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

Unclassified

Sectoral and Geographic Advisory

Underground Banking through Unregistered Money Services Businesses

May 2022
Reference Number: SGA 20/22-SIRA-001

Canada

Underground Banking through Unregistered Money Services Businesses

Area of Advisory

This Sectoral and Geographic Advisory focuses on money laundering and terrorist activity financing risks associated with underground banking through unregistered money services businesses (MSBs). Money services businesses that are not registered with FINTRAC—and therefore not fulfilling reporting and other obligations as required by the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA) and associated Regulations—are susceptible to misuse by criminals for money laundering and financing of terrorist activities. As such, this advisory is designed to help businesses, financial institutions and the public understand and identify the characteristics of this activity and the types of individuals and entities that may be involved to better identify suspicious financial transactions, which could be reported to FINTRAC in support of law enforcement investigations and FINTRAC compliance activities.

The advisory describes key attributes of underground banking in Canada, particularly as carried out by unregistered money services businesses in Metro Vancouver, the Greater Toronto Area, and, to a lesser extent, in the Calgary-Edmonton Corridor. The advisory reviews trends and patterns identified through FINTRAC's analysis of suspicious transaction reports and disclosures to law enforcement related to underground banking.

Overview

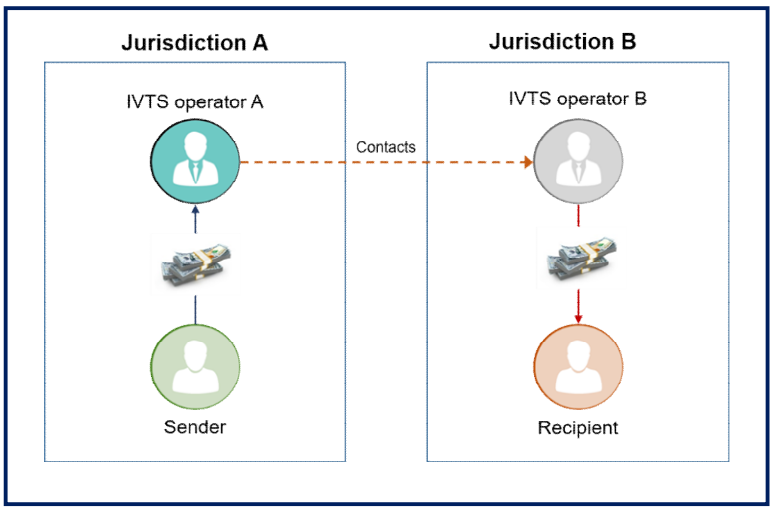
"Underground banking" is a generic term, commonly used to describe a form of informal value transfer.

Using informal value transfer systems (IVTS), parties in different jurisdictions remit or transmit money or value without necessarily moving the funds (see *Figure 1*).

IVTS service providers often have geographic, cultural or ethnic ties to the communities they serve.

Many operate within overseas diaspora populations, providing informal value transfer services to community members and expatriate workers.

Figure 1: Informal Value Transfer System



Canada regulates the informal funds transfer sector.

The PCMLTFA and associated Regulations set out registration and other obligations for individuals and entities, both foreign and domestic, that are engaged in the business of foreign exchange dealing, remitting or transmitting funds by any means or through any person, entity or electronic funds transfer network, issuing or redeeming money orders, traveller's cheques or other similar negotiable instruments except for cheques payable to a named person or entity, or dealing in virtual currencies.

Operating an unregistered money services business is a violation and an offence under the PCMLTFA.

Individuals and entities carrying out the above-noted activities are required to register with FINTRAC. Money services businesses must fulfill specific obligations as required by the PCMLTFA and associated Regulations, to help combat money laundering and terrorist activity financing in Canada. Not doing so could result in criminal or administrative penalties.

IVTS are global in reach and vulnerable to abuse.

While IVTS are often important to diaspora communities to enable the sending and receiving of legitimate funds overseas, the versatility and global reach of underground banking makes it equally susceptible to misuse, specifically by criminal groups for money laundering and financing of terrorist activities. For the purposes of this advisory, underground banking will refer to alternative mechanisms that facilitate the ***unlawful*** remittance of funds or value between jurisdictions.

Key Components of Underground Banking

Underground banking arrangements are often multi-layered and sophisticated.

They can manifest themselves in various ways and often involve formal financial services, international trade and multiple sectors. In light of these characteristics, it can be difficult to recognize underground banking activity and discern legitimate value transfers from criminal-based underground banking activities.

SUPPLY AND DEMAND

Restricted financial markets create black market opportunities.

The need for organized crime groups to launder the proceeds of crime—generally cash, but also electronic funds and virtual currencies—accounts for the supply of large amounts of illicit funds that can feed into underground banking systems.

The need to move funds between restricted and unrestricted jurisdictions drives demand for underground banking.

Foreign currency controls that limit capital flight[1] or the imposition of economic sanctions on foreign jurisdictions[2] represent two major drivers of underground banking. China and Iran, for example, are subject to these restrictions and have long established diaspora communities in Canada, particularly in Metro Vancouver and the Greater Toronto Area, that have traditionally made use of IVTS. The need for diaspora communities to access funds due to currency controls or sanctions accounts for the demand.

Cuckoo smurfing is a technique professional money launderers use to make criminal proceeds appear to have come from legitimate sources and to transfer funds across jurisdictions.

This technique leverages the bank accounts of multiple unwitting third parties to facilitate deposits of cash derived from criminal activity. The bank accounts usually belong to individuals and businesses in diaspora communities who are expecting remittances.

This technique derives its name from the cuckoo bird, which lays its eggs in the nests of other birds, tricking the host into raising its young.

FACILITATORS

The role of professional money launderers in facilitating underground banking is significant.

Professional money launderers specialize in providing services or advice on how to launder the proceeds of crime for others in exchange for a commission, fee or other type of payment. Professional money launderers may be business owners, lawyers, accountants or real estate agents. Regardless of their profession, they possess specialized skills, knowledge, contacts and networks to transfer or convert criminal proceeds via underground banking and other illicit methods.

Professional money launderers use a variety of techniques to transfer value and obscure the identity of those controlling the funds.

These techniques—which include using money mules, cuckoo smurfing and co-mingling remittances with trade payments—are often connected to a larger money laundering scheme. Identifying the use of these techniques presents opportunities to identify the illicit networks behind them and support disruption by law enforcement.

- **Money mules**—individuals who transfer funds or transport proceeds of crime on behalf of a criminal organization or money launderer—may be knowingly complicit or may work unwittingly or recklessly on behalf

of the money laundering network. Students, homemakers, unemployed persons, seniors and migrant labourers are frequent targets for money mule recruitment. Victims of fraud can be exploited or coerced into being money mules. Criminals can use the victim's bank account for the placement and transfer of illicit funds.

- IVTS customers can become victims of **cuckoo smurfing**. Account holders are often unaware of the illicit source of funds and are simply expecting the transfer of funds into their account in one jurisdiction following the transfer of funds in another.
- Professional money launderers may **co-mingle criminal proceeds with trade payments and remittances** via IVTS operators. Account settlement in underground banking is typically through trade in goods, with criminals using trade-based money laundering techniques to transfer value between jurisdictions. For example, companies owned or controlled by professional money launderers can issue invoices for real or fictitious trade, misrepresenting the true value of goods crossing borders.

Trade-based money laundering (TBML) is the process of disguising the proceeds of crime and moving value between jurisdictions through the use of real or fictitious trade transactions.

TBML schemes typically involve trade fraud and the deliberate falsification of declared prices, quantity or quality of goods being imported or exported as a way to transfer value across international borders.

Trends and Patterns in Money Laundering Linked to Underground Banking

FINTRAC's analysis of suspicious transaction reports linked to underground banking and suspected unregistered money services businesses identified several key characteristics of this activity in Canada: the use of suspected money mules; frequent use of email money transfers and international wire transfers; and the co-mingling of funds between various personal and business accounts, involving both registered and unregistered money services businesses.

USE OF MONEY MULES

Individuals identified as operating or facilitating unregistered money services businesses may be money mules.

FINTRAC's analysis reveals links to common entities that are connected to other suspected money mules and to businesses suspected to be operating as unregistered money services businesses. Suspected money mule accounts received a high volume of third-party cash deposits and email money transfers that do not align with the client's profile. These funds were rapidly depleted, primarily via outgoing email money transfers and bank drafts to unrelated third parties. These funds were also used to purchase investments, real estate, and vehicles being shipped to West Africa and Asia.

A number of suspected money mules are international students receiving wire transfers from individuals and entities in China and Hong Kong, as well as email money transfers and bank drafts from third parties in Canada. These funds appeared to flow through personal and business accounts, with little information on the source of the

funds or the ultimate beneficiary. While these transactions do not necessarily demonstrate a direct link to money laundering, the lack of details that would set the transactions out as legitimate is a concern.

Email money transfers and international wire transfers are the most commonly observed methods for moving funds through money mule accounts.

Professional money launderers often use the bank accounts of individuals and businesses as mule accounts for the placement and transfer of illicit funds. These individuals may also be straw buyers (a person who makes a purchase on behalf of another person) for vehicles, electronics and other goods used in trade-based money laundering, and nominees used to purchase real estate and pay mortgages.

Indicators of suspected money mules in underground banking

- Accounts receive a high volume of deposits (email money transfers and cash) from multiple third parties, along with international wire transfers that do not appear to be consistent with the client's personal use or profile.
- Cash (usually in amounts less than $10,000) is deposited across multiple branches and/or in different provinces from where the account is held.
- Funds are rapidly depleted through email money transfers, cash withdrawals, and/or bank drafts to unrelated third parties, including money services businesses and entities suspected to be operating unregistered money services businesses, real estate or brokerage firms, law firms, legal trust funds or investment firms. Funds may also be used to buy or make payments on investments (which are almost always redeemed early), real estate or vehicles.
- Accounts are used for pass-through activity—that is, to receive and subsequently send funds to beneficiaries.

CRIMINAL ABUSE OF IVTS

Individuals moving their wealth to Canada through underground banking channels run the risk of unknowingly accepting proceeds of crime and facilitating money laundering.

FINTRAC found that individuals and entities—including those reported to be operating unregistered money services businesses—appeared to be operating IVTS networks that facilitate the transfer of funds on behalf of individuals and entities located in Asia, Africa and the Middle East. Many of these individuals and entities received funds derived from fraud, including romance, business email compromise and investment fraud.

In many cases, these individuals and entities were also associated with buying and shipping used and auctioned vehicles to West Africa—an identified trade-based money laundering method. Professional money launderers can manipulate the value of vehicles being exported or imported to launder proceeds of crime on behalf of criminal clients and to transfer value across jurisdictions.

Suspected unregistered money services businesses transferring funds to and from West Africa were concentrated in the Greater Toronto Area and Calgary-Edmonton Corridor.

FINTRAC suspects that criminals likely recruit money mules and offer funds transfer services via word-of-mouth and other forms of advertising within these diaspora communities. Individuals identified in the reporting shared common ethnic backgrounds, occupations and sometimes employers.

CO-MINGLING OF FUNDS

Individuals conducted money services business activity out of personal bank accounts, from residential addresses and through other businesses.

Many of the individuals owned convenience stores, holding companies, construction and general contracting companies and import-export businesses, which shared addresses or telephone numbers with money services businesses, and appeared to be co-mingling in their personal and business accounts funds related to money services business activity. Reporting entities identified transactions that do not align with the stated nature of the business. These businesses were concentrated in Metro Vancouver and the Greater Toronto Area.

Some money services business operators may be misrepresenting the nature of their business to financial institutions in order to access financial services.

While conducting MSB services through personal or other business accounts is not contrary to the PCMLTFA, money services businesses must provide to FINTRAC information on all the bank accounts they use to carry out their MSB services.

These businesses may be front or shell companies.

FINTRAC suspects that these businesses may be front companies or shell companies used to receive cash proceeds of crime and illicit funds from jurisdictions identified as high-risk for money laundering and financing of terrorist activities. A number of these businesses received funds from entities connected to organized crime, drug trafficking or law enforcement investigations into money laundering and sanctions evasion. Professional money launderers may spread their criminal IVTS activity across multiple business accounts and financial institutions in an effort to avoid triggering the suspicions of financial institutions.

Suspicious transactions highlighted a general flow of funds from Iran and China, primarily through the United Arab Emirates, Hong Kong and Qatar, to these Canadian entities. In turn, these entities transferred the funds to multiple individuals and entities in Canada through bank drafts, cheques and account transfers.

Indicators of underground banking through unregistered money services businesses

- Accounts are funded by a high volume of large international wire transfers from general trading companies and/or foreign currency exchanges located in the United Arab Emirates, Hong Kong or Qatar.
- Remitting companies have addresses that correspond to a P.O. Box in major financial centres, such as Dubai or Hong Kong.
- Transactions involve individuals or entities linked by media, law enforcement and/or intelligence agencies to criminal activities.
- Accounts receive a high volume of incoming email money transfers, over-the-counter third-party cash deposits (usually structured in amounts less then $10,000), cheques and/or bank drafts, with little to no business activity that aligns with the stated business type.
- Accounts receive a high volume of cheques from money services businesses, along with cash deposits from different provinces, bank drafts and/or cheques from multiple financial institutions where the issuer/purchaser cannot be established.
- Funds are depleted through outgoing wire transfers, email money transfers, cheques and/or bank drafts to self and/or related businesses at different financial institutions, and/or to third parties, including law firms, trusts and real estate companies.

Detecting and Deterring Underground Banking

Underground banking risks may warrant enhanced due diligence.

The limited visibility and lack of transparency associated with underground banking transactions pose inherent money laundering and financing of terrorist activities risks. While not every individual and entity identified in suspicious transaction reporting was associated with organized crime, FINTRAC suspects that a portion of the funds moved via underground banking and unregistered money services businesses were proceeds of crime generated by organized criminal groups or funds that were illegally transferred (e.g., sanctions evasion). Strong compliance policies and procedures must describe the special measures that are required to be taken, including those related to client identification and beneficial ownership information, the frequency of updating that information, and ongoing monitoring of business relationships for transactions and business relationships identified as high-risk.

Consumers should protect themselves.

Consumers transferring funds to and from overseas can protect themselves by exercising due diligence and dealing only with financial institutions, and reputable money services businesses registered with FINTRAC.

To avoid becoming a money mule, beware of unsolicited phone calls, texts, emails or social media messages requesting personal information, and offers that sound too good to be true. Do not share bank account details or other personal information with third parties. Professional money launderers frequently target online and social media sites catering to the ethnic or demographic profiles of their targets. In addition to direct overtures, fake business advertisements can draw potential money mules into unwitting participation in money laundering schemes. Recruitment via social media tends to place heavy emphasis on the lure of quick and easy money and attractive lifestyles.

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[3] to FINTRAC about suspicions of money laundering or the financing of terrorist activities. Individuals believing that the situation requires an immediate law enforcement response should also report it directly to the local law enforcement agency.

REPORTING TO FINTRAC

To facilitate FINTRAC's disclosure process, reporting entities should include the term **#SGA2022** in Part G—Description of suspicious activity on the Suspicious Transaction Report. For guidance on submitting suspicious transaction reports to FINTRAC, see Reporting suspicious transactions to FINTRAC[4] at our website.

CONTACT FINTRAC

- **Email:** guidelines-lignesdirectrices@fintrac-canafe.gc.ca (include SGA 20/22-SIRA-001 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

RELATED CONTENT

Video – Sectoral and Geographic Advisory: Underground Banking through Unregistered Money Services Businesses[5]

Cat. No. FD4-26/2022E-PDF
ISBN 978-0-660-41323-5

[1] Report on exchange arrangements and exchange restrictions: https://www.imf.org/en/Publications/Annual-Report-on-Exchange-Arrangements-and-Exchange-Restrictions/Issues/2020/08/10/Annual-Report-on-Exchange-Arrangements-and-Exchange-Restrictions-2019-47102

[2] List of countries subject to Canadian economic sanctions: https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/current-actuelles.aspx?lang=eng

[3] Providing voluntary information about suspicions of money laundering or of the financing of terrorist activities: https://www15.fintrac-canafe.gc.ca/vir-drtv/public/

[4] Reporting suspicious transactions to FINTRAC: https://fintrac-canafe.canada.ca/guidance-directives/transaction-operation/Guide3/str-eng

[5] Video – Sectoral and Geographic Advisory: Underground Banking through Unregistered Money Services Businesses: https://youtu.be/9a3hU8iBGUU

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.