record—whether, according to the person or entity for which the information record is kept, they are acting on their own behalf only[226]	When you are required to report a casino disbursement of $10,000 or more— whether, according to the person or entity that makes the request for the disbursement, they are acting on their own behalf only[227]

PEP and HIO table[228]

PEP or HIO – Name (including close family /associate) and organization name	Date of the determination;	Facts or suspicions about a PEP or HIO	Business relationship or transaction	Source of funds, including VC[229]	Source of wealth	If there is a high-risk of ML/TF, please provide periodic updates indicating ongoing monitoring (date of update, followed by written description)	ID verification and retention (Y/N)	Senior management reviewer and date of review (if applicable)	Notes

[222] PCMLTFR, SOR/2002-184, ss. 134(3)(b), 135(3)(b), 136(3)(b), 137(3)(b).
[223] PCMLTFR, SOR/2002-184, s. 134(3)(a).
[224] PCMLTFR, SOR/2002-184, s. 134(3)(a).
[225] PCMLTFR, SOR/2002-184, s. 135(3)(a).
[226] PCMLTFR, SOR/2002-184, s. 136(3)(a).
[227] PCMLTFR, SOR/2002-184, s. 137(3)(a).
[228] PCMLTFR, SOR/2002-184, s. 122(9).
[229] PCMLTFR, SOR/2002-184, ss. 122.1(1) and 157 and PCMLTFA, S.C. 2000, c 17, s. 9.6(3); PCMLTFR, SOR/2002-184, ss. 122.1(3) and 157 and PCMLTFA, S.C. 2000, c 17, s. 9.6(2).

Schedule 4 – Reporting

STR or Unusual Activity table

Suspicious transaction amount	Provide details of the facts (e.g., date, time, location, account details, particular business lines, the client's financial history or information about the person or entity) AND context (e.g., events leading up to the suspicious transaction, any KYC details recorded, previous transaction behaviours)[230]	ML/TF indicator	Analysis

TPR table

Terrorist Property Type	Provide details of the facts AND context	Was there an attempted or completed transaction associated with this property? If so, add this to the STR table and report to FINTRAC	Analysis

LVCTR table (use Annex 1: Field instructions to complete an LVCTR.)

General information – includes information about you, the reporting entity, and your 24-hour period for reviewing aggregate transactions	Transaction information – includes information about each transaction being reported	Starting action – includes information about how the transaction started	Completing action – includes information about how the transaction was completed	Record kept?	Notes

ETF and VC Records and Reporting

For the:

Initiation of $10,000+

Final Receipt of $10,000+

Receipt of VC,

[230] PCMLTFR, SOR/2002-184, s 85.

complete the forms made available by FINTRAC from time to time in paper format and/or through the F2R reporting system, each as set out in the PCMLTFR.

Schedule 5 – Transaction Records

Large Cash Transaction Table

Date the cash was received	Any person involved in the transaction (including the person from whom the Company received the cash), their name, address, date of birth, and occupation, or in the case of a sole proprietor, the nature of their principal business	Any entity involved in the transaction (including the entity from which the Company received the cash), their name, address and nature of their principal business; the type and amount of each fiat currency received	Method by which the Company received the cash (for example, in person, by mail, by armoured car, etc.)	Exchange rates used and their source (if applicable)	If an account was affected by the transaction, include: the account number and type of account; and the name of each account holder	Every reference number related to the transaction that is meant to be similar to an account number	Purpose of the transaction (for example, the cash was used to purchase a money order, etc.)	The following details about the remittance (i.e. the disposition) of, or exchange for, the cash received: the method of remittance (for example, wire transfer, money order, etc.); if the remittance is in funds, the amount and type of funds involved; if the remittance is not in funds, the type of remittance (for example, virtual currency, etc.) and value if different from the amount received in cash; and the name of every person or entity involved in the remittance, their account number or policy number. If there is no account or policy number, their identifying number

Large VC Transaction Table

Date the VC was received	Any person involved in the transaction (including the person from whom the Company received the VC), their name, address, date of birth, and their occupation, or in the case of a sole proprietor, the nature of their principal business	Any entity involved in the transaction (including the entity from which the Company received the VC), their name, address and the nature of their principal business	Type and amount of each VC involved in the receipt	Exchange rates used and their source	If an account was affected by the transaction, include: the account number and account type; and the name of each account holder	Every reference number related to the transaction that is meant to be equivalent to an account number	Every transaction identifier (this may include a transaction hash or similar identifier, if applicable), and every sending and receiving address

Issuance of Money Orders table

Date of the receipt the money order was issued	If the client is a person, their name, address, date of birth and their occupation, or in the case of a sole proprietor, the nature of their principal business	If the client is an entity, their name, address and the nature of their principal business	The total amount receive d	Whether the amount received is in funds or virtual currency and the type and amount of each type of funds and each of the virtual currencies involved	The number of every account that is affected by the transaction, the type of account and the name of each account holder	Every reference number that is connected to the transaction and has a function equivalent to that of an account number	If the amount received is in VC, every transaction identifier, including transaction hashes or similar identifiers (as applicable), and every sending and receiving address

Redemption of Money Orders table

Date the money orders were redeemed	If the client is a person, their name, address, date of birth and their occupation, or in the case of a sole proprietor, the nature of their principal business	If the client is an entity, their name, address and the nature of their principal business	The total amount of the money order or money orders	Name of the issuer of each money order	The number of every account that is affected by the redemption, the type of account and the name of each account holder	Every reference number that is connected to the redemption and has a function equivalent to that of an account number	If the redemption involves VC, every transaction identifier, including transaction hashes or similar identifiers (as applicable), and every sending and receiving address

Initiating an electronic funds transfer of $1,000 or more table

Date the EFT was initiated	Amount and type of funds involved in the initiation	If the client is a person, their name, address, telephone number, date of birth and their occupation, or in the case of a sole proprietor, the nature of their principal business	If the client is an entity, their name, address, telephone number and the nature of their principal business	The exchange rates used and their source	The name and address of each beneficiary	If an account is involved in the initiation: the account number and account type; and the name of each account holder	Every reference number related to the EFT that is meant to be similar to an account number	The number of every account that is involved in the EFT, other than those involved in the initiation

Sending an international EFT of $1,000 or more table

Date the EFT was sent	If fiat currencies were exchanged in the course of sending the EFT, the amount and type of each fiat currency involved in the exchange	The exchange rates used and their source	For every account involved in sending the EFT: the account number and account type; and the name of each account holder;	Every reference number related to sending the EFT that is meant to be similar to an account number	Name and address of the person or entity that requested the initiation of the EFT, unless the information was not included with the transfer and cannot be obtained by taking reasonable measures

Final receipt of an international EFT of $1,000 or more table

Date the EFT was finally received	Amount and type of funds involved in the final receipt	The name, address, telephone number, date of birth and in the case of a sole proprietor, the nature of their principal business or occupation of each person who is a beneficiary	The name, address, telephone number and the nature of the principal business of each entity that is a beneficiary	Date of remittance	Exchange rates used for the remittance and their source	If the remittance is in funds, the amount and type of funds involved in the remittance	If the remittance is not in funds, the type of remittance (for example, virtual currency, precious stones, etc.) and its value, if different from the amount of funds finally received	For every account involved in the final receipt or remittance: the account number and account type; and the name of each account holder	Every reference number related to the EFT that is meant to be similar to an account number	The name and address of the person or entity that requested the initiation of the EFT, unless that information was not included with the transfer and cannot be obtained by taking reasonable measures

VC transfer in an amount equivalent to $1,000 table

Date of the transfer	Amount and type of VCs that are involved in the transfer	If the client is a person, their name, address, date of birth and occupation, or in the case of a sole proprietor, the nature of their principal business	If the client is an entity, their name, address and the nature of their principal business	The name and address of each beneficiary	For every account involved in the transfer: the account number and account type; and name of each account holder	Every reference number related to the transaction that is meant to be similar to an account number	Every transaction identifier transaction hashes or similar identifiers (if applicable) and every sending and receiving address	Exchange rates used and their source

Receipt of VC in an amount equivalent to $1,000 or more for remittance to a beneficiary table

Date of the receipt	Amount and type of VCs that are involved	Name, address, date of birth and occupation, or in the case of a sole proprietor, the nature of the principal business of each person who is a beneficiary	Name, address and the nature of the principal business of each entity that is a beneficiary	Date of the remittance	Exchange rates used for the remittance and their source	If the remittance is in VC, the amount and type of each VC involved	If the remittance is not in VC, the type and value of the remittance, if different from the value of the VC received	For every account affected by the transaction: the account number and account type; and the name of each account holder	Every reference number related to the transaction that is meant to be similar to an account number	Every transaction identifier, including transaction hashes or similar identifiers (if applicable), and every sending and receiving addresses	The name and address of the person or entity that requested the transfer unless, that information was not included with the transfer and cannot be obtained by taking reasonable measures

Foreign currency exchange transaction tickets table

Date of the transaction	If the foreign exchange transaction was equivalent to $3,000 or more and requested by a person, their name, address, date of birth and occupation, or in the case of a sole proprietor, the nature of their principal business	If the foreign exchange transaction was equivalent to $3,000 or more and requested by an entity, its name, address and the nature of its principal business	The amount and type of fiat currency received from the client the type and amount of each fiat currency given to the client	The method by which the payment was made and received	The exchange rates used and their source	For every account involved in the transaction: the account number and account type; and the name of each account holder	Every reference number related the transaction that is meant to be similar to that of an account number

VC exchange transaction tickets table

Date of the transaction	If the VC transaction was equivalent to $1,000 or more and requested by a person, their name, address, date of birth and occupation, or in the case of a sole proprietor, the nature of their principal business	If the VC transaction was equivalent to $1,000 or more and requested by an entity, its name, address and the nature of its principal business	The amount and type of funds and the amount and type of VCs involved in the payment made and received by the person or entity that requested the exchange	The method (for example, a VC currency exchange business) by which the payment was made and received	The exchange rates used and their source	For every account involved in the transaction: the account number and account type; and the name of each account holder	Every reference number related the transaction that is meant to be similar to that of an account number	Every transaction identifier, (this may include a transaction hash or a similar identifier, if applicable), and every sending and receiving address

Service agreement records table

The name, address, date of birth, and occupation or in the case of a sole proprietor, the nature of their principal business of every person who signs the agreement on behalf of the entity;	**An information record about the entity, which must include: name and address of the entity; and the nature of the entity's principal business**	**If the entity is a corporation, a copy of the part of its official corporate records that contains provisions relating to the power to bind the corporation in respect of transactions with the MSB or FMSB** (this could include a certificate of incumbency, the articles of incorporation or the bylaws of the corporation (or their equivalents) that set out the directors and officers duly authorized to sign on behalf of the corporation. If there were subsequent changes to the articles of incorporation or bylaws that relate to the power to bind the corporation regarding transactions, and these changes were applicable at the time the service agreement record was created, the board resolution stating the change should be included in the record)	**A list that includes the name, address and date of birth of each of the entity's employees who are authorized to order a transaction under the agreement**	**A list that includes the name, address and date of birth of each of the entity's employees who are authorized to order a transaction under the agreement**

Schedule 6 - Ministerial Directives

Ministerial Directives table

Directives in force:

- November 15, 2025: Islamic Republic of Iran
- December 9, 2017: Democratic People's Republic of Korea (DPRK)

Schedule 7 – Client Verification Discussion

The Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) states under section 6 that, every entity described in section 5, is required to keep records and verify clients as per the regulations.[231] PCMLTFA section 5 subsection "h" describes Money Service Businesses running in Canada need to verify clients and keep records.[232] The Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFR) s.105 gives different methods on how to verify client identity. The verification can be done as follows[233]:

a) Using identification documents issued by a federal or provincial government or a foreign government that contain the client's name and photo.

b) Asking the federal or provincial government to verify the name, address or date of birth provided by the client.

c) Using the client's credit file that is located in Canada, been in Canada for more than three years and information is from more than one source and verifies name, address and date of birth.

d) Using two of following:

i. Using a reliable source to confirm name and address;

ii. Using a reliable source to confirm name and date of birth; and

iii. Using information that has clients name and states that the client hold a deposit account, credit card or loan with financial entity

e) Confirming that the following entities verified the clients identity as per s.105 (a)-(d) of PCMLTFR including their name, address and date of birth: a.

i. Entities listed in s.5 of PCMLTFA, those being banks, credit unions., insurance companies and trust & loan companies affiliated to MSB;
ii. Entity that carries on business similar to MSB outside of Canada and is affiliated to MSB entity; and
iii. Entity that is a financial entity and is member of same financial group as MSB.

A. VERIFYING CLIENTS PHYSICALLY PRESENT

---

[231] https://lois-laws.justice.gc.ca/eng/acts/P-24.501/page-1.html#h-398238, Section 6
[232] 2 https://lois-laws.justice.gc.ca/eng/acts/P-24.501/page-1.html#h-398238, Section 5
[233] 3 https://lois-laws.justice.gc.ca/eng/regulations/SOR-2002-184/page-9.html#h-1296053, section 105

To verify a client physically present the PCMLTFR allows that a client can be verified by:

a) using government issued identification;[234]
b) asking the government to verify client;
c) using a client credit file that has been in Canada for three years or more and has more than one source whereas sources being a loan, credit card or other credit items on a credit file;[235]
d) using two reliable sources to verify name, address and date of birth;[236] and
e) confirming information with affiliated entities that have verified the client using section 105 of the PCMLTFR.[237]

The government has provided videos on how to verify clients using above-mentioned methods “a” and “c”, as follows:

d) https://fintrac-canafe.canada.ca/training-formation/id/id-eng
e) https://fintrac-canafe.canada.ca/training-formation/id/id2-eng

B. VERIFYING CLIENTS NOT PHYSICALLY PRESENT

To verify a client not physically present FINTRAC guidance provides that a client can be verified by using government identification but the identification needs to be validated. The process is in two parts, as follows:

a) To validate and authenticate that the identification is real and valid;[238] and
b) To match the photo of person on the identification to the person who is providing the Information.[239]

---

[234] https://fintrac-canafe.canada.ca/guidance-directives/client-clientele/Guide11/11-eng#s2a
[235] https://fintrac-canafe.canada.ca/guidance-directives/client-clientele/Guide11/11-eng#s2b
[236] https://fintrac-canafe.canada.ca/guidance-directives/client-clientele/Guide11/11-eng#s2c
[237] https://fintrac-canafe.canada.ca/guidance-directives/client-clientele/Guide11/11-eng#s2d
[238] https://fintrac-canafe.canada.ca/guidance-directives/client-clientele/Guide11/11-eng#s2a
[239] ibid

The guidance given for validating the identification by FINTRAC is to scan or take a picture of the identification and use technology to validate that the document provided is real by observing "characteristics (for example, size, texture, character spacing, raised lettering, format, design), security features (for example, holograms, barcodes, magnetic strips, watermarks, embedded electronic chips) or markers (for example, logos, symbols)" with government identifications of the same country.[240]

To match the photo on the identification with the client who has provided identification, the client can be viewed using live video chat with the client showing the identification with them **OR using facial recognition technology to match the identification with a selfie image of the client that will be provided by the client.**[241]

Given the foregoing, many MSB businesses engage with third-party businesses to provide such facial recognition/KYC services. *The Company may wish to do so as well, and refer to such engagement of third party service provider in the relevant policy and compliance documents.*

C. SAMPLE PROCEDURE FOR VERIFYING CLIENTS NOT PHYSICALLY PRESENT

Based on the above information, the Company may choose to incorporate the following procedures when verifying clients who are not physically present:

a) Clients must submit a copy of valid government issued ID documents (front and back) using a mobile advice or high-quality webcam. These documents must be picture ID, such as:

i. Driver's Licenses;
ii. Passports;
iii. Identity Cards; and
iv. Resident Permits.

b) Clients submit a "selfie" of themselves holding the government issued ID they submitted as well

[240] ibid
[241] ibid

as a paper with the name of the Company and the current date.

c) The Company will use technology, to validate that the government issued ID provided is real by observing “characteristics (for example, size, texture, character spacing, raised lettering, format, design), security features (for example, holograms, barcodes, magnetic strips, watermarks, embedded electronic chips) or markers (for example, logos, symbols) with government identifications of the same country;

d) The Company will use facial recognition technology, to match the government issued ID provided by the client with the “selfie” provided by the client, which technology will generate a report confirming the verification of the client and the date of such verification (the “**Verification Report**”);

e) The Verification Report will include a copy of the relevant government issued ID and “selfie” provided by the client, and the Verification Report will be saved to the client’s electronic file.

f) The verified client will be onboarded.