Financial Transactions and Reports Analysis Centre of Canada
Centre d'analyse des opérations et déclarations financières du Canada

Sectoral and Geographic Advisory

The role of virtual currency automated teller machines in laundering the proceeds of crime

May 2024
Reference Number: SGA SIRA-2024-005

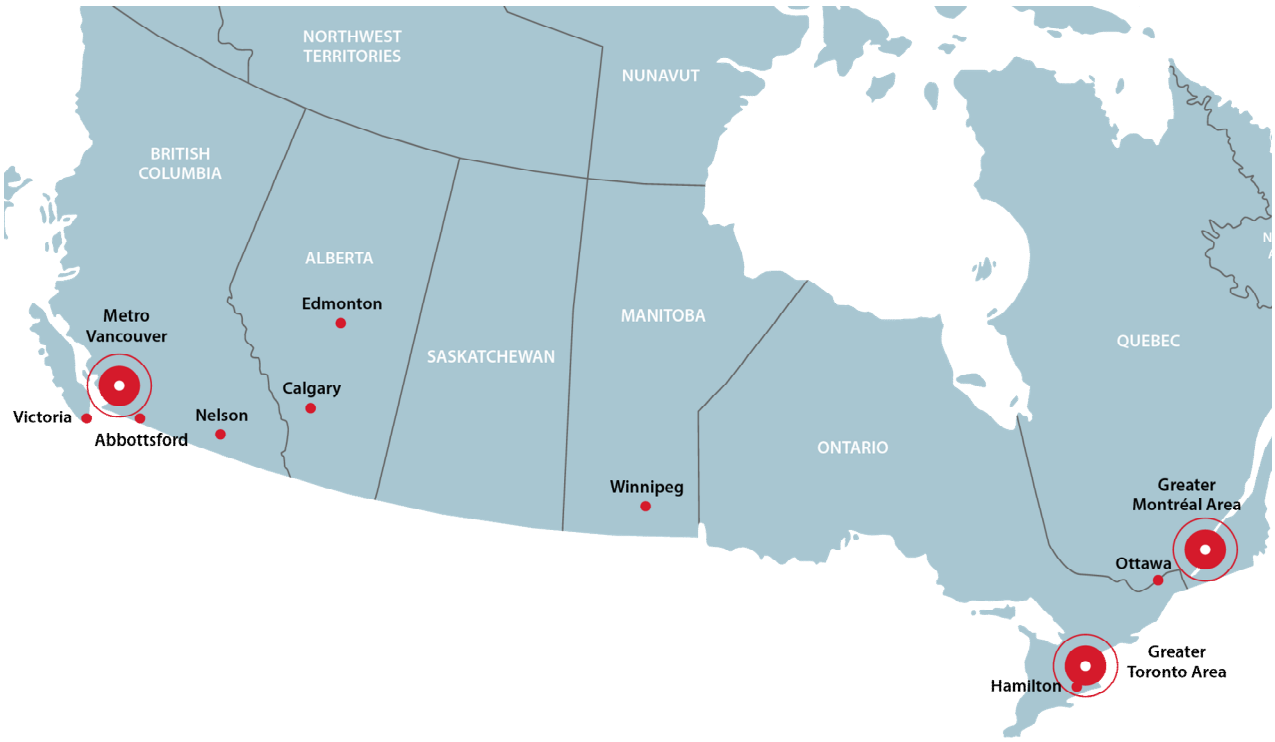
Canada

The role of virtual currency automated teller machines in laundering the proceeds of crime

Area of advisory

This Sectoral and Geographic Advisory describes the key money laundering and terrorist activity financing risks associated with virtual currency automated teller machines. This advisory is designed to help businesses, financial institutions and the public understand and recognize the characteristics of illicit activity involving virtual currency automated teller machines and the types of individuals and entities that may be involved. In particular, this will assist virtual currency money services businesses and virtual currency automated teller machines operators to better identify suspicious transactions to report to FINTRAC in support of law enforcement investigations and FINTRAC compliance activities. Virtual currency automated teller machine operators are to implement compliance policies, procedures and internal controls, including those related to client identification, education, and ongoing monitoring of business relationships for transactions and business relationships identified as high-risk.

Based on the review of suspicious transaction reports received, the advisory describes key attributes of virtual currency automated teller machines activity in Canada suspected of being related to money laundering or terrorist activity financing. In particular, suspicious transactions involving virtual currency automated teller machines are concentrated in the following hotspots, which remained noteworthy even after accounting for population size: the Greater Toronto Area, the Greater Montréal Area, and Metro Vancouver. FINTRAC also identified notable volumes of suspicious transactions at virtual currency automated teller machine terminals in Edmonton, Calgary, Winnipeg, Nelson, Abbotsford, Victoria, Ottawa, and Hamilton.



Overview

VIRTUAL CURRENCIES ARE DIGITAL ASSETS THAT USE DISTRIBUTED BLOCKCHAIN LEDGER TECHNOLOGY

Virtual currencies or "cryptocurrencies" are an encrypted digital medium of exchange in which transactions are verified and records are maintained by a decentralized system using cryptography—rather than by a centralized authority such as a bank—on what is known as a blockchain. Virtual currencies are a global phenomenon not bound by geography and are accessible across the world via a device and internet connection.

VIRTUAL CURRENCY EXCHANGES ARE MONEY SERVICES BUSINESSES

FINTRAC takes various measures to ensure the compliance of businesses subject to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (the Act) and associated Regulations with respect to specific obligations to help combat money laundering and terrorist activity financing in Canada. Persons and entities that deal in virtual currencies (i.e., they provide virtual currency exchange or value transfer services), such as operators of virtual currency automated teller machines, are considered money services businesses under the Act and associated Regulations. Their obligations include registering their business with FINTRAC, reporting certain types of financial transactions to FINTRAC, keeping records, verifying their client's identity, and implementing a compliance program.

Operating an unregistered money services business is a violation and an offence under the Act and associated Regulations.[1] Virtual currency automated teller machine operators that are not registered with FINTRAC—and therefore not fulfilling reporting and other obligations as required by the Act and associated Regulations—may be susceptible to misuse by criminals for money laundering and terrorist activity financing. A money services business that fails to fulfill its obligations under the Act and associated Regulations, including the obligation to register with FINTRAC, may be subject to administrative monetary penalties, or criminal penalties including fines of up to CAN $2,000,000 and/or up to five years imprisonment.

VIRTUAL CURRENCY AUTOMATED TELLER MACHINES ARE A PRIMARY METHOD TO CONVERT FIAT CURRENCY (GOVERNMENT-BACKED LEGAL TENDER) INTO VIRTUAL CURRENCY

Virtual currency automated teller machines (also referred to as Bitcoin automated teller machines, cryptocurrency automated teller machines or virtual currency kiosks) are internet-linked terminals that allow users to exchange fiat currency, such as Canadian dollars, for the purchase or sale of virtual currency. Virtual currency automated teller machines facilitate money transfers between a virtual currency automated teller machine operator and a customer's virtual currency wallet. Unlike traditional automated teller machines, which require a bank account to deposit or withdraw funds, virtual currency automated teller machines directly connect the user to the virtual currency exchange to purchase or sell virtual currency. The exchange rate of virtual currency can vary depending on the current market rate at the time of the transaction. While the majority of transactions involving virtual currency automated teller machines are likely legitimate, criminals may turn to virtual currency automated teller

[1] A registration with FINTRAC does not indicate an endorsement or licensing of the business. It indicates only that the business has fulfilled its legal requirement under the Act and associated Regulations to register with the federal government. FINTRAC does not regulate money services businesses beyond the framework of this specific legislation and therefore cannot offer any assessment of their overall business practices. Consumers are encouraged to do their own due diligence when considering using the services of a money services business and should ensure they fully understand the terms and conditions that are associated with it.

machines to convert their illicit proceeds into virtual currency, initiating the first step in what is known as the "placement stage" of the money laundering cycle.

Trends and patterns of virtual currency automated teller machine use in Canada

EMERGING ROLE IN LAUNDERING THE PROCEEDS OF CRIME

With the rise in the number of suspicious transaction reports concerning the use of virtual currency automated teller machines by criminals, FINTRAC assesses that virtual currency automated teller machines are becoming a key tool in the placement stage of money laundering, since the source of cash deposited is essentially untraceable. Virtual currency automated teller machines play an increasingly important role in the virtual-asset ecosystem as a fast and reliable method for transferring fiat to virtual currency and vice versa. However, the ease, accessibility and pseudo-anonymity of virtual currency automated teller machines can also make them susceptible to misuse by criminals seeking to launder their illicit funds outside the traditional financial system, allowing them to send or receive funds anywhere in the world.

USE OF VIRTUAL CURRENCY TO TRANSFER ILLICIT FUNDS, HIDE CRIMINAL ORIGINS, AND CONVERT INTO FIAT CURRENCY

FINTRAC's analysis of suspicious transaction reports indicate that fraud is the predominant suspected predicate offence associated with virtual currency automated teller machines, followed by human trafficking for sexual exploitation and cybercrimes. FINTRAC also identified instances where falsified identities and money mules—a third party who wittingly or unwittingly moves the proceeds of crime on behalf of a bad actor—were used when depositing or withdrawing funds at virtual currency automated teller machines with suspected links to criminal activities.

In a typical fraud scheme, criminals will direct victims to place fiat currency at a virtual currency automated teller machine or provide a QR code associated with the fraudster's virtual currency wallet for the victim to use during the transaction.

Once placed into the virtual currency ecosystem, funds are moved through a series of private wallet addresses and can be co-mingled with other wallets containing fraud proceeds. Fraudsters may then choose from a variety of obfuscation methods to launder the fraud proceeds and conceal the source of the funds.

The majority of virtual currency automated teller machine-related suspicious transaction reports analyzed by FINTRAC referenced transactional exposure to illicit or high-risk services such as **darknet markets**, **online gambling platforms**, **high-risk** and **Peer-to-Peer exchanges** and **mixing services**. Virtual currency automated teller machines can also be used to "off-ramp" virtual currency into fiat, once the proceeds of crime have been laundered through a variety of services that can disguise their origins and distance them from the initial criminal activity. FINTRAC analysis identified high volumes of suspicious transactions involving virtual currency automated teller machines located in the following major metropolitan hotspot areas, which remained significant even after adjusting for population density: the Greater Toronto Area, the Greater Montréal Area, and Metro Vancouver. FINTRAC also identified notable volumes of suspicious transactions at virtual currency automated teller machine terminals in Edmonton, Calgary, Winnipeg, Nelson, Abbotsford, Victoria, Ottawa, and Hamilton.

FRAUDSTERS ARE COACHING VICTIMS IN VIRTUAL CURRENCY AUTOMATED TELLER MACHINE USE

FINTRAC has identified a typology involving fraudsters coaching victims to limit direct interactions with the virtual currency automated teller machine operator. Suspicious transaction reports from virtual currency automated teller machine operators indicate that video monitoring footage in virtual currency automated teller machines increasingly shows victims on the phone during the transaction, likely receiving instructions on how to complete the virtual currency transfer. New investors, elderly persons and new immigrants may be particularly vulnerable to virtual currency-related fraud schemes. Criminals may use a variety of techniques at virtual currency automated teller machines to transfer value and obscure the identity of those controlling the funds.

VIRTUAL CURRENCY AUTOMATED TELLER MACHINES TECHNIQUES TO TRANSFER VALUE AND OBSCURE IDENTITY OF THOSE CONTROLLING FUNDS

These techniques include using money mules to conduct the transactions, avoiding contact with virtual currency automated teller machine operators, and providing falsified or altered identifiers such as phone numbers or dates of birth. The same individual can create multiple virtual currency automated teller machine account profiles under different phone numbers and personal identifiers. Suspicious transaction reports also identified excessive deposit or withdrawal amounts over a period of time (daily, weekly and monthly) under CAN $999 at multiple virtual currency automated teller machine terminals, using shared prepaid or Voice Over Internet Protocol phone numbers to avoid identification.

Verifying client identity is a foundational element of Canada's anti-money laundering and anti-terrorist financing regime. Money services businesses, such as virtual currency automated teller machine operators, must ensure that the identifiers in an identification document or information from another source matches the information that the person or entity provided.

Darknet markets are commercial websites that bring buyers and sellers together to exchange virtual currency for illicit goods and services.

Online gambling platforms increase the risk for money laundering, as criminals may use these websites to layer the proceeds of crime.

High-risk exchanges feature little to no anti-money laundering compliance procedures including Know Your Client onboarding when opening accounts, may have publicly documented ties to criminal activity, and/or high amounts of exposure to risky services. These exchanges are located in offshore jurisdictions known for public corruption, weak judiciaries or weak anti-money laundering and anti-terrorist financing regulations.

Peer-to-Peer exchanges allow users to transact directly with one another. Unlike centralized exchanges, which require users to provide Know Your Client information in order to process a transaction, some peer-to-peer services allow users to send or receive virtual currency without verifying their identity.

Mixers are websites or software used to pool incoming funds from addresses on the blockchain and redistribute those funds such that there is no direct connection to the original source. They serve as an off-ramp for selling the “cleaned” virtual currency.

CONCEALING CLIENT IDENTIFICATION AND CIRCUMVENTING RECORD-KEEPING AND REPORTING THRESHOLDS

Suspicious transaction reporting identified individuals using shared or altered identification documents or identifiers such as name, address, date of birth or phone numbers, in an attempt to circumvent client identification requirements. Often, the observed level and volume of transactional activity did not correspond with the client information, such as occupational profile or financial standing of the individual conducting the transaction. Users who falsified their identity were also suspected of facilitating deposits or withdrawals associated with darknet markets, human trafficking for sexual exploitation and investment or authorities fraud. FINTRAC observed that once the funds were placed into virtual currency automated teller machine terminals, they were sent to multiple intermediary addresses that had exposure to high-risk exchanges, including peer-to-peer exchanges that do not require Know Your Client information when opening accounts, making them attractive for money laundering activities.

Reporting entities 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.

LAYERING AND INTEGRATION TECHNIQUES INVOLVING HIGH-RISK SERVICES

Criminal actors may seek to avoid standard Know Your Client information collection thresholds and usual business hours

FINTRAC analysis of suspicious transactions at virtual currency automated teller machine terminals identified users across Canada depositing high volumes of low-dollar transactions between CAN $100-$999, and sending funds to darknet marketplaces for the purchase of drugs, child sexual abuse material, cyber exploit marketplaces for malicious cyber-tools or services and fraud shops for compromised payment information or identity documents.

Suspicious transaction reporting has identified layering techniques involving the use of high-risk services such as darknet markets, online gambling platforms, high-risk exchanges, peer-to-peer exchanges, and mixers. These services can help conceal the criminal origins of funds and obfuscate the money trail to create a perception of legitimacy. Additionally, users conducting suspicious transactions at virtual currency automated teller machines are often doing so outside usual business hours between late night and early morning (9 p.m. – 3 a.m.).

Suspected criminal proceeds deposited at virtual currency automated teller machines off-ramped at high-risk exchanges

Suspicious transactions reported to FINTRAC referenced virtual currency automated teller machine deposits destined to high-risk exchanges ranging from CAN $999 to CAN $10,000 that were associated with the proceeds of fraud, cybercrimes and human trafficking for sexual exploitation. Blockchain activity indicated that the funds were off-ramped at exchanges located in Iran, Russia, Belarus and neighbouring jurisdictions with weak anti-money laundering and anti-terrorist financing regulations, and/or other comprehensively sanctioned jurisdictions.

Suspicious transaction reports identified a large proportion of funds sent to mixers and off-ramped at multiple virtual currency automated teller machines throughout Canada associated with fraud, ransomware, and fraud shop material or narcotics on darknet market places. FINTRAC identified that the withdrawals at virtual currency automated teller machines appear to be conducted at various times between late night and early morning and consist of high volumes of low dollar transactions.

Detecting and deterring illicit virtual currency automated teller machine activities

REPORTING ENTITIES SHOULD BE WARY OF INDIVIDUALS THAT APPEAR TO BE STRUCTURING DEPOSITS IN AMOUNTS JUST BELOW REPORTING REQUIREMENTS

Structured deposits at virtual currency automated teller machine terminals may involve individuals using shared or altered identification documents or identifiers such as name, address, date of birth or phone numbers to circumvent reporting obligations. Structuring may also involve depositing funds at multiple virtual currency automated teller machine terminals that are just below the reporting threshold, several times a day, and using a different phone number for each transaction. Reporting entities should consider implementing controls and mitigation measures tailored to these risks within their risked-based approach for ongoing business activities and clients.

VIRTUAL CURRENCY AUTOMATED TELLER MACHINES RISKS WARRANT ENHANCED DUE DILIGENCE

The high concentration of virtual currency automated teller machines in Canada and ease of accessibility make virtual currency automated teller machines susceptible to illicit transactions that pose inherent money laundering or terrorist activity financing risks. Virtual currency automated teller machine providers are required to implement compliance policies, procedures and internal controls, including those related to client identification, education, and ongoing monitoring of business relationships for transactions and business relationships identified as high-risk. Virtual currency automated teller machine providers are encouraged to identify and assess potential gaps or weaknesses within their compliance program. For example, using a Risk-Based Approach, virtual currency automated teller machine providers can identify and assess risks that could affect other parts of their compliance program, such as gaps in written policies, procedures or training programs. Reporting entities are also encouraged to exercise caution for clients with direct[2] or indirect[3] sending exposure to darknet markets (child sexual abuse material, cyber exploit marketplaces, fraud shops, and ransomware), online gambling platforms, high-risk or peer-to-peer exchanges, and mixing services or any other associated illicit activity. Blockchain analysis tools can identify virtual currency addresses connected to illicit or high-risk services allowing virtual currency automated teller machine operators to identify risky sending or receiving exposure.

[2] Direct exposure: refers to funds sent from one party to another without intermediaries in between. There is a direct connection between the source and the destination of funds.

[3] Indirect exposure: refers to an indirect connection between an intermediary, wallet or service between the source and destination of funds.

VIRTUAL CURRENCY AUTOMATED TELLER MACHINE RED FLAGS

- The user is sending or receiving large volumes of high frequency low dollar amounts to private wallet addresses, peer-to-peer platforms, mixers, gambling platforms, scams, darknet marketplaces (child sexual abuse material, cyber exploit marketplaces, fraud shops and ransomware) or high-risk exchanges.
- The user is maxing out daily funding limits at virtual currency automated teller machines.
- Video monitoring footage shows the user on the phone or accompanied by an individual and instructed or coached during the transaction.
- The user is attempting to conceal their identity by using shared, falsified, stolen or altered identification (address, telephone number, email).
- The level or volume of transactional activity involving a virtual currency automated teller machine is inconsistent with the client's apparent financial profile, their usual pattern of activities, occupational information, or declared business information.
- The use of Voice Over Internet Protocol phone numbers or prepaid phone numbers when depositing or withdrawing funds at virtual currency automated teller machine terminals.
- Sending exposure to high-risk exchanges that lack in customer identity verification measures, transactional due diligence, and legal/regulatory compliance measures or may be located in offshore jurisdictions with a history of tax havens and banking secrecy, or in foreign countries known for public corruption.
- Excessive under threshold deposits under CAN $999 to a single address over a short period of time multiple times a day or week and/or at several different virtual currency automated teller machines terminals.
- Transactions conducted by a single individual or accompanied by multiple individuals that occur in the later hours of the night or early morning (9 p.m. – 3 a.m.).

Consumers should protect themselves

Individuals should be wary of persons on social media or dating websites attempting to solicit investments in virtual currencies, as well as criminal actors impersonating government, law enforcement or private sector companies in order to extort payment for alleged criminal action or billing and or to obtain access to personal or financial information. These are clear flags that the offer is likely fraudulent. No government agency will request payment in virtual currencies.

Individuals should also avoid becoming unwitting participants in money laundering activities associated with virtual currency automated teller machines. Treat with suspicion any employment opportunities or financial offers based on the physical transfer of funds to and from virtual currency automated teller machines.

Consumers transferring funds to and from virtual currency automated teller machines can protect themselves by exercising due diligence, carefully researching a virtual currency investment, and exercising caution for offers that sound too good to be true. Always verify the legitimacy of an exchange, wallet provider, or investment opportunity

before sending any funds. Once a virtual currency transaction is completed, there is no way to cancel or reverse the transaction.

In general, users should be vigilant and take appropriate precautions to protect their personal and financial information when using virtual currency automated teller machines.

Report suspicions of money laundering or the financing of terrorist activities

Consumers should immediately report any unusual or irregular transactions to their financial institution. Anyone can voluntarily submit information[4] to FINTRAC about suspicions of money laundering or the financing of terrorist activities or the operation of unregistered virtual currency automated teller machines in contravention of the Act. Individuals believing that the situation requires an immediate law enforcement response should also report it directly to the local law enforcement agency. Those who believe they are victims of fraud are encouraged to report to the Canadian Anti Fraud Centre.

Reporting to FINTRAC

To facilitate FINTRAC's disclosure process, reporting entities should include the term **#SGA2024** in Part G—Description of suspicious activity on Suspicious Transaction Reports relevant to this advisory. For guidance on submitting suspicious transaction reports to FINTRAC, see Reporting suspicious transactions to FINTRAC[5] at our website.

CONTACT FINTRAC

- **Email:** guidelines-lignesdirectrices@fintrac-canafe.gc.ca (include SIRA-2024-005 in the subject line)
- **Telephone:** 1-866-346-8722 (toll free)
- **Facsimile:** 613-943-7931
- **Mail:** FINTRAC, 24th Floor, 234 Laurier Avenue West, Ottawa ON, K1P 1H7, Canada

Cat. No. FD4-33/2024E-PDF
ISBN 978-0-660-68213-6

Sectoral and Geographic Advisories (SGAs) identify sectors or geographic areas more at risk from specific money laundering or financing of terrorist activities typologies. However, these Advisories are not legal advice. Reporting entities should refer to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and its associated Regulations for the full description of reporting obligations.

[4] Providing voluntary information about suspicions of money laundering or the financing of terrorist activities https://fintrac-canafe.canada.ca/individuals-individus/vol/1-eng

[5] Reporting suspicious transactions to FINTRAC: https://fintrac-canafe.canada.ca/guidance-directives/transaction-operation/str-dod/str-dod-eng