MERKLE SCIENCE

A GUIDE TO THE CANADIAN REGULATIONS FOR CRYPTOASSET BUSINESSES

TABLE OF CONTENTS

OVERVIEW OF CRYPTOCURRENCY REGULATIONS IN CANADA

Canada started regulating the entities dealing with virtual currencies on 11 February 2014 by bringing them under the purview of Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) .On 24 August 2017, the Canadian Securities Administrators (CSA) — which provides guidance to Canada's provincial and territorial securities regulators — issued a staff notice which extended the application of securities law to cryptocurrencies.

The Financial Transactions and Report Analysis Centre of Canada (FINTRAC) is Canada's financial intelligence unit with a mandate to facilitate the detection, prevention and deterrence of money laundering and the financing of terrorist activities while ensuring the protection of personal information under its control.

According to FINTRAC, virtual currency is defined as a digital representation of a value that can be used for payment, investment or retail activities such as buying and selling of goods and services. The definition of virtual currencies includes blockchain-based such as bitcoins.

This definition, however, does not include certain kinds of digital currencies. Digital currencies used in virtual economies, such as those present in online games, are not included in this definition because these digital currencies can only be used for redeeming gift cards or loyalty programmes. Such digital currencies can neither be converted into fiat currencies nor be exchanged for virtual currencies; therefore, they can not be used for investment, payments, and retail transactions.

Entities dealing in virtual currencies include those entities that offer virtual currency exchange services and virtual currency transfer services. Virtual currency exchanges services include exchanging funds for virtual currency or vice versa and one virtual currency for another virtual currency.

As per the CSA, if a coin or token is deemed to be a security, then businesses issuing such coin has to meet the registration and prospectus requirements. Accordingly, CSA noted that "Securities may only be sold after a receipt has been received from a securities regulatory authority for a comprehensive disclosure document called a "prospectus", or pursuant to a private placement in reliance on a prospectus exemption."

Under FINTRAC, Crypto Asset Trading Platforms are Money Service Businesses

FINTRAC has oversight over crypto-asset trading platforms (CTPs — the preferred term used by Canadian regulators for crypto exchanges), which are regulated as Money Service Businesses (MSBs) under the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFA).

Under FINTRAC, entities dealing in virtual currencies fall under the definition of domestic MSBs. These MSBs need to be (a) incorporated in Canada, (b) physically located in Canada, and (c) have employees, agents or branches in Canada.

FINTRAC also regulates foreign money service businesses (FMSBs). FMSBs include those entities that do not have a place of business in Canada but direct their MSB services towards individuals or businesses in Canada. Foreign crypto trading platforms that cater to Canadian clients fall under the

CTPs facilitate the exchange of:	Virtual currency transfers include:
• funds for virtual currency (fiat to crypto) • virtual currency for funds (crypto to fiat) • virtual currency for another virtual currency (crypto to crypto)	• transferring virtual currency at the request of a client (on behalf of someone else) • receiving a transfer of virtual currency for remittance to a beneficiary (on behalf of someone else)

definition of FMSBs and are required to fulfil all the obligations that are placed on MSBs such as implementing a compliance programme and registering with FINTRAC.

According to FINTRAC, entities "dealing" with virtual currencies include both virtual currency exchanges (CTPs) and virtual currency transfer services. CTPs and virtual currency transfers dealing in virtual currencies must register with FINTRAC as MSBs.

On 23 March 2021, FINTRAC updated its Know Your Customer Guidance. As per the new guidance, MSBs in Canada will have to put in place robust KYC compliance programs in line with PCMLTFA from 1 June 2021.

Additionally, cryptocurrencies are also covered under the Income Tax Act. The Canadian Revenue (CRA) identifies cryptocurrencies as commodities. However, exchanging cryptocurrencies for goods and services falls under barter transactions and is taxed accordingly.

FEDERAL GOVERNMENT ENTITIES REGULATING CRYPTO

(i) Federal Level Registration Requirements for Crypto Trading Platforms (CTPs)

On 29 March 2021, the Investment Industry Regulatory Organization of Canada (IIROC) — a national self-regulatory organization that oversees all investment dealers and trading activity — along with the CSA, issued Staff Notice 21-239. The staff notice provides guidance on how securities legislation will apply to CTPs that "facilitate or propose to facilitate the trading of (a) crypto assets that are **securities** and (b) crypto assets that are not securities (such as Bitcoin) but which the CSA view as instruments or contracts that are subject to Canadian securities and/or derivatives regulation due to their trading processes and structures (**Crypto-Asset Contracts**)."

Per the above definition, CTPs that do not immediately settle crypto trades fall under the scope of crypto-asset contracts. If the users do not take direct possession of the crypto assets in their personal wallet, then there is an obligation on the CTPs to give such users their crypto-asset at a later date. While the trade is not immediately settled, a crypto-asset contract is considered a security and is therefore covered by securities law. The press release accompanying the Notice directs Canadian and global CTPs, which provide services to Canadian-resident users, to contact the CSA and discuss the registration process and application requirements. The notice clarifies that the Canadian regulation will apply to CTPs that have users in one or more Canadian provinces.

Should CTPs fail to comply with the notification requirements, they stand to face possible enforcement action. The CSA clarified that it may entertain exemptions to the existing frameworks and, in certain circumstances, permit a "two-year interim period registration approach" before full compliance is attained. As per the notice, if the CTPs deal in "securities then they will have to, based on their business activities, be further classified and registered as 'Marketplace Platforms' or 'Dealer Platforms'. CTPs need to consider in light of their business model and with the help of legal advisors whether they should be regulated as a dealer or a marketplace.

Marketplace Platforms brings together multiple parties to trade tokens or crypto asset contracts	**Dealer Platforms** buy and sell orders do not interact directly with each other and the dealer is the counterparty for every client trade
• Constitute, maintain or provide a market or facility for bringing together buyers and sellers parties to in Security Tokens and/or Crypto Contracts • Bring together orders of security tokens and/or Crypto Contracts of buyers and sellers or parties to the contracts • Use established, non-discretionary methods under which orders for Security Tokens and/or Crypto Contracts interact with each other and buyers and sellers or parties entering the orders to agree on the terms of trade	• Distribute security tokens • Trade security tokens • Enter intro crypto contracts exclusively on prospectus exempt basis (i.e. only selling to accredited investors) and that do not offer margin or leverage • Dealer Platforms that offer margin or leverage for Security Tokens must be registered as an investment dealer (under the relevant provincial securities regulators) and are IIROC members.

a) Dealer Platform Registration

Per the Notice, **Dealer Platforms** are those "platforms that (a) solely distribute or (b) trade security tokens, or (c) enter into crypto contracts exclusively on prospectus exempt basis and that do not offer margin or leverage." In general, if buy and sell orders on the CTP do not interact directly with each other and the dealer is the counterparty for every client trade, then the dealer platform registration will most likely apply.

In order to bring their operations into compliance, CTPs should seek clarification regarding the registration process and other relevant requirements directly from their local securities regulators. After seeking such clarification, they should analyze their business models and actively take steps to design an 'internal interim regulatory plan'. The CTPs should then approach IIROC with this plan and get 'restrictive registration' or a customized exemption before being accorded the full investment dealer status.

For those applying for dealer registration, CTPs should complete these tasks within a timeframe of two years to be recognized as investment dealers and receive IIROC membership. The platforms that use crypto asset contracts rather than security tokens will find some relief in form of exemptions such as dispensation from prospectus filing requirements and countertrade reporting requirements.

Dealer Platforms are required to register under the appropriate category of dealer registration. A Dealer Platform that "does not offer margin or leverage, and solely facilitates the distribution of Security Tokens pursuant to prospectus exemptions, will generally be required to register as an exempt market dealer, or a restricted market dealer, as appropriate." However, any Dealer Platforms offering margin or leverage for Security Tokens must register as an investment dealer and obtain IIROC membership.

The Notice also outlines that "Dealer Platforms trading Crypto Contracts are required to register under an appropriate dealer category and where they trade or solicit trades for retail investors that are individuals, they will generally be required to register as an investment dealer (under the corresponding provincial securities regulator such as the Ontario Securities Commission) and obtain IIROC membership."

b) Marketplace Platform Registration

A CTP has to be regulated as a marketplace rather than a dealer if the CTP operates a market or facility for bringing together multiple buyers and sellers or parties to trade in tokens or crypto asset contracts. In those circumstances, the CTP will generally be required to obtain IIROC membership, operate under the oversight of the CSA, and most likely will wind up being regulated under the national marketplace instrument, NI 21-101, as an "alternative trading system" aka ATS.

The **Marketplace Platform** has to fulfil the following three requirements:

a. Constitute, maintain or provide a market or facility for bringing together buyers and sellers parties to in Security Tokens and/or Crypto Contracts;
b. Bring together orders of security tokens and/or Crypto Contracts of buyers and sellers or parties to the contracts; and
c. Use established, non-discretionary methods under which orders for Security Tokens and/or Crypto Contracts interact with each other and buyers and sellers or parties entering the orders to agree on the terms of trade.

Because Marketplace Platforms have multiple buyers and sellers, they are also subject to requirements such as IIROC's Universal Market Integrity Rules (UMIR). There are also clearing and settlement arrangements that must be followed, which also has its own set of regulatory requirements. Other relevant instruments include: National Instrument 23-101 Trading Rules (NI 23-101) and National Instrument 23-103 Electronic Trading and Direct Electronic Access to Marketplaces (NI 23-103)

c) Hybrid Dealer and Marketplace Platforms
The Notice also points out that some platforms may have characteristics of both dealer and marketplace platforms. That situation calls for a more complex discussion with FINTRAC and the CSA that may result in a customized suite of exemptions from rules.

ii) Requirements for FINTRAC Registration
As previously mentioned, MSBs have to register with FINTRAC and comply with PCMLTFA and its associated regulations going forward. Every cryptocurrency business or dealers in virtual currency had to register with FINTRAC effective 1 June 2020.

As per FINTRAC, every virtual currency business subject to the PCMLTFA regulations must develop a comprehensive and effective AML compliance program. According to FINTRAC, this is the basis for meeting all regulatory requirements under the PCMLTFA and its associated Regulations.

MSBs must appoint an individual who will be responsible for implementing the compliance program and the first point of contact for FINTRAC. Based on the organization's size, this individual can be the owner of the business, an employee, or an independent AML compliance professional.

Each virtual currency business must develop and maintain AML policies and procedures manual, which must be approved by a senior member of the organization and kept up to date. At a minimum, the AML policy must include a procedure for (a) establishing a business relationship with client (b) client identification (c) Third Party beneficiary determination (d) Record Keeping (e) Reporting suspicious activities (f) Reporting large virtual currency transactions.

FINTRAC stated that it will exercise flexibility and reasonable discretion in the course of assessing reporting entities' compliance programs, and noting that it will not begin to conduct compliance assessments with respect to the new obligations until April 1 2022. Accordingly, from 1 June 2021 - 31 March 2022, FINTRAC will only assess reporting entities' compliance programs against the regulatory regime in force before1 June 2021.

iii) Politically Exposed Persons
All Reporting Agencies must determine if their clients are "**politically exposed persons**" (PEP) and provide additional risk assessments of such clients. To stay compliant with PCMLTFA regulations, reporting entities are required to screen both Foreign and Domestic PEPs as well as Head of International Organizations.

In February 2021, FINTRAC updated its guidance on (PEP) and heads of international organizations (HIOs), as well as related guidance for account-based reporting entity sectors, including "securities dealers" (i.e. dealers and advisors). This guidance came into effect on June 1, 2021.

Domestic PEPs include those individuals who hold or have held within the last 5 years, a specific office or position on behalf of the Canadian federal, provincial, or municipal government such as governor-general, member of the Senate or House of Commons, and deputy minister.

A person ceases to be a domestic PEP 5 years after they have left office or 5 years after they are deceased. This means that reporting entities must continue to mitigate the risk associated with domestic PEPs or their family members, ex-spouse and partners till they cease to be domestic PEPs. This 5-year rule is also applicable to HIOs.

An **HIO** is an individual who holds or has held, within the last 5 years, the office or position of an international organization. Such international organization must be either established under a treaty or by another institution that is also set up by an international organization. To be deemed an international organization the following conditions have to be met:

a. The International Organization is set up by governments of more than one country
b. Conducts activities in several countries
c. It is bound by a formal agreement among member countries
d. It has its own legal status

Essentially, HIO is a person who leads the organization, for example, the president or a general secretary. An HIO would be subjected to FINTRAC's PEP and HIO guidance, irrespective of whether he is a Canadian citizen or not.

A **Foreign PEP** is a person who holds an office or positions listed out by FINTRAC in a foreign state or on behalf of it. These positions include head of state or government, deputy minister, ambassador, and head of government agencies amongst others. The aforementioned entities fall under the category of the foreign state regardless of citizenship, residence status or birthplace. Unlike HIOs and domestic PEPs, once an individual is designated as foreign PEP he remains a foreign PEP forever (this includes deceased PEPs).

a) Treating PEPs and HIOs as High-Risk Clients

As per FINTRAC, the access, influence and control that PEPs and HIOs have can make them vulnerable to corruption, and potential targets of criminals who could exploit their status and use them — knowingly or unknowingly — to carry out AML/CFT offences. Further, the family members and close associates of PEPs and HIOs fall under the list of potential targets as well because they can more easily avoid detection.

According to FINTRAC, MSBs must prima facie flag foreign PEPs, along with family members or close associates, as high-risk clients. However, domestic PEPs, HIOs, or their family members or close associates can only be flagged as high risk after MSBs conduct a thorough risk assessment. After the risk assessments, if the MSBs find that there is a high chance of an AML/CFT offence being committed, then these entities can be flagged as high risk.

Once the MSBs determine that there is a high risk of an AML/CFT offence being committed by PEPs or HIOs, they must adhere to PCMLTFA Regulations and FINTRAC's risk assessment guidance for PEPs and HIOs. MSBs are also required to closely monitor PEPs and HIOs and take additional measures to ensure compliance with PCMLTFA regulations. These measures have to be documented in a separate set of written compliance policies and procedures created for PEPs and HIOs.

b) Enhanced Measures

Enhanced Measures are the additional controls and processes that the MSBs have to put in place to manage and reduce the risks associated with their high-risk clients and business areas. As mentioned above, MSBs must in their compliance programme develop a set of written policies and procedures that give details of the enhanced measures that MSBs will take to mitigate the AML/CFT risks if their clients are identified as high.

The policies and procedures developed by MSBs must include:

a. MSBs should explain how they are going to conduct risk assessments. MSBs should then conduct the risk assessment process and ascertain the level of risk attached to each client.
b. After the risk assessment, MSBs will have to list the additional steps that it is going to take to verify the identity of a person or an entity.
c. MSBs should obtain additional information on clients they consider to be high risks, such as information from public databases and the internet.
d. They should also obtain information on the clients' source of funds or source of wealth.
e. MSBs must routinely update high-risk clients' identification and beneficial ownership information. The frequency at which this information has to be updated depends upon the level of risk attached to each client.
f. Further, MSBs should also conduct ongoing

monitoring of business relationships that high-risk clients maintain. The frequency of the monitoring process is based on the level of risk.

g. Obtain information on the reasons for attempted or conducted transactions.

iv) KYC & The Travel Rule

The Canadian financial intelligence unit requires all obligated reporting entities, including MSBs that received over CA$10,000 in a virtual currency transaction, to collect transaction details, identify the originator party and report the transaction to FINTRAC.

On 10 July 2019, FinCEN published final amendments to PCMLTFA. Prior to the amendment, reporting entities could only rely on documents that were "**original, valid and current**" to verify customer identity. This impeded the ability of reporting entities to carry out their operations electronically in a non-face-to-face environment.

The requirement that an identity document is "original" has been removed and reporting entities can now rely on documents that are "valid, authentic and current." This means that reporting entities can rely on scanned and photocopied documents. This change came into force on 25 June 2019 and took immediate effect.

a) Expanding on the 2019 amendment

On 1 June 2021, more amendments to PCMLTFA came into force. The amendment to the travel rule now requires specific identifying information to be recorded when an electronic funds transfer (EFT) or virtual currency transfer is sent or received.

All reporting entities including MSBs have to submit an electronic funds transfer report to FINTRAC when they initiate or receive funds electronically in an international transaction. The threshold for reporting transactions is set to $10,000 or more for a single transaction or multiple small transactions that take place over a 24-hour period.

As per the 2021 amendments, identifying information includes the (a) name, address and account or another reference number (if any) of the person or entity who requested the transfer, (b) name and address of the beneficiary, and (c) if applicable, the beneficiary's account or other reference numbers. The FINTRAC has extended these requirements to include not just domestic MSBs and financial institutions but also foreign MSBs (and casinos with respect to EFTs).

b) Suspicious Transaction Reporting

The revised regulations require suspicious transactions or attempted transactions to be reported to FINTRAC "as soon as reasonably practicable" after reporting entities have taken measures that enable them to establish that there are reasonable grounds to suspect that a transaction or attempted transaction is related to a money laundering offence or a terrorist financing activity offence.

c) 24 Hour Rule

The amendments (1) clarify that multiple transactions within a 24-hour period are considered to be a single transaction when they total $10,000 or more, (2) ensure that the 24-hour rule applies to beneficiaries of multiple transactions, and (3) clarify that only one report should be submitted for all aggregated transactions within a 24-hour period.

d) Client Identification

Previously, reporting entities could either conduct client identification themselves or rely on information collected by an agent or affiliate. The amendments expand this to permit reporting entities to rely on customer identification information that has been previously obtained by another reporting entity, subject to certain requirements being met.

e) Beneficial Ownership

Beneficial ownership refers to the natural person or persons who ultimately own a legal entity. Within the Canadian guidelines, beneficiaries have to take reasonable measures to confirm the accuracy of

beneficial ownership information in the course of ongoing monitoring.

v) Privacy Laws in Canada
Canada has a comprehensive legal framework that governs the protection of the personal information of individuals in both public and private sectors. The primary source of constitutionally enforced privacy rights in Section 8 of the Canadian Charter of Rights and Freedoms.

The Office of the Privacy Commissioner (OPC) oversees compliance with federal privacy laws. Canada also has two privacy laws: the Privacy Act which covers the personal information-handling practices of federal government departments and agencies. The second one is the Personal Information Protection and Electronic Documents Act (PIPEDA) which applies to the commercial transactions of organizations that operate in Canada's private sector.

Section 5 of PIPEDA notably contains specific obligations concerning the organization's collection, dissemination, and use of customer's personal information. Section 7(3)(d) states that an organization may, without the individual's knowledge or consent or judicial authorization, disclose personal information that it believes could be useful in investigations in case any laws have been broken — whether federal, provincial, or those of a foreign jurisdiction. This obligation is also applicable to the MSBs

If a province or territory has its own set of privacy laws, then provincial law applies; if a province or territory does not have its own privacy laws, then federal law applies. Alberta, British Columbia, and Quebec notably have legislation that applies to private sector businesses like MSBs that collect, use, and disclose personal information while carrying out business within these provinces. If there is information transfer involved in any province-to-province transfers, then federal law applies.

vi) Guidelines from the Investment Industry Regulatory Organization of Canada (IIROC)
On 16 January 2020, the IIROC and CSA published a joint staff notice to provide guidance on how securities legislation would apply to entities that facilitate transactions relating to crypto assets, including buying and selling of crypto.

The staff notice explained that in some cases, clear bifurcation can be made between security and derivatives. For example, a tokenized security carries rights traditionally attached to common shares such as voting rights and rights to receive dividends. On the other hand, a crypto asset is considered a derivative when a token provides an option to acquire an asset in the future.

Further, IIROC also stated that the securities legislation may apply to those platforms that facilitate the buying and selling of crypto assets, including crypto assets that are commodities, because the user's contractual right to the crypto asset may itself constitute a derivative.

Where does the securities legislation not apply?
Platforms would not be subjected to securities legislation if each of the following applies: (a) the underlying crypto asset itself is not a security or derivative and (b) the contract or instrument for the purchase, sale, or delivery of crypto assets results in an obligation to immediately deliver and settle the crypto asset to the platform's typical commercial practice.

vii) Regulatory Sandbox
The CSA Regulatory Sandbox is an initiative of the Canadian Securities Administrators (CSA) to support fintech businesses seeking to offer innovative products, services, and applications in Canada. It allows firms to register and/or obtain exemptive relief from securities laws requirements, under a faster and more flexible process than through a standard application, in order to test their products, services and applications throughout the Canadian market on

a time-limited basis.

Firms that want to apply should be ready to provide CSA with live environment testing, a business plan, and a discussion of potential investor benefits, including how the product or service will minimize investor risks. Firms that intend to operate in the CSA Regulatory Sandbox should be prepared to provide CSA staff with data on their operations for monitoring and data collection purposes. Participating firms are subject to CSA compliance reviews and surveillance.

Firms that are interested in participating in the initiative should also contact their local securities regulator to discuss the firm's business model and applicable securities law issues. The firm's local securities regulator will analyze each business model on a case-by-case basis.

HIGHLIGHTS OF SECURITIES LAWS IN KEY PROVINCES

i) Ontario

The Ontario Securities Commission (OSC) expectations are consistent with the **regulatory framework** issued by the Canadian Securities Administrators (CSA). As part of this framework, platforms currently facilitating trading in security tokens or instruments or contracts involving crypto assets in Canada are required to register as an investment dealer and become a member of the Investment Industry Regulatory Organization of Canada (IIROC). An interim registration approach may be available, as described in the framework. Platforms located outside of Ontario that allow Ontarians access are regarded as operating in Ontario for the purposes of securities regulation

On 29 March 2021, Ontario Securities Commission issued a staff notice notifying crypto-asset trading platforms "that currently offer trading in derivatives or securities to persons or companies located in Ontario, must bring their operations into compliance with Ontario securities law or face potential regulatory action."

On 25 May 2021, the OSC issued a press release announcing the publication of the **Statement of Allegations** against Polo Digital Assets, Ltd. (Poloniex) for failing to comply with Ontario securities law. Poloniex, incorporated in the Republic of Seychelles, is operating an unregistered crypto asset trading platform, encouraging Canadians to use the platform, and allowing Ontario residents to trade crypto asset products that are securities and derivatives. The OSC continues to add unregistered crypto-asset trading platforms to its Investor Warning List.

Crypto-asset trading platforms had to contact OSC staff by 19 April 2021, to discuss how to bring their operations into compliance. If a platform that is currently trading in derivatives or securities in Ontario does not do so by the deadline, the OSC will take steps to enforce its securities law requirements.

The notice also states that the "OSC is aware of platforms seeking to become reporting issuers through initial public offerings or through reverse take-overs, changes of business, Capital Pool Company qualifying transactions or similar transactions. Platforms must contact OSC staff at **cryptocompliance@osc.gov.on.ca** if they intend to become reporting issuers through an initial public offering or other transaction."

ii) British Columbia

On 7 April 2021, the British Columbia Securities Commission (BCSC) issued a clarification of requirements for crypto asset trading platforms in line with the CSA Staff Notice 21-329 (as mentioned above).

The notification stated that the platforms headquartered in British Columbia that facilitate trading in crypto assets that are securities or derivatives, or in instruments or contracts based on crypto assets, are expected to immediately start engaging with the BCSC to obtain authorization from appropriate regulatory authorities if they have not done that.

If a platform operating in British Columbia is headquartered in another Canadian province or territory, the platform is expected to communicate with the securities regulator where it is headquartered.

On 25 January 2021, BCSC released an early intervention notification urging British Columbia residents to exercise caution when dealing with firms that are not registered to trade or advise in BC such as Mercury Crypto Invest.

iii) Alberta

When it comes to crypto, the Alberta Securities Commission has mostly been focused on enforcement. However, the ASC recently began to get their toes wet with its crypto registration. On 8 July 2021, Tetra Trust became Canada's first regulated custodian for cryptocurrency assets after being registered by the Alberta Government

iv) Quebec

The Autorité des marchés financiers (AMF) is the organization responsible for financial regulation in Quebec. Quebec's Money-Services Businesses Act, which came into effect on 1 April 2012, implies that businesses providing money services, including conversions, fund transfers, issuance or redemption of traveller's checks, money orders or bank drafts, check to cash, and the operation of privately owned ATMs, must acquire the appropriate licensing from the AMF. These applications are to be reviewed by the AMF, the Sûreté du Québec (Quebec's provincial police service), and the local municipal police.

Per the Money-Services Businesses Act, identifying information about the MSBs' directors, officers, and partners must be provided. While the AMF oversees businesses conducting crypto transactions, the organization does not regulate digital currencies.

As of February 2015, cryptocurrency ATMs and exchanges have been included in Quebec's Money-Services Business Act. This means that a cryptocurrency ATM operator or exchange needs to register with FINTRAC, abide by the PCMLTFA, receive a license from theAMF, and comply with AMF regulations to operate their crypto business in Quebec.

COMPLIANCE AND REPORTING REQUIREMENTS FOR MSBs

i) Ongoing Monitoring Requirements

On 1 February 2021, FINTRAC released ongoing monitoring requirements under PCMLTFA for all reporting entities including MSBs, meaning that reporting entities must develop a process to review the information that they have obtained about the clients with whom they have business relationships.

Ongoing monitoring is done for the following reasons:

a. Detect any suspicious transactions that the MSBs are required to report to FINTRAC;
b. Keep client identification information, beneficial ownership information, and the purpose and intended nature of the business relationship record up to date;
c. Reassess the level of risk associated with your client's transactions and activities;
d. Determine whether transactions or activities are consistent with the client information you obtained and your risk assessment of the client.

The MSBs must conduct transaction monitoring as soon as they enter into a business relationship with a client. Further, they must also conduct periodical monitoring based on their risk assessment of the client. Additionally, high-risk clients will require enhanced measures. This means that MSBs must,based on the level of risk attached to each high-level client, take extra measures in addition to what is required.

As per FINTRAC, the MSBs must adopt the following methods to conduct enhanced ongoing monitoring of their high-risk clients.

a. Review transactions based on an approved schedule that involves management sign-off;
b. Develop and review reports of high-risk transactions more frequently;
c. Flag certain activities such as those activities that deviate from the expectations of the MSBs and raise concerns;
d. When deemed necessary, set business limits or parameters on accounts or transactions that would trigger early warning signals and require a mandatory review;
e. Review transactions more frequently against suspicious transaction indicators relevant to business relationships.

On 1 June 2021, FINTRAC issued new guidance that introduced additional obligations applicable to the MSBs. These additional obligations include:

a. keeping records of the processes used to record information gathered during ongoing monitoring; and
b. keeping records of processes used to record information gathered during enhanced ongoing monitoring of high-risk clients.

As with other ongoing monitoring records, these additional measures are to be maintained from 1 June 2021 onward and must be kept for at least five years from the date on which the record is created.

ii) Terrorism and Terrorist Financing

In May 2021, FINTRAC released updated guidance on Reporting Entities' obligations to make terrorist property reports, which took effect on 1 June 2021. This updated guidance replaced "Guideline 5: Submitting Terrorist Property Reports to FINTRAC".

Under subsection 83.1 of the Criminal Code or Section 8 of the Regulations Implementing the United Nations Resolutions on the Suppression of Terrorist (RIUNRST), MSBs are required to make a disclosure of terrorist financing and submit a Terrorist Property Report (TRP) to FINTRAC under the PCMLTFA. FINTRAC suggests MSBs familiarize themselves with the Criminal Code and RIUNRST obligations for proper compliance with the lawFurther, MSBs may also be subject to additional obligations regarding terrorist groups, listed persons and other sanctioned individuals and entities (known as 'Designated Persons').

MSBs submit a TPR to FINTRAC **immediately** once they are required to make a disclosure under the Criminal Code or the RIUNRST. Under subsection 83.1(1) of the Criminal Code, **every person in Canada** and **every Canadian outside Canada** must disclose without delay to the Commissioner of the Royal Canadian Mounted Police (RCMP) or to the Director of the Canadian Security Intelligence Service (CSIS) the existence of property in their possession that they know is owned or controlled by or on behalf of a **terrorist group**. According to subsection 83.01(1) of the Criminal Code, a **terrorist group** is defined as: (a) an entity that has as one of its purposes or activities facilitating or carrying out any terrorist activity, (b) a listed entity and (c) an association of such entities. Similarly, under subsection 8(1) of the RIUNRST, every person in Canada, every Canadian outside Canada, and certain prescribed entities including MSBs must disclose without delay to the Commissioner of the RCMP or the Director of CSIS the existence of property in their possession or control that they have reason to believe is owned, held or controlled by or on behalf of a **listed person**. According to sections 1 and 2(1) of the RIUNRST, a **listed person** is an individual or entity that is listed in the Schedule of the RIUNRST because there are reasonable grounds to believe that the individual or entity: (a) has carried out, attempted to carry out, participated in or facilitated the carrying out of terrorist activity, (b) is controlled directly or indirectly by any such individual or entity and (c) is acting on behalf of, or at the direction of, or in association with any such individual or entity.

In addition, MSBs must also disclose, to the RCMP or CSIS, information about a transaction or proposed transaction in respect of such property.

According to FINTRAC, TPRs differ from other reports that are submitted to it because a transaction or attempted transaction does not have to occur for you to submit a TPR. Instead, it is the mere existence of property (such as a bank account) owned or controlled by or on behalf of a terrorist group or listed person that prompts your obligation to submit a TPR.

iii) Suspicious Reporting

According to the notification issued by FINTRAC on 1 June 2021, all reporting entities, including MSBs,must report suspicious transactions under PCMLTFA and associated regulations. Reporting entities must report certain transactions to FINTRAC. Reporting entities include financial institutions, MSBs and security dealers as well as others within its ambit.

FINTRAC defines a suspicious transaction report (STR) as a “type of report that must be submitted to FINTRAC by a reporting entity 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, MSBs will need to ensure that they have completed “the measures that enable them to establish reasonable grounds to suspect the transaction is related to the commission of an ML/TF offence.” These measures include:

- screening for and identifying suspicious transactions;
- assessing the facts and context surrounding the suspicious transaction;
- linking ML/TF indicators to your assessment of the facts and context;

- explaining your grounds for suspicion in an STR, where you articulate how the facts, context and ML/TF indicators allowed you to reach your conclusion.

iv) Threshold Reporting

On 1 June 2021, CSA issued guidance on reporting "Large Virtual Currency Transactions" to FINTRAC. As per the guidance, "large virtual currency transaction reporting requirements under the PCMLTFA and associated regulations are applicable to all reporting entities."

Even though an employee may be the one designated to be the reporting entity, the employer is ultimately the one responsible for meeting FINTRAC's Large Virtual Currency Transaction Reporting (LVCTR) requirements. Similarly, if a reporting entity hires an agent and authorizes him to act on behalf, ultimately, it is still the responsibility of the reporting entity to LVCTR requirements.

FINTRAC has provided reporting entities a transition period between 1 June 2021 and 1 December 2021 to put new LCVTR systems in place.

A reporting entity can also enter into "Service Provider Arrangements" with a service provider to have them submit and correct reports to FINTRAC on their behalf. However, the Reporting entity will be ultimately responsible for meeting the requirements under the PCMLTFA and associated regulations, even if a service provider is reporting on their behalf. This legal responsibility cannot be delegated.

When the MSBs receive any transactions equivalent to $10,000 or more in a single transaction, they must report it and submit an LVCTR to the FINTRAC.

MSBs must also submit an LVCTR to FINTRAC in accordance with the 24-hour rule. This means that when MSBs receive multiple transactions of virtual currency that total $10,000 or more within a consecutive 24-hour window and the transactions meet **one** of the following:

- 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.

To determine if a transaction is reportable, MSBs must first determine when they are in receipt of virtual currency and then determine if the amount received meets the reporting threshold of $10,000.

As the Bank of Canada does not publish exchange rates for virtual currency, MSBs must use the rate they establish in the normal course of business to determine whether they have reached the reporting threshold amount. The process for establishing an exchange rate must be outlined in the policies and procedures within their Compliance Program.

MSBs must submit LVCTRs to FINTRAC electronically if they have the technical capabilities to do so. If they do not have the technical capabilities to report electronically, they can submit paper reports. Furthermore, each LVCTR must include at least one transaction and may include up to 99 transactions. If there are more than 99 transactions, then MSBs will have to use more than one report for LVCTR filing.

MSBs must include the Reporting Entity report reference number to allow FINTRAC to apply any changes to previously submitted reports or link related reports. The Reporting Entity report reference number is the unique number that an MSB assigns to each report.

There are exceptions to the rule: according to the guidance, MSBs are not required to submit an LVCTR if they receive 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 you know the amounts are for a beneficiary that is:

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

Further, MSBs do 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 (a) compensation for the validation of a transaction that is recorded in a distributed ledger; or (b) a nominal amount of virtual currency for the sole purpose of validating another transaction or a transfer of information.

CANADIAN LAWS CHECKLIST

Federal Level

- FINTRAC requires entities dealing in virtual currency such as crypto exchanges to register with it as an MSB. Additionally, even if certain crypto businesses are already registered as an MSB with a province, they will still have to register with FINTRAC.
- Once such entities get registered as MSBs they are subject to the regulatory oversight of FINTRAC and must fulfil all the record-keeping and reporting requirements.
- On 1 June 2021, FINTRAC introduced new regulatory amendments for REs that are subject to the PCLTFA. These amendments are - (a) Regulations Amending Certain Regulations Made Under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, 2019 (SOR/2019-240)
- Regulations Amending the Regulations Amending Certain Regulations Made Under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, 2019 (SOR/2020-112).
- All reporting entities including MSBs have to submit LVCTR when they receive virtual currency amounting to C$10,000 through single or multiple transactions in 24 hour period.
- As of 1 June 2021, REs must (i) keep records of all reportable transactions, (ii) complete the implementation of an LVCTR system as soon as possible prior to 1 December 2021, and (iii) submit all unreported large virtual currency transactions for the period of 1 June 2021, to 30 November 2021 as soon as possible and no later than 31 March 2022, using FINTRAC Upload or the FINTRAC web reporting system (F2R). After 1 December 2021, REs are required to submit LVCTRs within five business days after the date on which the virtual currency amount is received.
- MSBs are also required to submit EFT report to FINTRAC when they receive or initiate an international EFT of C$ 10,000 or more in a single transaction or over a 24-hour period.
- As REs transition their reporting systems to meet this requirement, FINTRAC expects that there may be instances of over or under-reporting for a period of time. In both situations, a voluntary self-declaration of non-compliance (VSDONC) form must be submitted to FINTRAC. Furthermore, transactions that are not required to be reported should be deleted from FINTRAC's database as soon as possible.
- For transactions that cannot be reported, REs must keep a record of reportable transactions until their reporting systems are updated to comply with the requirements. Reporting systems must be updated by 1 December 2021, and REs have until 31 March 2022 to submit all unreported EFT transactions for the period between 1 June 2021 and 30 November 2021.

CANADIAN SECURITIES COMMISSION — PROVINCIAL MEMBERS CONTACT INFORMATION

General Information	CSA Secretariat	Tel: (514) 864-9510	Tour de la Bourse 800, Square Victoria Suite 2510 Montreal Quebec H4Z 1J2	www.securities-administrators.ca	csa-acvm-secretariat@acvm-csa.ca

Province	Regulator	Contact Information	Address	Website	Inquiries
Alberta	Alberta Securities Commission	Tel: (403) 297-6454 Toll-Free: 1-877-355-0585	Ste. 600 - 250, 5th Street SW Calgary, AB T2P OR4	www.albertasecurities.com	Inquiries@asc.ca
British Columbia	British Columbia Securities Commission	Tel: (604) 899-6500 Toll-Free: 1-800-373-6393	P.O. Box 10142, Pacific Centre 701 West Georgia Street Vancouver, BC V7Y 1L2	www.bcsc.bc.ca	inquiries@bcsc.bc.ca
Manitoba	The Manitoba Securities Commission	Tel: (204) 945-2548	500 - 400 St. Mary Avenue Winnipeg, MB R3C 4K5	www.mbsecurities.ca	securities@gov.mb.ca
New Brunswick	Financial and Consumer Services Commission	Toll Free: 1-866-933-2222	85 Charlotte Street, Suite 300 Saint John, NB E2L 2J2	http://www.fcnb.ca	info@fcnb.ca
Newfoundland and Labrador	Office of the Superintendent of Securities Service Newfoundland and Labrador	Tel: (709) 729-4189	2nd Floor, West Block Confederation Building P.O. Box 8700 St. John's, NL A1B 4J6	www.gov.nl.ca/gs	-

Nova Scotia	Nova Scotia Securities Commission	Tel: (902) 424-7768	Ste. 400, Duke Tower 5251 Duke Street PO Box 458 Halifax, NS B3J 2P8	nssc.novascotia.ca	NSSCinquiries@gov.ns.ca
Ontario	Ontario Securities Commission	Tel: (416) 593-8314 Toll-Free: 1-877-785-1555	20 Queen Street West 22nd Floor Toronto, ON M5H 3S8	www.osc.gov.on.ca	Inquiries@osc.gov.on.ca
Prince Edward Island	Office of the Superintendent of Securities	Tel: (902) 368-4569	Consumer, Corporate and Financial Services Division Office of the Attorney General 95 Rochford Street, P.O. Box 2000 Charlottetown, PE C1A 7N8	www.gov.pe.ca/securities	-
Quebec	Autorité des marchés financiers	Tel: Montréal (514) 395-0337 Toll Free: 1-877 525-0337	800, Square Victoria, 22e étage C.P. 246, Tour de la Bourse Montréal, QC H4Z 1G3	www.lautorite.qc.ca	-
Saskatchewan	Financial and Consumer Affairs Authority of Saskatchewan	Tel: (306) 787-5645 (Regina)	6th Floor 1919 Saskatchewan Drive Regina, SK S4P 3V	http://www.fcaa.gov.sk.ca/	-

Territory	Regulator	Contact Details	Address	Website	Inquiries
Northwest Territories	Department of Justice Government of the Northwest Territories 1st Floor Stuart M. Hodgson Building 5009 - 49 th Street P.O. Box 1320 Yellowknife, NT X1A 2L9	Tel: (867) 767-9305	Office of the Superintendent of Securities	https://www.justice.gov.nt.ca/en/divisions/legal-registries-division/securities-office/	-

Yukon	Office of the Yukon Superintendent of Securities	Tel: (867) 667-546	Community Services,Yukon Government 307 Black Street, 1st Floor, Whitehorse, Yukon Y1A 2N1	https://yukon.ca/en/doing-business/securities	-
Nunavut	Nunavut Securities Office	Tel: (867) 975-659	Department of Justice Government of Nunavut 1st Floor, Brown Building P.O. Box 1000 - Station 570 Iqaluit, NU X0A 0H0	http://nunavutlegalregistries.ca/sr_index_en.shtml	securities@gov.nu.ca

WHY MERKLE SCIENCE

Merkle Science provides blockchain transaction monitoring and intelligence solutions for cryptoasset service providers and financial institutions to address their risk exposure to virtual currency-related crime in accordance with FCA AML/CTF compliance requirements.

Our Blockchain Monitor enables compliance teams to go beyond using a database of bad addresses and configure custom risk rules to identify and detect high-risk transactions or addresses. The following are a few ways through which compliance teams can customize risk parameters:

- Detect direct or indirect interactions with high-risk entities (such as coin-mixers, darknet marketplaces), ransomware addresses, scam addresses, theft and hack addresses, the US OFAC list, and other sanctioned or criminal addresses
- Set specific parameters related to frequency, size of transactions, and custom patterns to flag otherwise concealed criminal activity on the blockchain. (See FATF's Virtual Asset Red Flag Indicators of Money Laundering and Terrorist Financing for more information)
- Test and optimize risk rules within a "sandbox" environment before implementation to avoid false positives and too many/few relevant risk alerts.

For more information about how Merkle Science could help your firm comply with FCA virtual currency requirements reach us at contact@merklescience.com.

Contact Us

Contact@merklescience.com

Follow Us merklescience @MerkleScience merklescience Merkle Science

ABOUT THE AUTHORS

Mary Beth Buchanan

President Americas & Global Chief Legal Officer

Merkle Science

Mary Beth Buchanan is the President Americas and Global Chief Legal Officer at Merkle Science, where she leads the company's expansion into the Americas and directs the company's global legal, regulatory and government affairs efforts. Mary Beth is also currently a Member of the Board at the Cardano Foundation. Mary Beth brings over three decades of deep expertise at the intersection of federal law enforcement, global interagency cooperation, corporate compliance, digital assets, and emerging regulatory frameworks. Prior to joining Merkle Science, Mary Beth was the Chief Legal and Compliance Officer at Menai Financial Group, the Global Chief Legal Officer at Bitstamp and the General Counsel at Kraken.

Having been active in the digital currency space since late 2013, Mary Beth is dedicated to education efforts with regulators and policy makers on the potential of blockchain and cryptocurrency technology. Throughout her career, she has seen first-hand both the key role that clear regulations can play in supporting innovation and entrepreneurship, as well as the difficulties faced by digital asset startups in meeting their new compliance mandates.

Mary Beth also served for eight years as the Presidentially appointed United States Attorney for the Western District of Pennsylvania. Early in her career, Mary Beth was an Assistant United States Attorney, with a focus on financial crimes, often working in parallel with the SEC, CFTC, IRS, and state regulators. Mary Beth also served as the United Nations' Ethics and Reputational Risk Officer, leading the United Nations' first ethics and reputational risk assessment for UN Peacekeeping and Special Political Operations.
Mary Beth holds a Juris Doctorate from the University of Pittsburgh School of Law and a Bachelor of Science from the California University of Pennsylvania.

Contact Us

Contact@merklescience.com

Follow Us merklescience @MerkleScience merklescience Merkle Science