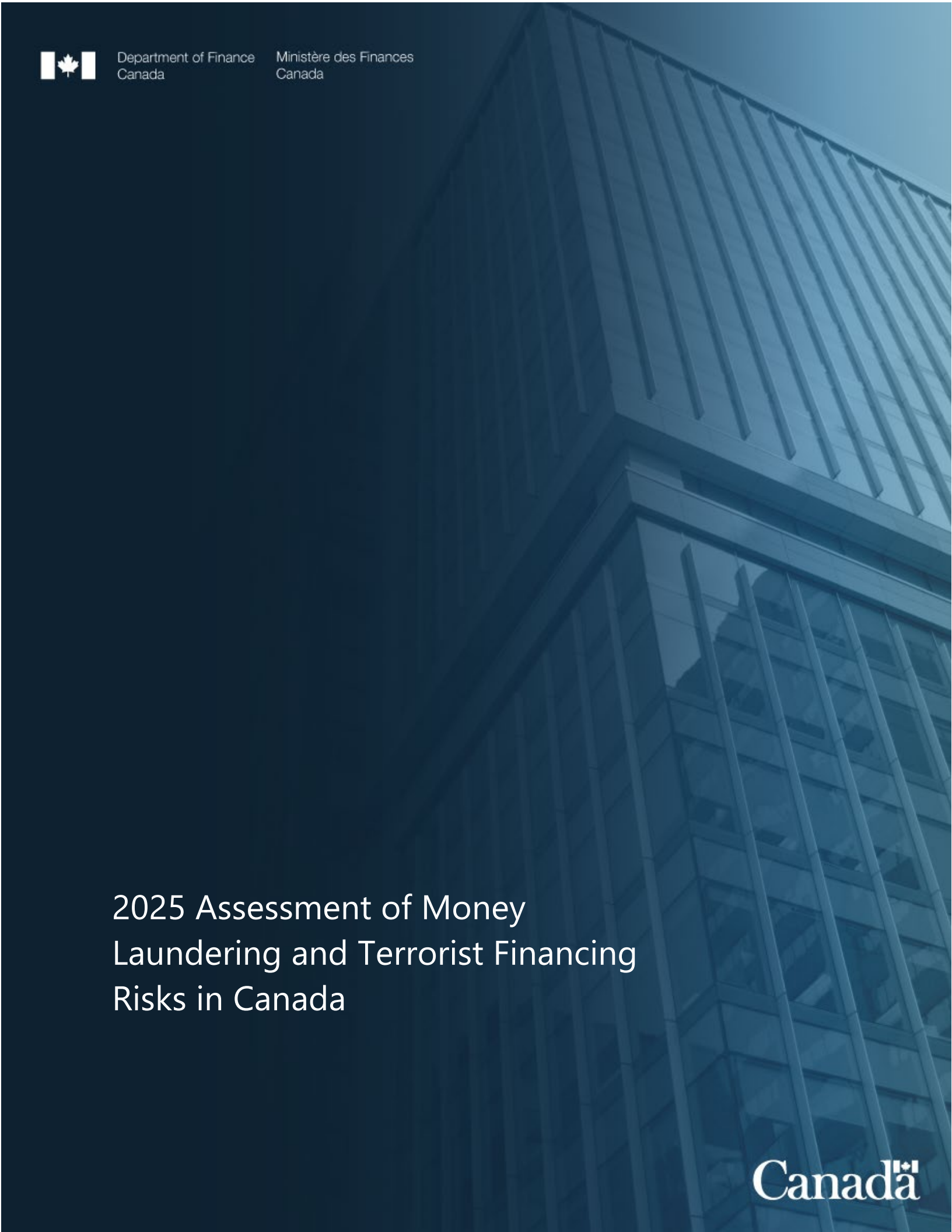
Department of Finance Canada | Ministère des Finances Canada

2025 Assessment of Money Laundering and Terrorist Financing Risks in Canada



Canada

Cette publication est également disponible en français.

Cat. No.: F2-218/2023E-PDF
ISBN: 978-0-660-37662-2

Table of Contents

Executive Summary

Canada has a robust Anti-Money Laundering and Anti-Terrorist Financing (AML/ATF) Regime that contributes to its efforts to combat transnational organized crime and is a key element of its counter-terrorism strategy. It comprises 13 federal departments and agencies with policy, regulatory, intelligence, and enforcement mandates. The federal Regime works with provincial and municipal counterparts and over 38,000 Canadian businesses with reporting obligations under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA), known as reporting entities, to prevent, detect, and disrupt financial crime.

An accurate, nuanced, and up-to-date understanding of risks, informed by an assessment of money laundering and terrorist financing threats, vulnerabilities, and consequences, is the foundation for applying a risk-based approach to combatting these financial crimes in Canada. This includes balancing priorities of protecting the integrity of Canada's financial system and the safety and security of Canadians, respecting privacy and other rights of people in Canada, and mitigating regulatory burden and unintended consequences that may be faced by industry and the clients to whom they provide services.

The *2025 Assessment of Money Laundering and Terrorist Financing Risks in Canada* is a comprehensive assessment of the most pressing money laundering and terrorist financing threats and vulnerabilities in Canada. It assesses inherent risks and discusses the mitigation measures put in place to respond to them. Findings are informed through consultations with federal government authorities and external stakeholders, including provincial and territorial governments, the private sector, non-profit organizations, and international partners.

The purpose of this report is to support evidence-based policymaking, resource allocation, and priority setting for public authorities, and to support private sector businesses and non-government organizations to apply focused and proportionate measures to mitigate risks.

Key Findings

- A strong, open and stable economy and financial sector make Canada an attractive source, destination, and transit point for proceeds of crime. Organized crime groups (OCGs) and third-party enablers are the main money laundering threat actors in Canada. Most large-scale and sophisticated money laundering operations in Canada involve specialized third parties who provide money laundering services in exchange for commissions, fees, or other benefits.
- Illegal drug trafficking remains the highest money laundering threat in Canada, followed by fraud, commercial trade fraud and trade-based money laundering, and tax crimes. These threats are each estimated to involve billions of dollars in illicit proceeds annually in Canada. These proceeds are often laundered using complex methods and sophisticated enablers. Further, these crimes can have devastating impacts on Canadians, including loss of life and financial insecurity. Illegal gambling, human smuggling, human trafficking, robbery, theft (including auto theft), cross border smuggling, corruption, ransomware, and other types of extortion also remain substantial money laundering threats that pose significant harms to Canadians. Collectively, these threats involve OCGs and money laundering networks that are national and international in scope.

- Canada’s terrorism financing landscape overall remains low volume and low value. Most terrorist attacks in Canada over the past decade have been perpetrated by ideologically motivated lone actors. These ideologically motivated attacks have had a low level of sophistication, which generally require fewer resources. The main foreign-based threat actors with observed terrorism financing links to Canada are religiously and/or politically motivated. These groups are observed to rely on diversified funding sources and methods, including crowdfunding, cryptocurrencies, informal value transfer systems (IVTS), state sponsorship, abuse of non-profit organizations (NPOs), and criminal activity.

- Canada's vulnerability landscape remains relatively stable. Domestic systemically important banks, private corporations, express trusts, crypto assets, and certain types of money services businesses (MSBs) are the sectors, corporate structures and payment products most inherently vulnerable to exploitation for money laundering and terrorist financing. They are highly accessible to individuals both within Canada and abroad and feature high transaction volumes and rapid processing times. In some cases, they offer the potential for transactions to be conducted with reduced transparency and complex structures that obscure the origin and destination of funds. Businesses that engage with politically exposed persons, jurisdictions that have weak AML/ATF frameworks or where listed terrorist entities are known to operate, may be exposed to higher money laundering and terrorist financing risks requiring enhanced due diligence.

- Most higher risk sectors, including those offering high-risk products and services, are regulated under the PCMLTFA, which requires robust compliance measures and due diligence to prevent, detect, and report suspected money laundering and terrorist financing. Other higher risk sectors, such as corporations and legal professionals, are also subject to federal, provincial or territorial regulatory requirements, or professional standards. These mitigation measures contribute to lowering inherent money laundering and terrorist financing vulnerabilities.

- The vast majority of NPOs in Canada present little to no risks for money laundering and terrorist financing, with only a small sub-set undertaking activities that are vulnerable to terrorist financing abuse. These risks should be evaluated on a case-by-case basis, based on credible information and taking into account mitigation measures. NPOs are subject to administrative oversight at the federal, provincial, and territorial levels, particularly regarding incorporation or tax status.

- Since 2018, the Government of Canada has invested nearly $470 million to strengthen data resources, financial intelligence, information sharing, and investigative capacity to support money laundering and terrorist financing investigations. Public-private partnerships have been established to target several of Canada’s higher money laundering and terrorist financing threats. Canada continues to prioritize advancing further measures to strengthen the prevention, detection, and disruption of money laundering and terrorist financing and address persistent and emerging risks.

- Looking ahead, the Government of Canada is monitoring key trends that are expected to shape Canada’s money laundering and terrorist financing risk landscape. Foreign interference that seeks to threaten Canadian communities and undermine Canada’s sovereignty, democratic institutions, and national interests remains a concern. Fraud remains a dynamic and growing threat increasingly enabled by new technologies, such as artificial intelligence, and mis-and-disinformation. There is also a growing nexus between transnational organized crime and terrorism, including terrorist actors who leverage organized crime networks for support, and OCGs that can carry out terrorist activities. The Government of Canada continues to develop risk-based responses to protect Canadians and the Canadian financial system.

Introduction

Money laundering and terrorist financing pose serious threats to the safety and security of Canadians, as well as the integrity of the financial system.

Money laundering underpins most criminal activity in Canada and is the process used by criminals to convert or conceal the origin of proceeds of crime to make it appear as if it originated from legitimate sources. It supports, rewards, and perpetuates criminal activity, such as drug and human trafficking, theft, and fraud, by enabling criminals to benefit from the proceeds of their crimes. Though difficult to quantify due to the clandestine nature of these activities, the Criminal Intelligence Service Canada (CISC) estimates that between $45 billion and $113 billion[1] is laundered in Canada per year.

Terrorist financing, in contrast, is the collection and provision of property, such as funds, obtained from lawful or unlawful sources, for the benefit of, or use by, a lone terrorist actor or terrorist group. While the volume of terrorist financing in Canada is assessed to be low, the consequences of enabling deadly and destructive terrorist attacks in Canada and abroad are grave.

The Government of Canada is committed to combating money laundering and terrorist financing. This is achieved through a robust and federal AML/ATF Regime composed of 13 federal departments and agencies with related policy, regulatory, intelligence, and enforcement mandates. The federal Regime works with provincial and municipal counterparts and over 38,000 Canadian businesses with reporting obligations under the PCMLTFA, known as reporting entities, to prevent, detect, and disrupt these unlawful activities.

Understanding money laundering and terrorist financing risks is a foundational element of Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime Strategy, which sets out the government's priority actions to respond to its ever-evolving risk and operating environment and improve performance and outcomes.

The National Risk Assessment is a core element of a larger framework to support an ongoing process to identify, assess, and mitigate money laundering and terrorist financing risks in Canada. This framework is summarized in Figure 1.

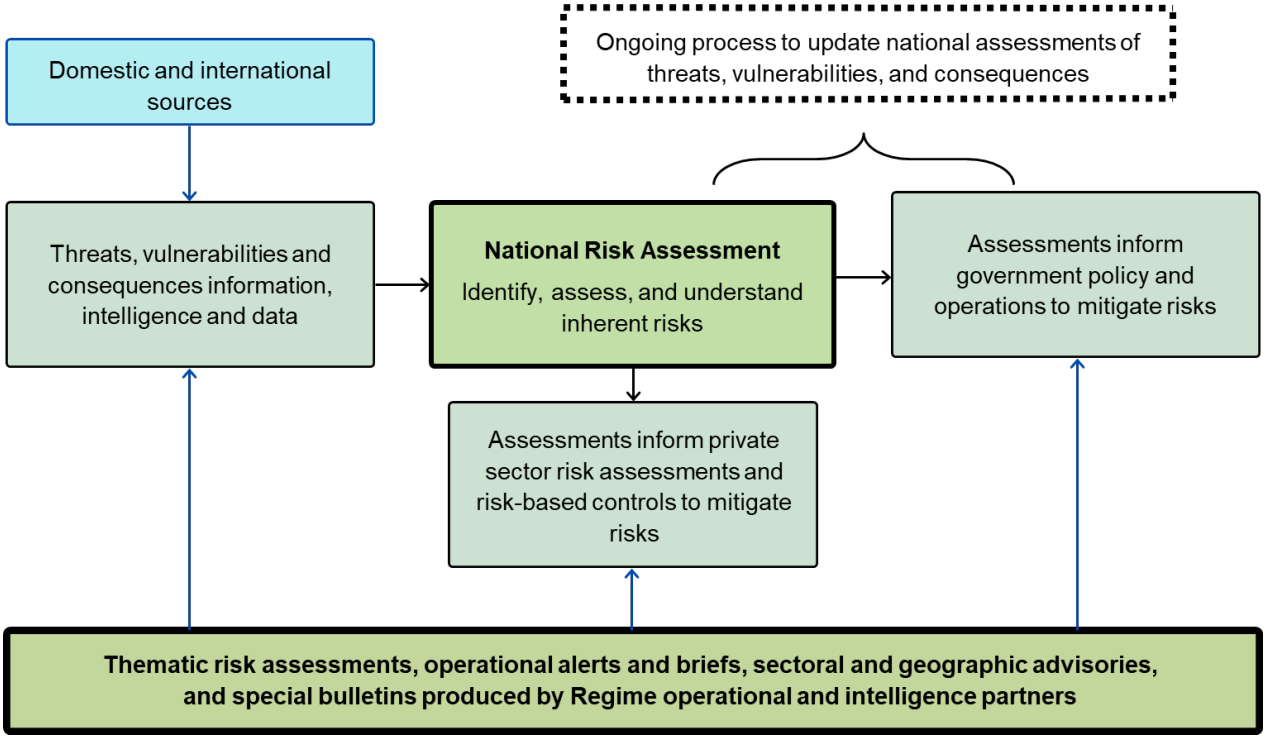
The 2025 *Assessment of Money Laundering and Terrorist Financing Risks in Canada* (the 2025 Report) facilitates a coherent, risk-based approach to mitigating the most pressing money laundering and terrorist financing risks in Canada. It is intended to support evidence-based policymaking, resource allocation, and operational priority setting by public authorities. It also supports the application of focused and proportionate mitigating measures by private sector businesses and non-government organizations to combat money laundering and terrorist financing.

The 2025 Report integrates insights from operational activities, financial intelligence, and reporting entities and other stakeholders. The assessment includes analysis of qualitative and quantitative data from various sources, including observations of law enforcement, tax and border authorities, financial and criminal intelligence, public and private sector data, and insights drawn from international collaborations.

[1] All dollar denominations cited in the 2025 Report are in Canadian dollars (CAD), unless otherwise indicated.

Figure 1

Canada's Money Laundering and Terrorist Financing Risk Assessment Framework



The 2025 Report builds on risk assessments published in 2015 and 2023 to enhance the analysis of inherent threats and vulnerabilities. Notably, the 2025 Report applies a residual risk lens to highlight the ongoing measures the Government of Canada, provincial and territorial governments, supervisory bodies, law enforcement, and the private sector are applying to mitigate the money laundering and terrorist financing vulnerabilities faced by specific businesses, professions, corporate structures, and financial products. This additional analysis helps contextualize the inherent threats and vulnerabilities present across the Canadian risk landscape within the tangible actions taken by various actors to keep these risks in check.

The 2025 Report provides a snapshot of Canada's risk situation with information available up to December 31, 2024, unless otherwise noted, and excludes some information for reasons of national security. It is complemented by strategic intelligence products, risk assessments and risk-based guidance published by Regime partners on an ongoing basis, further outlined in Annex C.

Chapter 1: Canada's Risk Context

Consequences of Money Laundering and Terrorist Financing

Money laundering and terrorist financing have serious social, economic, and political consequences (see Table 1). Although money laundering and terrorist financing may involve different threat actors and typologies, both exploit the economy and financial systems by leveraging the vulnerabilities that allow for anonymity and opacity in transactions.

Financial motivation ultimately underpins organized criminal activity in Canada, including that related to drug trafficking, human trafficking, fraud, and auto-theft. Money laundering is what enables these criminals to enjoy the profits of their crimes, helping sustain a wide range of serious criminality, both in Canada and abroad. This in turn poses risks to the safety, security, and financial well-being of Canadians, while also causing reputational damage to Canada's economy and international standing.

Money laundering can have negative economic and social consequences for Canadians. It enables criminal activity such as fentanyl trafficking leading to opioid overdoses that are devastating communities and families across Canada. A 2024 study by the Australian Institute of Criminology highlights how money laundering can drive corruption, unfair competition, and overall market distortions as a result of criminal activities or as criminals divert funds from victims into assets that are attractive for money laundering.[2] For example, the Expert Panel on Money Laundering in British Columbia (BC) Real Estate cautiously estimated a 5 per cent increase in the price of residential real estate in BC due to money laundering.[3]

Money laundering linked to tax evasion deprives governments of revenues and capacity to spend on public infrastructure, goods, and services. Statistics Canada estimated underground economic activity, i.e., activity that escapes measurement due to being hidden, illegal, or informal, at $68.5 billion, or 2.7 per cent of total gross domestic product (GDP) in 2021.[4]

Terrorist financing supports the activities of ideologically, politically, and religiously motivated violent extremist or terrorist groups. It does not require substantial financial resources to facilitate high impact attacks. The consequences of terrorist violence can contribute to a state of insecurity both at home and abroad, and include the loss of life, destruction of property, and a climate of fear and diminished level of civic trust among Canadians.

Canada's prosperity, financial and economic integrity, and reputation are harmed when public or private institutions fail to observe high professional, ethical, or legal standards, or otherwise effectively combat money laundering and terrorist financing. This in turn can impact investment decisions and investor confidence in Canada as a good place to do business, as well as Canada's standing more broadly with key international partners.

[2] Australian Institute of Criminology (2024) Impacts of money laundering and terrorism financing: Final Report.
[3] Expert Panel on Money Laundering in BC Real Estate (2019) Combatting Money Laundering in BC Real Estate
[4] Statistics Canada (2023) The underground economy in Canada, 2021

Table 1
Harmful Effects of Money Laundering and Terrorist Financing in Canada

Societal Consequences • Increased serious and organised criminal and terrorist activity • Increased corruption risks and victimization, including financial victimization, loss of property, physical violence, loss of life and emotional trauma • Loss of public revenues available to fund health, education and social services due to lost tax revenues and increased spending on law enforcement and security
Economic Consequences • Increased distortions across consumption and savings, market signals and investment that undermine economic growth and prosperity • Criminal abuse of financial institutions eroding stability and undermining the integrity of the financial system • Growing underground economy, characterized by unfair competition, and reduced wages, benefits, and government tax revenues • Reputational damage to Canada's economy and vulnerable business sectors and professions
Political Consequences • Perceived attractiveness as a jurisdiction for money laundering and terrorist financing • Lower confidence and trust in Canada's private and public institutions both domestically and internationally

Canada's Domestic Context

The geopolitical, socio-economic, governance, and legal structures of a country are all elements that shape its national context and risk landscape. Canada has a stable and open economy with strong democratic institutions. These features are among Canada's strengths but may also be exploited by criminals to launder proceeds of crime and finance criminal or terrorist activities.

Legal Framework, Geography, and Demographics

In Canada, legislative powers are divided between the two orders of government – federal and provincial.[5] At the federal level, the Parliament of Canada exercises exclusive legislative jurisdiction over various matters including criminal law and procedure, the regulation of trade and commerce, currency and coinage, banking, and matters of national concern. The Canadian Parliament also has jurisdiction to make laws in relation to the incorporation of certain companies. The federal AML/ATF Regime is underpinned by laws rooted in federal jurisdiction. These laws notably include the *Criminal Code* of Canada, which sets out the general criminal law offences applicable across the country, as well as the core procedural framework applicable to criminal prosecutions.

At the provincial level, each provincial legislature exercises exclusive legislative jurisdiction within its respective territory over certain matters, including the administration of criminal and civil justice, property and civil rights, the incorporation of certain companies, and matters of a local nature. As a result, many businesses and professions that are vulnerable to money laundering and terrorist financing threats are regulated at the provincial level, while also being subject to federal regulation for AML/ATF.

[5] Government of Canada (2021) The constitutional distribution of legislative powers

The prosecution of most *Criminal Code* offences is the responsibility of provincial Attorneys General. The Public Prosecution Service of Canada (PPSC), on behalf of the Attorney General of Canada (AGC), has responsibility for the prosecution of criminal offences under other Acts of Parliament, notably the *Controlled Drugs and Substances Act* and the *Cannabis Act*. The AGC may also prosecute the laundering of proceeds of crime obtained from the commission of offences which the AGC has jurisdiction to prosecute, such as for terrorism and terrorist financing offences and specified organized crime offences.

Policing is similarly a matter of shared responsibilities and cooperation, with both the Royal Canadian Mounted Police (RCMP) and provincially constituted police forces (whether municipal or provincial) engaged in the application and enforcement of criminal law. Given its national scope of operations, the RCMP through its Federal Policing mandate plays a primary role in addressing complex money laundering schemes and serious organized crime.

Strong coordination between the federal, provincial, and territorial governments on AML/ATF matters is vital to understanding and mitigating money laundering and terrorist financing risks and for effective enforcement action.

Canada's geographic expanse and proximity to the Unites States (US), the world's largest economy and financial centre, can create opportunities for criminal activity and the laundering of proceeds of crime. In particular, the close economic ties between Canada and the US, characterized by the high volume of passengers, goods, and funds that flow across the border on a routine basis, present opportunities that transnational OCGs and money launderers can exploit to move funds and value across the border. Canada's vast territory also creates challenges for the detection and disruption of criminal activity and movement of associated proceeds of crime.

Approximately 87 per cent of Canada's 41 million residents live in the country's four largest provinces: Ontario (39 per cent), Québec (22 per cent), BC (14 per cent), and Alberta (12 per cent).[6] Canada's three largest cities by population – Toronto, Montreal, and Vancouver – are major cultural and economic hubs with a significant financial sector presence. Organized criminal activity is often targeted to the concentration of population and economic activity in these areas, including financial crime, auto theft, frauds targeting specific diaspora communities, and exploitation of hot real estate markets. At the same time, new economic opportunities in underdeveloped parts of Canada, such as Canada's northern or more remote communities, which often have more limited law enforcement resources, can also be exploited by criminal groups.

Canada fosters a multicultural and diverse society that continuously integrates new Canadians. According to Statistics Canada's 2021 Census, 26.4 per cent of the population are first-generation Canadians, and Canadians encompass more than 450 ethnic origins.[7] Many Canadians have strong personal and financial ties to communities around the world. The World Bank estimates that in 2023, Canadians sent over US$8.5 billion in overseas remittances and received close to US$850 million.[8] Remittances are an important and necessary source of financing for sustainable economic growth and development in many parts of the world. However, this activity may nonetheless be exploited by illicit threat actors. Canada has prioritized promoting affordable channels, with AML/ATF controls, to send and receive money from abroad.

[6] Statistics Canada (2022) Census Profile, 2021 Census of Population
[7] Statistics Canada (2022) The Canadian census: A rich portrait of the country's religious and ethnocultural diversity
[8] World Bank (2023) Personal remittances, paid (current US$) - Canada | Data; Personal remittances, received (current US$) - Canada | Data

Economy, Trade and Financial System

As of year-end 2023, the International Monetary Fund (IMF) estimated that Canada ranked as the 10th largest economy in the world in terms of nominal GDP.[9] According to Statistics Canada, international trade in goods and services represents more than 64 per cent of Canada's GDP.[10]

Canada's largest trading partner is the US – in 2023, over 77 per cent of Canada's merchandise exports went to the US, and over 50 per cent of Canada's merchandise imports came from the US.[11] Approximately 51 per cent of Canada's total exports of services went to the US, while roughly 59 per cent of its total imports of services came from the US.[12] Canada ranked among the top five global destinations for US foreign direct investment (FDI),[13] while 50% of Canada's FDI went to the US in 2023.[14] Other key trading partners include the European Union, China, Mexico, Japan, and the United Kingdom, for both merchandise and services exports and imports.[15]

Canada's open and extensive trade with countries around the world present vulnerabilities for trade fraud and trade-based money laundering, threats which the government has increased resources and tools to combat.

Canada has a large and mature financial system, with $8.3 trillion in assets held by financial institutions as of year-end 2023.[16] According to the Canadian Bankers Association, 40 per cent of financial institution assets are concentrated in the banking sector, which is dominated by six large domestic systemically important banks (D-SIBs), two of which are also considered to be globally systemically important,[17] which in aggregate, hold 93 per cent of total banking assets.[18] The life insurance sector in Canada is also highly concentrated, with the three largest life insurers accounting for over 70 per cent of total net premiums.[19]

Canada has a high rate of financial inclusion with 99.6 per cent of the population over the age of 15 having an account with a formal financial institution.[20] The adoption of digital finance, alternative financial technologies, and non-face-to-face financial interactions is on the rise across the country, with 82 per cent of Canadian Internet users conducting online banking in 2022.[21]

[9] IMF (2024) World Economic Outlook Database, April 2024 (imf.org)
[10] Statistics Canada (2025) Gross domestic product, expenditure-based, at 2017 constant prices, annual (x 1,000,000)
[11] Global Affairs Canada (2024) Highlights of Canada's merchandise trade performance - 2023 update
[12] Statistics Canada (2024) Annual international trade in services, 2023
[13] Bureau of Economic Analysis – US Department of Commerce (2024) Direct Investment by Country and Industry, 2023
[14] Statistics Canada (2024) Foreign direct investment, 2023
[15] Global Affairs Canada (2024) Highlights of Canada's merchandise trade performance - 2023 update
[16] IMF (2025) Financial Sector Assessment Program
[17] Canada's DSIBs include the Bank of Montreal, Bank of Nova Scotia, Canadian Imperial Bank of Commerce, National Bank of Canada, Royal Bank of Canada, and Toronto Dominion Bank. The Royal Bank of Canada and Toronto Dominion Bank are also considered to be globally systemically important. OSFI (2024) Systemically important banks
[18] Bank of Canada (2025) The International Exposure of the Canadian Banking System
[19] Estimate based on Canadian life insurance company 2023 annual reports.
[20] World Bank (Accessed 2025) Global Financial Inclusion data, 2021.
[21] Statistics Canada (2024) Trends in online banking and shopping

A 2023 study by the Ontario Securities Commission found that 10 per cent of Canadians own crypto assets, with crypto asset adoption in Canada primarily driven by investors.[22]

Given the dominance and concentration of the formal financial sector in Canada, it is an important area of focus for AML/ATF regulation and supervision policy initiatives, including adapting Canada's framework to address the growing use of new technologies.

Cash Dynamics in the Canadian Economy

While cash remains widely available in Canada, its use has declined since the early 2000s. According to Payments Canada, cash was used in 11 per cent of transactions in 2023. The average cash transaction was $26, and cash use declined by 20 per cent in terms of volume since 2019.[23] Cash is most typically obtained in Canada through automated-banking machines, also referred to as 'automated-teller machines' (ATMs), and used for purchases.[24]

Quick Definitions

Crypto assets and cryptocurrency

Crypto assets, as defined by the Canadian Securities Administrators, are purely digital assets that use public ledgers over the internet to prove ownership. They use cryptography, peer-to-peer networks, and distributed ledger technology, such as blockchain, to create, verify, and secure transactions. They may be used as a medium of exchange, a way to store value, or for other business purposes.

There are different types of crypto assets. One such type is ***cryptocurrency***, which is a digital currency or medium of exchange that is not legal tender. It can be used to buy products or services, or for speculative purposes, such as trading on crypto asset trading platforms.

The PCMLTFA and its Regulations use the terminology "virtual currency," which can broadly include types of both crypto assets and cryptocurrency. Whenever the term "virtual currency" is used in the document, it is in specific reference to the meaning under the PCMLTFA and its Regulations.

The use of cash on its own is not indicative of the presence of criminal activity. However, certain inherent characteristics of cash, particularly its anonymity, can make it attractive to money launderers and terrorist financiers. For example, economically motivated crimes, such as drug or firearm trafficking, generate large amounts of illicit cash proceeds. Cash is also used to transport large sums of money obtained from criminal activities, including across international borders.

Money launderers can use cash transactions to convert the proceeds of crime into legitimate assets that store value and can be sold, thereby effectively 'cleaning' the funds, and/or for personal consumption, such as purchasing real estate, vehicles, jewellery, and other goods or services.

For these reasons, individuals and businesses transacting in a substantial amount of cash, and with no reasonable explanation for its source, may pose high money laundering risks. Large cash transaction reporting requirements help mitigate these risks.

[22] Ontario Securities Commission (2023) Crypto-Asset Survey 2023 - Final Report
[23] Payments Canada (2024) Canadian Payment Methods and Trends
[24] Bank of Canada (2024) 2023 Methods-of-Payment Survey Report: The Resilience of Cash

International Context

Canada is a founding member of the FATF, the international AML/ATF standard setting body. The FATF publishes lists of high-risk jurisdictions with serious strategic deficiencies to counter money laundering, terrorist financing, and proliferation financing. The FATF requires its members to apply enhanced due diligence, and in the most serious cases, countermeasures to protect the international financial system from these jurisdictions.

Canada also undertakes its own assessments to identify jurisdictions of concern for money laundering, terrorist financing, and sanctions evasion that are not included on the FATF's list of high-risk jurisdictions. This may include intermediary jurisdictions observed to be used to bypass controls for FATF high-risk jurisdictions; those with strong financial links to Canada that have significant informal banking sectors or banking secrecy, high levels of corruption, and/or social, economic, or institutional instability; or jurisdictions or locations of concern according to Canada's national security interests.

In order to safeguard the integrity of Canada's financial system, Canada's Minister of Finance can issue directives to PCMLTFA reporting entities to apply enhanced measures when dealing with foreign entities and/or foreign states at both the national and sub-national levels. These directives provide the Minister of Finance a mechanism to respond to emerging cross-border risks based on information provided by international organizations or domestic competent authorities.

Ministerial Directives have been issued specific to the Democratic People's Republic of Korea (DPRK) in December 2017, and the Islamic Republic of Iran in July 2020, which are subject to call for action by the FATF. [25] A Ministerial Directive specific to the Russian Federation was issued in February 2024 due to emerging money laundering concerns identified by the Government of Canada, and supported by a FINTRAC bulletin.[26] These Ministerial Directives are regularly reviewed and updated in response to emerging risks. The Ministerial Directives on Russia and DPRK were updated in March 2025 due to the growing risks associated with these two jurisdictions, stipulating additional measures to be taken by reporting entities in order to safeguard Canada's financial sector.

FINTRAC also requires its reporting entities to be aware of the risks and encourages enhanced customer due diligence for financial transactions related to Myanmar, which is subject to a FATF call for enhanced and risk-based due diligence measures.

FINTRAC data suggests that the scale of the financial connectivity between Canada and Iran and Russia is very small, with each jurisdiction representing less than one per cent of the value of all international electronic funds transfers reportable to FINTRAC in any given year. Further, there is no direct trade or financial links between Canada and the DPRK due to the comprehensive prohibitions in place under Canadian sanctions laws. However, analysis by FINTRAC and its partners shows that some illicit actors use intermediary jurisdictions to obfuscate the source and destination of funds in order to bypass Canadian reporting requirements and restrictions.

[25] FINTRAC (2025) FINTRAC guidance relating to the Ministerial Directive on the Democratic People's Republic of Korea (DPRK) issued on December 9, 2017; FINTRAC (2024), FINTRAC guidance related to the Ministerial Directive on Financial Transactions Associated with the Islamic Republic of Iran issued on July 25, 2020

[26] FINTRAC (2025) FINTRAC guidance related to the Ministerial Directive on Financial Transactions Associated with Russia issued on February 24, 2024; FINTRAC (2023) Special Bulletin on Russia-linked money laundering activities

FINTRAC has highlighted other jurisdictions and locations of concern. Chinese professional money launderers have been observed to exploit underground banking schemes that enable circumvention of Chinese government currency controls. The United Arab Emirates has been highlighted as an observed intermediary jurisdiction used for illicit financial flows from China, Hong Kong, and Iran. FINTRAC has also observed Türkiye and countries of the Commonwealth of Independent States as intermediary jurisdictions for Russia-linked money laundering and sanctions evasion schemes.

In developing assessments relevant to cross-border risks, FINTRAC draws insights on existing and developing issues from a range of domestic and international sources, as well as private sector reporting.

Emerging Trends Shaping Canada's Risk Context

Canada's money laundering and terrorist financing risk context remains dynamic and evolving, influenced by broader trends in geopolitics, criminality, technology, culture, and the domestic and global regulatory and enforcement landscape. These trends and associated money laundering risks continue to be monitored by Canada's AML/ATF Regime partners.

Emerging risks from foreign interference

The *Canadian Security Intelligence Service Act* (CSIS Act) defines "threats to the security of Canada" as including "foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person." These activities are commonly called foreign interference and are almost always conducted to further the interests of a foreign state to Canada's detriment. Foreign interference poses a threat to Canada's sovereignty, democratic institutions, national interests, and values.

Quick Definitions

Disinformation is false or manipulated information, deliberately spread with the intent to mislead others by individuals who know it to be untrue.

Misinformation is false or manipulated information, spread without the intent to deceive or mislead.

Foreign states use a variety of techniques to conduct foreign interference, such as elicitation, cultivation, coercion, illicit financing, malicious cyber activities, mis-and-disinformation, and espionage. Examples of interference by foreign states, or those acting on their behalf, include:

- threats, harassment or intimidation by foreign states, or those acting on their behalf, against anyone in Canada, Canadian communities, or their loved ones abroad; and
- targeting officials in different Canadian jurisdictions to influence public policy and decision-making in a way that is covert, deceptive, or threatening.[27]

Foreign states seeking to interfere in Canada often rely on networks of proxies within Canada to carry out their activities. These actors and their proxies may use financial resources, whether legally or illegally obtained, to support transnational repression methods, such as harassment, intimidation, threats, and violence.

Money laundering techniques are often employed to obscure the origin of funds, typically provided by state actors, and their destination, which is used to finance foreign interference activities. Foreign states seeking to funnel money into foreign interference activities can take advantage of existing networks, often

[27] Public Safety Canada (2023) Foreign Interference and Canada

criminal in nature, to co-mingle and launder funds from different sources. They may also transfer funds to specific communities in Canada, religious or cultural organizations, or politically exposed persons (PEPs) who are vulnerable to being exploited for money laundering and terrorist financing.

The RCMP has identified the collaboration between foreign actors and OCGs in Canada to carry out intimidation and other interference activities. This potential connection between hostile states and transnational OCGs heightens the threat of foreign interference.

While the threat of foreign interference is not new, it remains a significant concern as the world becomes more competitive and some states become more willing to use all means available to them to challenge democracy and the existing global order.[28]

Nexus between transnational organized crime and terrorism

As highlighted by the 2019 *United Nations Resolution 2482*, there is a growing nexus between terrorism and transnational organized crime, creating a bond of mutual interest. Terrorists can leverage organized crime for logistical support and to finance their activities through illicit trade in natural resources, kidnapping for ransom, extortion, and other illegal operations.

In February 2025, Canada listed several transnational OCGs as terrorist entities for their involvement in terrorism. These entities are criminal organizations that, through their activities and operations, carry out, attempt to carry out, participate in or facilitate terrorist activity by taking hostages, attacking civilian and critical infrastructure, and working to diminish the ability of local governments to function effectively and enforce laws. These groups have also used improvised explosive devices to generate terror and intimidate local populations, including attacking roads, hindering the passage of state forces, and striking specific targets. In addition, the drug trafficking activities of these groups threaten national security and must be stopped using all tools available.

New and developing technologies

Rapid technological advancements have profoundly impacted Canada's AML/ATF operating environment in recent years. Technology continues to shape criminal financial activity, as well as the mitigation efforts advanced by Canadian regulators and law enforcement.

Notably, the misuse of artificial intelligence (AI), particularly generative AI,[29] presents growing risks of exploitation by criminals and OCGs, who increasingly rely on technology to automate and enhance their illicit operations. The power of AI can be magnified when coupled with other emerging technologies, such as quantum computing, which has potential capabilities to enable faster and more accurate processing of complex data.

Quick Definitions

Generative artificial intelligence is a type of artificial intelligence trained on large data sets to produce content like text, audio, code, videos, and images based on user input.

Quantum computing combines computer science and physics and uses the principles of quantum mechanics to solve problems that are too complex in scope for classical computers.

According to the Canadian Centre for Cyber Security, the use of chatbots and AI-generated persuasive emails is expected to further escalate fraud and scams, causing greater harm to victims. Generative AI tools can produce counterfeit identification documents, which can be used to establish shell companies or open bank accounts, bypassing traditional

[28] Public Safety Canada (2023) Countering Foreign Interference

[29] Government of Canada (2024) Guide on the use of generative artificial intelligence

identity verification processes and further aiding criminals in carrying out their fraudulent activities. FINTRAC has noted that extremist groups and fraudsters may use AI-generated images depicting fabricated human rights abuses, conflict zones, or natural disasters to raise funds. Furthermore, generative AI can automate and obscure financial transactions, making it more challenging to trace the origins and destinations of illicit funds.

Despite these risks, AI offers transformative potential to enhance the effectiveness and efficiency of AML/ATF efforts. In 2023, FINTRAC launched a new modernization vision to address emerging threats arising from technological innovation. This initiative focuses on establishing and enhancing the skills, processes, and technologies FINTRAC needs to detect and combat money laundering and terrorist financing in real time. Advanced AI systems also support risk management and compliance functions at financial institutions by analyzing complex financial data, detecting anomalous trends, and identifying potential indicators of money laundering and terrorist financing.[30]

The rise of decentralized finance (DeFi) also demonstrates potential to impact the evolving AML/ATF operating environment. "DeFi" is an umbrella term for an internet-based financial system that uses blockchain technology to enable individuals to transact with each other directly without the need for intermediaries to facilitate transactions. DeFi platforms deal exclusively in crypto assets and can host virtual versions of traditional financial products and services, such as lending, options, and derivatives.

DeFi platforms are online and therefore have global reach, enabling anonymous and rapid cross-border transfers, often without employing the identity verification and client due diligence processes typically conducted by traditional financial intermediaries, such as banks, MSBs or stock exchanges. As a result, transnational criminals are increasingly using crypto assets and DeFi platforms to move illicit funds to avoid triggering AML/ATF obligations.[31]

Stereotypes, bias, and online discourse

Social media and the internet have the power to amplify both information and mis-and-disinformation at unprecedented speeds. Governments, law enforcement, and the private sector must remain vigilant about the potential consequences of mis-and-disinformation, stereotypes and implicit bias when collecting and analyzing information to assess money laundering and terrorist financing risk. Indigenous, racialized, and religious minority communities in Canada experience an increased risk of negative stereotypes and bias.

Stereotypical assumptions fueled by biased or incomplete portrayals of certain groups, races or religions are particularly problematic, as they can skew perception and overestimate the risk of certain customers or sectors relative to actual money laundering and terrorist financing threats. This can contribute to derisking or limiting access to financial services to entire communities or sectors who may then turn to informal or unregulated financial channels that are even more vulnerable to money laundering and terrorist financing risks. Customer due diligence and risk assessment processes should seek to draw on credible, evidence-based, and corroborated information and objective analysis to counteract the challenges of mis-and-disinformation and bias.

[30] Citigroup (2023) Artificial Intelligence – A Game Changer
[31] Financial Crime Academy (2025) Unmasking the Shield: A Closer Look at AML Frameworks for DeFi Platforms

Changing regulatory enforcement landscape

As Canada continuously adapts its AML/ATF framework and supervisory and enforcement responses to evolving AML/ATF risks, threat actors will continue to shift their money laundering and terrorist financing methods and techniques. Illicit actors may seek out unregulated or under-regulated sectors, such as those not covered by the PCMLTFA or subject to robust AML/ATF requirements, to exploit gaps in regulation and enforcement.

For example, as beneficial ownership registries are established and implemented across Canada and globally, illicit actors may seek out jurisdictions with lower corporate ownership transparency requirements. Increased transparency in certain jurisdictions will aid authorities in unraveling the complex corporate structures often exploited by threat actors and third-party money launderers. However, jurisdictions with lower corporate transparency may become more vulnerable to money laundering and terrorist financing threats.

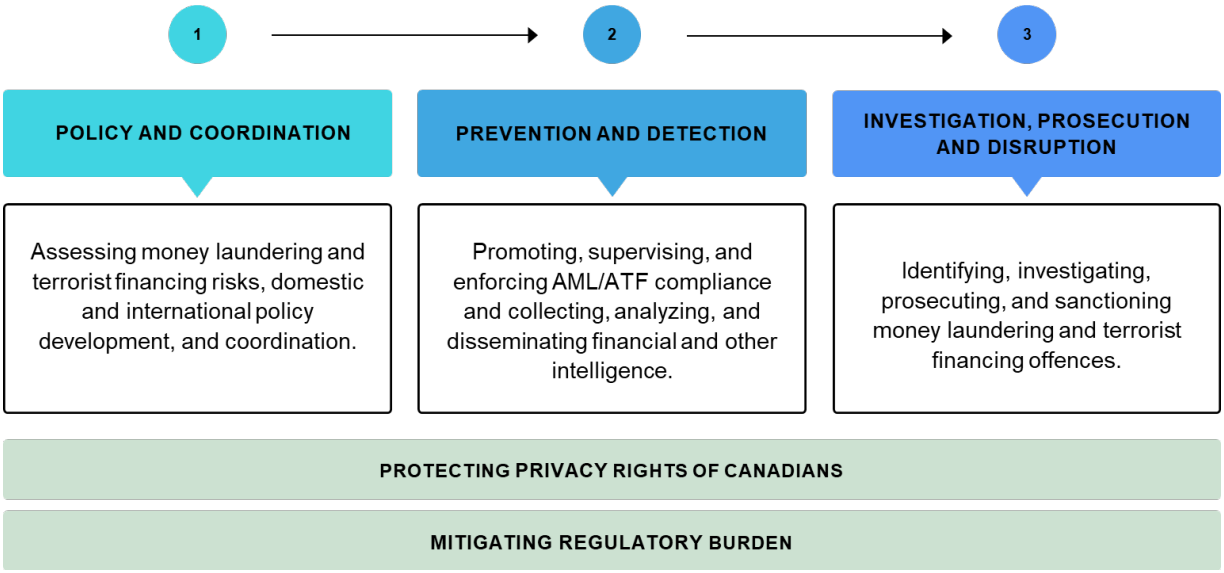
Chapter 2: Canada's Risk Mitigation Framework

Canada has a comprehensive AML/ATF Regime that provides a coordinated approach to mitigating the money laundering and terrorist financing risks identified in this assessment and in combating financial crime more broadly. The Regime also complements the work of law enforcement and intelligence agencies engaged in fighting domestic and transnational organized crime and terrorism.

The AML/ATF Regime consists of 13 federal Regime partners, including the Canada Border Services Agency (CBSA), the Canada Revenue Agency (CRA), the Canadian Security Intelligence Service (CSIS), Finance Canada, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), Global Affairs Canada (GAC), Innovation, Science and Economic Development Canada (ISED), Justice Canada, the Office of the Superintendent of Financial Institutions (OSFI), the Public Prosecution Service of Canada (PPSC), Public Safety Canada, Public Services and Procurement Canada (PSPC), and the Royal Canadian Mounted Police (RCMP).

The AML/ATF Regime operates on three interdependent pillars: (i) policy and coordination; (ii) prevention and detection; and (iii) investigation, prosecution, and disruption.

Figure 2
AML/ATF Regime Pillars



i. Policy and Coordination

The first pillar consists of the Regime's policy and legislative framework, as well as its domestic and international coordination led by Finance Canada. The PCMLTFA is the legislation that establishes Canada's AML/ATF framework, in conjunction with other key statutes, including the *Criminal Code*.

The PCMLTFA requires financial institutions and designated non-financial businesses and professions, known as reporting entities, to identify their clients, keep records, and establish and administer an internal AML/ATF compliance program. The PCMLTFA creates a mandatory reporting system for suspicious financial transactions, large cross-border currency transfers, and other prescribed transactions. It also creates obligations for reporting entities to identify money laundering and terrorist financing risks and to put in place measures to mitigate those risks.

The PCMLTFA also establishes an information sharing regime where, under prescribed legal thresholds, information submitted by reporting entities is analyzed by FINTRAC and the results are disseminated to operational Regime partners. Information disseminated under the PCMLTFA can assist the investigation and prosecution of money laundering and terrorist financing related offences. This information can also inform FINTRAC trend and typology reports to help educate the public and reporting entities on related issues.

The *Criminal Code* is Canada's general criminal statute setting out the substantive criminal law and procedure. It contains the laundering proceeds of crime and terrorist financing offences, as well as a broad range of other offences, including those that may be predicate offences for money laundering. These include fraud, extortion, corruption, illegal gaming, counterfeiting, robbery and theft, and trafficking in persons offences, among others.

The *Criminal Code* also sets out general investigative powers available to law enforcement, including production orders, tracking and tracing powers, as well as search, seizure, and restraint powers. The *Criminal Code* includes sentencing rules as well as frameworks for forfeiture of offence-related property and proceeds of crime.

Other statutes also contribute to Canada's AML/ATF framework. For example, the federal *Income Tax Act* contains obligations regarding the registration of trusts with the CRA, and the *Canada Business Corporations Act* and equivalent provincial and territorial statutes set out beneficial ownership transparency requirements.

Domestic policy coordination on AML/ATF issues takes place through three main committee structures that meet regularly throughout the year. These include:

1) An interdepartmental governance structure, consisting of senior-level representatives from the AML/ATF Regime partners, that advances new and ongoing policy initiatives and monitors performance;
2) A public-private Advisory Committee on Money Laundering and Terrorist Financing (ACMLTF), consisting of senior representatives from federal agencies and reporting entity sectors, that facilitates the exchange of information relevant to money laundering and terrorist financing risks, policy development and implementation; and
3) Federal, provincial, and territorial working groups, consisting of policy and supervisory representatives from financial sector regulation, security, corporate law, and law enforcement across all Canadian jurisdictions, that coordinate on policy issues in areas where jurisdiction is shared. This includes advancing a pan-Canadian beneficial ownership transparency framework.

The AML/ATF Regime supports and enhances the efforts of law enforcement and intelligence agencies engaged in fighting domestic and transnational organized crime as well as terrorism, contributing to Canada's broader counter-terrorism and national security efforts. Cutting off revenue streams and depriving terrorists and other violent extremist groups of funds and property is one of the most effective ways to undermine their activities. The AML/ATF Regime's efforts are aligned with Canada's counter-terrorism strategy, which is currently being updated. The upcoming strategy will provide the Government of Canada strategic direction to address emerging terrorist and violent extremist threats; offer the Canadian public greater insights into today's threat environment and how the Government of Canada is addressing it; and enhance public trust and confidence in Canada's security and intelligence community by taking a whole-of-government approach that is focused on engagement with key partners in Canada and abroad.

Protecting the integrity of the international financial system from money laundering and terrorist financing requires a strong international presence to enhance legal, institutional, and operational capacity globally. Canada's international AML/ATF initiatives are advanced through the leadership role it plays in the G7, the G20, the Egmont Group of Financial Intelligence Units, the Joint Chiefs of Global Tax Enforcement (J5), and the counter-financing work stream of the Global Coalition against Daesh.[32]

Canada is a founding member and active participant in the FATF. Canada served as FATF Vice President from 2023 to 2025 and as Co-Chair of the FATF Regional Body, the Asia-Pacific Group on Money Laundering, from 2022 to 2024. The FATF develops international AML/ATF standards and monitors their effective implementation among its 40 FATF members and over 200 countries in the global FATF network through peer reviews and public reporting. The FATF also leads international efforts related to policy development, risk analysis, and identifies and reports on emerging money laundering and terrorist financing trends and methods. This work helps to ensure that countries have the appropriate tools in place to address money laundering and terrorist financing risks.

Canada also provides expertise and funding to increase AML/ATF capacity in countries seeking to strengthen their regimes, including through the Anti-Crime Capacity Building Program and the Counter-Terrorism Capacity Building Program administered by GAC.[33] These Programs also support the other AML/ATF Regime pillars by strengthening the capacity of other countries to prevent, detect, investigate, prosecute and disrupt AML/ATF activities, including those that may impact Canada.

ii. Prevention and Detection

The second pillar involves measures to prevent individuals from placing proceeds of crime or terrorist-related property into the financial system, as well as measures to detect the placement and movement of such property.

Central to the second pillar are the reporting entities that implement prevention and detection measures under the PCMLTFA, and the regulators that supervise them. FINTRAC is the primary agency conducting AML/ATF assessments of all reporting entities, including federally regulated financial institutions, to promote compliance with the PCMLTFA and its associated regulations. OSFI focuses on the prudential implications of a federally regulated financial institution's AML/ATF compliance, as part of its ongoing assessment of their regulatory compliance management frameworks. Certain reporting entities are also overseen by provincial and territorial regulators, many of whom issue guidance to their members in meeting their PCMLTFA obligations and enter into information sharing agreements with FINTRAC. The CRA also works to prevent the misuse of the charitable sector for terrorist financing purposes.

Greater transparency of legal persons, including corporations, and legal arrangements, including trusts, also contributes to preventing and detecting money laundering and terrorist financing. Consequently, the Government of Canada has put in place a publicly accessible beneficial ownership registry to improve the transparency of federally incorporated corporations, with similar measures being taken at the provincial level. Additional obligations on reporting entities to identify discrepancies in the beneficial owners of the corporations with whom they do business will also help support accurate and up to date registries to prevent the misuse of corporations for illicit activities.

FINTRAC is also Canada's financial intelligence unit; it acts at arm's length and independently from law

[32] Daesh, also known as the Islamic State, is listed as a terrorist entity in Canada. The Global Coalition against Daesh consists of 87 members that are committed to tackling Daesh on all fronts, including tackling Daesh's financing and economic infrastructure.

[33] Government of Canada (2019) Security Capacity Building Programs

enforcement authorities, such as the RCMP, provincial and municipal police services, and other entities to which it is authorized to disclose financial intelligence, such as securities regulators and foreign financial intelligence units. In 2023–24, FINTRAC produced more than 4,600 financial intelligence disclosure packages containing 297,733 financial transaction reports covering more than 900,000 financial transactions, in support of investigations of money laundering and terrorist financing and threats to the security of Canada.

iii. Investigation, Prosecution, and Disruption

The final pillar involves the investigation, prosecution, and disruption of money laundering and terrorist financing. Enforcement partners, supported by FINTRAC's intelligence disclosures, undertake investigations related to money laundering, terrorist financing, and other profit-oriented crimes.

As the national police force, and as the provincial or local police force in many jurisdictions, the RCMP plays a fundamental role in Canada's AML/ATF Regime by investigating money laundering and terrorist financing cases, making arrests, laying charges, and seizing funds or assets believed to be offence-related property (including property used in support of terrorist activity) or proceeds of crime. The RCMP also works with police of jurisdiction at the provincial and municipal levels in Canada to investigate and disrupt money laundering and terrorist financing activity in their communities, including through joint and independent investigations and through the Canadian Integrated Response to Organized Crime (CIROC). CIROC brings together major police forces in Canada to coordinate a strategic plan for combatting organized or serious crime through the integration of Canadian police efforts at the municipal, provincial, territorial, and national levels.[34]

The CBSA has the mandate and the authorities to detect, identify, and investigate the commercial trade fraud that underlies many trade-based money laundering schemes. Where a *Criminal Code* mandate is identified in addition to border legislation, the CBSA works with the RCMP through referral and support or more formally through cooperative joint force operations. CBSA also draws on its reporting authority under PCMLTFA Part 2 making it responsible for the administration and enforcement of reporting on the cross-border movement of currency or monetary instruments valued at $10,000 or more and any associated seizures as well as its authority under new PCMLTFA Part 2.1 to ensure the compliance of all goods imported and exported to and from Canada.

The CRA enforces tax laws through its Criminal Investigations Program, which investigates tax evasion, other serious tax crimes, and the money laundering activities linked to those offences with a view to refer cases to the PPSC. The CRA also utilizes a specialized civil audit program, the Illicit Income Audit Program, to audit individuals and businesses who are known to or suspected of deriving income from illicit activities and works with partners to coordinate actions such as garnishments, asset liens, and cash seizures to recover amounts owing.

The PPSC is responsible for initiating and conducting federal and territorial prosecutions, including those that involve money laundering and terrorist financing offences, and provides legal advice to law enforcement agencies over the course of their investigations. They are further supported by provincial prosecution services, who, according to Integrated Criminal Court Survey (ICCS) data from Statistics Canada, prosecute most money laundering offences brought before the courts in Canada. Provincial and territorial civil forfeiture offices also play an important role in the forfeiture of property suspected to relate to criminal activity.

[34] National Security and Intelligence Committee of Parliamentarians (2023) Special Report on the Federal Policing Mandate of the Royal Canadian Mounted Police - Chapter 4: Federal Policing Partnerships; The Canadian Integrated Response to Organized Crime (2020) National Methamphetamine Strategy

As money laundering and terrorist financing frequently have international dimensions, operational Regime partners have built and maintained partnerships with key foreign counterparts. The RCMP acts as a liaison for exchanging criminal intelligence with international police forces, including in the US and Five Eyes partner countries, and liaison officers assist in pursuing international money laundering and terrorist financing cases. The CRA can pursue international cases of tax evasion with the use of Exchange of Information instruments, such as bilateral and multilateral agreements. Canada also engages in formal mutual legal assistance and extradition led by the International Assistance Group of Justice Canada.

Further to this work, Regime partners participate in a wide range of working groups and committees to facilitate investigation and disruption internationally, such as the North American Drug Dialogue, the Five Eyes Law Enforcement Group, the INTERPOL Expert Group on AML, and the J5.

Regime Oversight and Enhancements

Assessments of Canada's AML/ATF Regime

Canada's AML/ATF Regime is subject to regular external reviews, including by committees and offices of Parliament, and international organizations, to ensure its effective operation and continuous improvement.

Key reviews contributing to Canada's policy responses to money laundering and terrorist financing risks include a statutory review of the PCMTFA by the Parliament of Canada every five years (most recently completed by the House of Commons Finance Committee in 2018), a privacy audit of FINTRAC every two years by the Office of the Privacy Commission (most recently in 2024), engagement between federal, provincial and territorial Ministers of Justice and Public Safety, and ad-hoc reviews of regime partners by the National Security and Intelligence Review Agency, to ensure national security and intelligence activities are lawful, reasonable, and necessary.

From 2019-2022, the Government of Canada participated in the Commission of Inquiry into Money Laundering in BC, known as the Cullen Commission, which examined money laundering activities in that province.

Canada's AML/ATF Regime is also subject to periodic international peer review by the FATF. Canada's last full review was completed in 2016, with the findings of its next mutual evaluation anticipated to be published in 2026.

Enhancing the Regime: Highlighted Actions

The Government of Canada takes financial crimes seriously. Canada's AML/ATF framework is constantly adapted to address new and emerging risks, including those identified through the various reviews of the AML/ATF Regime and the National Risk Assessment process. To this end, measures to enhance the AML/ATF framework have been announced in every federal Budget since 2019, as well as in the 2023 and 2024 *Fall Economic Statements*.

Most recently, recognizing the role of money laundering in supporting and perpetuating cross-border crimes, such as fentanyl trafficking, the government has prioritized measures to tackle these harmful crimes through various initiatives in 2025, including:

- Issuing a **Prime Ministerial Directive on Transnational Crime and Border Security** to provide guidance to federal national security, law enforcement, and intelligence agencies on how to support whole of government efforts to combat the illegal drug trade and the transnational criminal networks that conduct it.

- Announcing $200 million in new capacity to allow Public Safety Canada and the Communication Security Establishment (CSE) to gather intelligence on transnational organized crime and share with North American partners.
- Launching the **Integrated Money Laundering Intelligence Partnership** (IMLIP) to enhance sharing of tactical information between law enforcement and the financial sector to detect, deter, and disrupt sophisticated money laundering networks; and
- Creating a **Joint Operational Intelligence Cell** (JOIC), focusing on transnational organized crime, money laundering, border security, and drug-trafficking, to facilitate the expedient and effective flow of intelligence to support law enforcement operations in Canada and abroad.

More broadly, combatting financial crime requires investments to enhance operational effectiveness to keep pace with increasingly organized and sophisticated criminal activity, as well as ongoing changes to the legislative and regulatory framework to provide effective tools to confront new money laundering and terrorist financing techniques.

In recent years Canada has prioritized investments and policy changes in several key areas, including investments in operational Regime partners, and legislative and regulatory changes to improve corporate transparency, information sharing, and extend or enhance AML/ATF obligations to vulnerable sectors.

Spotlight: Investing in Operational Effectiveness

Since 2018, the government has invested nearly $470 million to strengthen data resources, financial intelligence, information sharing, and investigative capacity to support money laundering and terrorist financing investigations in Canada. This includes:

- $90.6 million over five years, starting in 2018-19, for the CRA to combat additional cases of tax evasion and aggressive tax avoidance;
- $16.9 million over five years, starting in 2019-20, and $1.9 million ongoing, to strengthen operational capacity at FINTRAC to improve oversight of modern financial practices, expand public-private partnerships and increase outreach and examinations in the real estate and casino sectors;
- $78.9 million over five years and $20 million ongoing starting in 2019-20 to the RCMP for enhanced federal policing capacity, including to support the creation of new, dedicated Integrated Money Laundering Investigative Teams in BC, Alberta, Ontario, and Québec, and information technology infrastructure and digital tools to pursue complex financial crimes;
- $16 million over five years for PSPC, starting in 2020-21 to build a team of dedicated forensic accountants in support of money laundering and terrorist financing investigations;
- $28.6 million over four years, beginning in 2020-21, with $10.5 million ongoing, to create the CBSA Trade Fraud and Trade-Based Money Laundering Centre of Expertise to identify and investigate complex trade fraud;
- $89.9 million over five years, starting in 2022-23, and $8.8 million ongoing, for FINTRAC to implement new AML/ATF requirements, enhance expertise, modernize compliance functions, and improve its internal systems;
- $27 million over five years, starting in 2024-25, and $2.3 million ongoing, for FINTRAC to enhance its cyber resiliency and ensure the implementation of additional data security

safeguards over the long-term;

- $1.7 million over two years, starting in 2024-25, to Finance Canada to finalize the design and legal framework for the Canada Financial Crimes Agency; and
- $29.9 million over five years, starting in 2024-25, with $4.2 million ongoing, for CBSA to implement new trade-based money laundering authorities and create a Trade Transparency Unit to better identify illicit financial flows.

Spotlight: Strengthening Canada's Legislative and Regulatory Framework

Parliament amended the *Criminal Code* in 2023-2024 to provide new tools to support investigations and prosecutions. These include a new offence specifically targeted at the laundering of proceeds of crime for the benefit of a criminal organization, and provisions facilitating the prosecution of laundering proceeds of crime by third parties not involved in the associated predicate crimes. *Criminal Code* reforms in 2023-2024 also included provisions to facilitate the search and seizure of digital assets (which can include crypto assets) that are proceeds of crime, and other measures to facilitate investigations, such as a court order requiring a person to keep an account open to assist an investigation and a production order that enables law enforcement to obtain documents or data on multiple specified dates while the order is in effect.

Legislative changes have also been introduced to the PCMLTFA to allow FINTRAC to disclose financial intelligence to additional government organizations when it has reasonable grounds to suspect that the information would be relevant to investigating or prosecuting a money laundering offence, a terrorist activity financing offence, sanctions evasion offence, or threat to the security of Canada. This includes provincial and territorial civil asset forfeiture offices; Immigration, Refugees and Citizenship Canada (IRCC); Environment and Climate Change Canada and Fisheries and Oceans Canada enforcement officers; OSFI; the Competition Bureau; and Revenue Québec, to support efforts relevant to each of these organization's mandates.

Spotlight: Reinforcing Corporate Transparency and Information Sharing

Corporations can be structured to conceal the true ownership of property, businesses, and other valuable assets. With authorities unable to ascertain their true ownership, these corporations can become tools for those seeking to launder money, avoid taxes, or evade sanctions. To address this, Canada has made significant advancements to increase transparency of corporate structures at both the federal and the provincial/territorial levels.

In January 2024, the federal government launched a public, searchable beneficial ownership registry of federal corporations, with access to non-public information for FINTRAC, law enforcement, and other investigative bodies. Additionally, starting for tax years ending after December 30, 2023, trusts must report the identity of their beneficial owners to the CRA.

Corporations Canada, under the *Canada Business Corporations Act*, has the authority to ensure the accuracy of the federal beneficial ownership registry. The Government has introduced regulations to complement these efforts by requiring PCMLTFA regulated entities to flag discrepancies in beneficial ownership information with the federal registry that they observe in their regular course of business directly to Corporations Canada. This obligation will only apply in cases where reporting entities assess there to be a high risk of money laundering and terrorist financing and will come into force in October 2025.

All provinces and territories remain actively engaged in discussions with the federal government through a working group to support the establishment of a pan-Canadian approach to beneficial ownership transparency. Several provinces have already taken concrete action to advance corporate transparency in

their respective jurisdictions:

- In March 2023, Québec launched a beneficial ownership registry covering corporations and legal entities incorporated or registered to do business in the province, which became publicly searchable in March 2024. The non-public information of the registry is accessible to law enforcement and other government agencies to help them fulfill their mandate.
- BC passed legislation to create a public beneficial ownership registry and has established a Land Owner Transparency Registry, which includes information about beneficial owners of land in that province.
- In the 2024 Ontario Economic Outlook and Fiscal Review, Ontario announced that it is also exploring options for a beneficial ownership registry. Ontario 2025 Budget: *A Plan to Protect Ontario* announced its intention to launch public consultations to inform the establishment of a beneficial ownership registry, and other potential measures to empower regulators and law enforcement to fight money laundering and the financing of organized crime.

Private sector information sharing

Canada recognizes that criminals can take advantage of the lack of information sharing abilities between reporting entities to facilitate illicit activities and to evade detection. Legislative amendments came into force in March 2025 to enhance the ability of PCMLTFA reporting entities to share information with each other to better detect and deter money laundering, terrorist financing, and sanctions evasion, while maintaining privacy protections for personal information. Reporting entities that participate in the voluntary framework must establish a Code of Practice that outlines their roles and responsibilities. The framework includes an oversight role for the Office of the Privacy Commissioner under regulations.

Spotlight: Strengthening Canada's Legislative and Regulatory Framework

Since 2020, Canada has introduced amendments to the PCMLTFA and its Regulations to extend obligations to sectors assessed as posing heightened vulnerabilities to money laundering and terrorist financing. This includes armoured car companies; unregulated mortgage lenders; title insurers; payment service providers previously excluded from AML/ATF regulation; crowdfunding platforms; intermediary companies, known as "acquirers," offering cash withdrawal services for white-label ATMs; factoring companies; cheque cashing businesses; and financing and leasing companies.

Given the heightened vulnerabilities posed by MSBs, the government has also strengthened the PCMLTFA registration framework to require domestic MSBs to submit criminal record checks of their chief executive officers, president, directors, and every person who directly or indirectly controls 20% or more of the business upon registration. These requirements address the heighted risk where a criminal actor infiltrates the corporate structure of a MSBs and will come into force on October 1, 2025. The government has also criminalized the operation of an unregistered MSB.

Chapter 3: Assessment of Money Laundering Threats

Overview

Canada is a source, destination, and transit point for proceeds of crime. Billions of dollars are estimated to be laundered in Canada every year, generated by a range of profit-oriented crimes conducted by a variety of threat actors. Threat actors perpetuating profit-oriented crime in Canada range from unsophisticated, criminally inclined individuals, including petty criminals and street gang members, to OCGs and third-party money launderers.

Money Laundering Threat Actors in Canada

Organized Crime Groups

An OCG is a structured group of three or more persons acting in concert with the aim of committing criminal activities to obtain, directly or indirectly, a material benefit, including a financial benefit. OCGs generate billions of dollars of proceeds of crime annually that are laundered through Canada's financial sector and other vulnerable businesses and professions.

According to the CISC 2024 Public Report on Organized Crime, there are more than 4,000 OCGs operating across the country. Of those assessed by CISC, seven OCGs are considered to pose a national high-level threat due to their highly capable and entrenched networks, and involvement in multiple crime areas including money laundering.

Fluid and informal associations between OCGs are increasing, facilitated by advanced technologies, allowing them to more easily expand and diversify their operations. The three most interconnected criminal networks in Canada continue to be outlaw motorcycle gangs, mafia groups, and street gangs. The most influential OCGs in Canada are transnational in scope, with ties to various countries in the Americas, Europe, and Asia. According to CISC, sophisticated OCGs operating in Canada possess the infrastructure and networks to launder large amounts of proceeds of crime across multiple business sectors using diverse methods to evade detection and disruption.

Quick Definitions

What is Money Laundering?

Money laundering is the process used to disguise the source of money or assets derived from criminal activity. There are three commonly recognized (though not necessarily mutually exclusive) stages in the money laundering process:

1) **Placement** involves placing the proceeds of crime in the financial system.
2) **Layering** involves converting the proceeds of crime into another form and creating complex layers of financial transactions to disguise the trail, source, and ownership of funds. This stage may involve transactions such as the buying and selling of stocks, commodities or property.
3) **Integration** involves placing the laundered proceeds back in the economy to create the perception of legitimacy.

The money laundering process is continuous, with new 'dirty' money constantly being introduced into the financial system.

Common Laundering Methods

Money laundering can involve multiple techniques and methods. Notable examples include:

1) **Structuring** (sometimes also referred to as **smurfing**) involves executing financial transactions in specific patterns to avoid reporting thresholds.
2) **Cuckoo smurfing** is a structuring technique where criminals use the accounts of unwitting bank customers to launder their funds.
3) **Money mules** are individuals who, unwittingly or wittingly, transfer or transport funds on behalf of the perpetrator of a crime, or a money launderer.
4) **Nominee** is an individual authorized to conduct transactions on behalf of another person or entity. The use of a (unwitting or witting) nominee is a common method used by criminals to distance themselves from the transactions that could be linked to suspected laundering.
5) **Bulk cash smuggling** involves criminals transferring large sums of physical cash as a step in the money laundering process. These transactions often take place in public areas, with large quantities of cash often carried in suitcases or large backpacks.

Money laundering techniques continue to evolve as criminals adapt to new technology

Quick Definitions

Professional & Third-Party Money Launderers

Large-scale and sophisticated money laundering operations in Canada almost always involve third parties, including professional enablers, who are generally not involved with the commission of the predicate offence(s) that generate the proceeds of crime.[35] They can also involve non-professional third parties, such as nominees and money mules.

Professional money laundering is the provision of money laundering services in exchange for a commission, fee or other benefit. Professional money launderers have the capacity to collect and orchestrate the transfer of illicit financial flows and to engage in complex money laundering schemes on behalf of transnational OCGs, terrorist groups, and other illicit actors. They do this by utilizing global cash pools to settle transactions on behalf of illicit actors in multiple locations at the same time and often cooperate with one another to complete transactions in different markets to support money laundering, sanctions evasion, or the evasion of currency controls.

Professional money launderers may operate within a network that includes money collectors and coordinators, who coordinate cash pick-ups and money mules, and international money controllers, who broker money laundering deals on behalf of transnational criminal clients and other illicit actors. Professional money launderers may have professional credentials, training, infrastructure or other specialized knowledge that makes it easier to co-opt the financial and international trade sectors.

Less sophisticated third parties, such as nominees and money mules, can also be coopted, with or without their knowledge, to participate in complex money laundering schemes. Nominees are individuals, often without a criminal background, who are recruited by or affiliated with criminals to assist in laundering proceeds from illicit activities. Nominees may open bank accounts, acquire real estate, or incorporate businesses in their name, thus masking the true ownership and criminal links to these assets. Nominees may knowingly take part for compensation, be coerced into participation, or be unknowingly involved in such schemes.

OGCs may also rely on individual bulk cash transporters, who take the proceeds derived from smaller illicit

[35] FINTRAC (2023) Updated indicators: Laundering the proceeds of crime through underground banking schemes

transactions, such as drug sales, and amalgamate them into bulk cash for the purpose of handing it off to a professional money launderer. The professional money launderer in turn is responsible for masking the criminal origin of those funds and putting them back into the legitimate economy.

Money mules are individuals who transport proceeds of crime, knowingly or unknowingly, for criminal organizations or money launderers. They play a role in the movement and placement of proceeds of crime into the financial system. Money mules can also act as straw buyers for real estate, vehicles, electronics, and goods involved in trade-based money laundering schemes, and can secure real estate loans and make payments to layer and integrate proceeds of crime. Money mules often include students, unemployed persons, seniors, and migrant workers, and can be recruited through online fraudulent job offers. FINTRAC analysis has shown that money mules may open accounts with forged, falsified or stolen identifying information. In many instances, FINTRAC has observed that the account activity or volume of transactions appears to be inconsistent with the client's apparent financial standing and reported occupation information.

Enforcement Action Spotlight: Project Collecteur

Project Collecteur was a large-scale investigation led by the RCMP's Integrated Proceeds of Crime unit supported by RCMP investigators from Ontario and the CRA that uncovered a sophisticated professional money laundering network providing money transfer services to OCGs using an informal value transfer system (IVTS) with connections to Lebanon, United Arab Emirates, Iran, the US, and China. The funds were then returned to cocaine exporters in Colombia and Mexico. To date, 18 individuals have been arrested, and more than $32 million in assets have been seized or restrained in connection with the investigation.[36]

Enforcement Action Spotlight: Project Carnet

In 2020, the RCMP launched an investigation into a professional money laundering organization from Montreal in response to a tip from the US Drug Enforcement Administration. The investigation resulted in the RCMP laying charges, including for money laundering, against three individuals from Montreal and Laval after uncovering their connections to Colombian criminal organizations. The investigation revealed the laundering of over $18 million in less than a year.[37]

[36] RCMP (2019) Collecteur Project: a vast money laundering network dismantled
[37] RCMP (2022) Project Carnet: three individuals charged in money laundering investigation

Enforcement Action Spotlight: Interprovincial Money Laundering Scheme

In 2024, the RCMP Federal Policing Northwest Region's Federal Financial Crime Team arrested a BC resident following an investigation that revealed a scheme that laundered approximately $47 million in proceeds of crime derived from online illicit cannabis sales between 2018 and 2020.

Officers determined that the money laundering network was comprised of various numbered companies operating as unregistered MSBs. These companies are alleged to have received, transferred or converted proceeds of crime through illicit cannabis sales via a variety of online dispensaries. The BC resident was charged with money laundering, committing an offence for a criminal organization, unauthorized possession of cannabis for the purpose of selling, and failing to register an MSB.

Five other individuals have been charged and convicted for failing to register as an MSB and ordered to forfeit proceeds of crime in connection with the investigation.[38]

Discussion of the Money Laundering Threat Assessment Results

Money laundering threats were assessed using the following criteria:

1. *Level of Actor Sophistication:* the ability demonstrated by threat actors to orchestrate and execute complex money laundering operations.
2. *Complexity of Money Laundering Activity:* the complexity observed or suspected in the money laundering activity related to this type of threat.
3. *Scope of Money Laundering Activity:* the overall breadth of money laundering activity related to this type of threat, including the extent of its geographic reach and the diversity of networks.
4. *Estimated Value of Proceeds of Crime:* the magnitude of the estimated dollar value of the proceeds of crime being generated annually from the profit-oriented crime.

While the dynamics for each assessed threat are unique, the ratings are set out in Table 2.

[38] RCMP (2025) Federal Financial Crime Team charges B.C. resident in connection to $47 million interprovincial money laundering scheme

Table 2
Threat Ratings

High Threat	Involves sophisticated and established threat actors with a broad geographic reach and extensive money laundering networks, either internationally or domestically, as well as significant proceeds of crime (over $1 billion annually). Associated threat actors may exploit vulnerabilities across multiple business sectors; use a range of delivery channels, actors, and obfuscation techniques; and employ complex money laundering methods that involve operations both within and beyond the Canadian borders.
Medium Threat	Involves moderately sophisticated threat actors with money laundering operations concentrated in a few geographic areas, with limited OCG links and/or involving moderate proceeds of crime (between $100 million to $1 billion annually). Associated threat actors typically exploit vulnerabilities in a limited number of business sectors and products and/or use rudimentary techniques.
Low Threat	Involves threat actors with a low level of sophistication and/or involving limited proceeds of crime (under $100 million annually) with limited scale of money laundering operations and geographic reach. Associated threat actors typically exploit vulnerabilities in a limited number of business sectors and products and/or use rudimentary techniques.

This report highlights assessed threats, ranked from "high" to "low". These threats are the most relevant in the Canadian context as they generate or involve the highest proceeds of crime and pose the greatest risk to Canada's security and the safety of Canadians.

Table 3
Overall Money Laundering Threats

High Threat Rating
• Illegal Drug Trafficking • Fraud • Commercial Trade Fraud and TBML • Tax Evasion and Other Tax Crimes
Medium Threat Rating
• Corruption, Bribery, and Collusion • Cross-Border Smuggling • Human Smuggling and Human Trafficking • Illegal Gambling • Ransomware and other types of Extortion • Robbery and Theft (including Auto theft)
Low Threat Rating
• Environmental Crimes • Loan Sharking • Counterfeiting and Piracy (with Currency Counterfeiting as a typology)

High Money Laundering Threats

ML Threat from Illegal Drug Trafficking: Canada continues to grapple with an opioid overdose crisis that is driven by profit-motivated organized crime groups and the illegal fentanyl they sell. These OCGs seek to maximize their profits by incorporating fentanyl and other illegal synthetic opioids into the illegal drug supply because these substances are inexpensive and easy to produce and conceal. [39]

Due to the lucrative nature of the illegal fentanyl market in particular, drug trafficking yields significant proceeds of crime in Canada, incentivizing criminals to perpetuate their activities and fueling other types of criminal activity. Transnational OCGs are the principal players in supplying the domestic market and facilitating the trafficking of drugs to and from Canada. The CISC's 2024 *Public Report on Organized Crime* noted that 93 per cent of assessed OCGs are involved in both manufacturing and distribution of illegal drugs, primarily to serve the domestic market, enabling them to be more self-sufficient. Most OCGs are involved in the trafficking of cocaine, although OCG involvement in fentanyl trafficking has increased by more than 42 per cent since 2019, attributed to the high profits associated with the illicit fentanyl trade.[40]

Canada's Policy Response

The Canadian Drugs and Substances Strategy (CDSS) sets out Canada's response to the illegal drug threat. Renewed in 2023, the CDSS balances both public health and safety priorities. The CDSS encompasses four integrated action areas related to substance use: prevention and education; evidence; substance use services and supports (treatment, harm reduction and recovery); and substance controls.

Through the renewed CDSS and Budget 2023, the Government of Canada has provided $42 million for the RCMP to strengthen intelligence and operational capacity, $6.4 million for PSPC to expand access to forensic accounting services, and $4.6 million to Public Safety Canada to develop an online overdose mapping application.

More recently, **Canada's Border Plan** invests $1.3 billion to strengthen the Canadian border, including to counter the threat of illegal fentanyl production and distribution. These investments support:

- efforts to detect and disrupt the production and trade of illegal fentanyl through enhanced border control, drug profiling capacity, precursor regulatory processes, and expanded law enforcement action;
- additional tools such as chemical detection devices, helicopters, drones, mobile surveillance towers, personnel and additional detector dog teams;
- the appointment of a Commissioner for Canada's Fight against Fentanyl (Fentanyl Czar);
- the development of a new Integrated Money Laundering Intelligence Partnership;
- the listing of several transnational organized crime groups as terrorist entities to provide law enforcement with additional tools to dismantle and disrupt the operations of these organizations; and,
- ensuring round-the-clock surveillance of the Canada-US border.

[39] Public Safety Canada (2025) Illegal Drugs
[40] CISC (2024) Public Report on Organized Crime

OCGs exploit the vulnerability of various economic sectors, including MSBs, banks, and casinos, as well as the vulnerability of different payment products, like cash, prepaid cards, and crypto assets, to launder the proceeds from illegal drug sales. Although the use of cash remains prevalent in the laundering of drug trafficking proceeds, the use of crypto assets to illegally procure drugs and precursor chemicals via dark web and surface web sources has become more common, presenting new challenges for law enforcement.

OCGs active in illegal drug trafficking employ a wide range of money laundering methods, including blending illicit funds with legitimate business revenues, funneling illicit funds through shell companies, bulk cash smuggling, trade-based money laundering, investing in real estate to legitimize financial transactions, and cyber-enabled money laundering using online financial technology platforms. Sophisticated drug traffickers establish complex business structures involving multiple nominees, various addresses, and concealed beneficial ownership of assets. The businesses may also receive services from accountants and lawyers, who possess knowledge and skills that may be exploited by criminal actors.

Virtually every large-scale transnational OCG uses third-party money launderers to launder the proceeds of illegal drug sales. These third-party money launderers may hold various occupations; however, they are often owners or associates of trading companies or MSBs, who use their occupation and knowledge, the infrastructure associated with their line of work, and their networks to facilitate money laundering, providing a veneer of legitimacy to criminal organizations. Major, often transnational, drug trafficking organizations appear to exploit IVTS[41] which offer security, anonymity, and versatility that can be susceptible to misuse.

[41] See Table 6 in Chapter 4: Assessment of Terrorist Financing Threats for more information on IVTS

Public-Private Collaboration: Project Guardian

Project Guardian, launched in 2018, is a public-private partnership led by the Canadian Imperial Bank of Commerce (CIBC) and supported by Canadian law enforcement agencies, international partners and FINTRAC to combat the trafficking of illegal fentanyl.[42]

Tracing the movement of funds related to the trafficking of illegal fentanyl is a priority for FINTRAC. Through a strategic analysis of its financial intelligence, and in collaboration with Canada's financial institutions and the RCMP, FINTRAC released an operational alert on money laundering indicators related to this illicit activity in 2025.[43] In 2023-24, FINTRAC disclosed 93 suspicious transaction reports on 354 different subjects to law enforcement.

Public-Private Collaboration: Project Legion

Project Legion is a public-private partnership led by Toronto-Dominion Bank (TD), supported by Canadian law enforcement agencies and FINTRAC. Project Legion targets illicit cannabis activities by focusing on the money laundering aspect of the crime. [44] The illicit cannabis market results in a significant loss of tax revenue and helps fund other illegal and harmful activities by OCGs in communities across the country.

In 2023-24, FINTRAC produced over 60 financial intelligence disclosures in support of law enforcement investigations involving illicit cannabis activities at the municipal, provincial, and federal levels.

Enforcement Action Spotlight: Project Doom

In October 2023, the RCMP Manitoba Organized Crime Unit recognized FINTRAC's contribution to Project Doom, an investigation into suspicious activity in Winnipeg casinos. Through the investigation, it was determined that an individual from Winnipeg was supplying illegal drugs to remote First Nation communities. The cash proceeds of these illegal drug sales were then used at casinos to hide the connection to criminal activity. An individual was charged with trafficking fentanyl and cocaine, money laundering, and possession of proceeds of crime. Police also seized 498 grams of crack cocaine, 882 counterfeit OxyContin tablets (fentanyl), 241 Percocet tablets, and 26 gabapentin tablets.[45]

[42] FINTRAC (accessed 2025) Project Guardian
[43] FINTRAC (2025) Operational Alert: Laundering the proceeds of illicit synthetic opioids
[44] FINTRAC (2022) Operational alert: Laundering of proceeds from illicit cannabis
[45] RCMP (2023) RCMP Manitoba Organized Crime Unit lay money laundering charge in Project Doom

Enforcement Action Spotlight: Project Carlos

In August 2023, the Alberta Law Enforcement Response Teams acknowledged FINTRAC's financial intelligence contribution to Project Carlos, which led to the arrest of seven individuals for their role in a multi-million-dollar drug trafficking operation. A total of 33 charges were laid with offences ranging from drug trafficking to money laundering, to criminal conspiracy and organized crime-related offences. Project Carlos resulted in the seizure of more than $4.5 million worth of drugs, including fentanyl, and nearly $1 million in cash.[46]

Enforcement Action Spotlight: Online Illicit Cannabis

In January 2024, the Sûreté du Québec acknowledged FINTRAC's contribution to an investigation that led to the dismantling of a network of producers and traffickers who were illegally selling cannabis online. More than 70,000 transactions, totaling $15 million, were allegedly carried out by traffickers linked to organized crime. Ten people were charged with money laundering and the production, possession, trafficking and sale of illicit cannabis.[47]

Enforcement Action Spotlight: Project Odeon

In August 2023, the Hamilton Police Service dismantled a significant clandestine producer of fentanyl and other synthetic drugs in the Greater Hamilton and Toronto Area. Following a lengthy investigation, 48 criminal charges were laid against 12 people, including possession for the purpose of trafficking, production of a controlled substance, proceeds of crime and firearm possession. Police also seized an operational fentanyl drug lab, more than 64 kilograms of drugs, including 25.6 kilograms of fentanyl, 18 kilograms of methamphetamine, and 6 kilograms of ketamine, well as $350,000 of proceeds of crime, including cars, jewellery, and cash.[48]

Enforcement Action Spotlight: CRA Illicit Income Audit Program

Following the withdrawal of charges in relation to an investigation into alleged importation and trafficking of drugs in which over $3 million in suspected proceeds of crime, including cash and luxury items, were seized, the CRA Illicit Audit Income Program conducted audits on three taxpayers and implicated corporations. Through these audits, the CRA established a total debt of $5.73 million, including penalties and interest, for tax years ranging from 2017 to 2022. Following three federal court orders, the CRA has intercepted $815,000 of the seized cash, helping to prevent these proceeds from being reinvested in illicit activities.

[46] ALERT (2022) Multi-million-dollar drug bust in Calgary; ALERT (2023) Update: Charges laid in Project Carlos
[47] FINTRAC (2024) FINTRAC Annual Report 2023-2024
[48] Hamilton Police Service (2023) Project Odeon Dismantles Significant Illegal Opioid Producers

ML Threat from Fraud: Fraud involves dishonest conduct with the intention to deprive victims of money, property, or information. Reported losses from fraud are increasing year over year, with the Canadian Anti-Fraud Centre (CAFC) reporting $638 million in losses in 2024.[49] Official reported losses are believed to be vast underestimations, with only 5 to 10 per cent of victims believed to report incidents of fraud.[50] It is estimated that significant proceeds of crime are generated through fraud in Canada annually. Fraud inflicts detrimental consequences on victims that exceed the evident financial losses. Many victims report emotional and psychological distress stemming from feelings of shame, embarrassment, and anxiety. Victims may also experience social isolation due to strained relationships resulting from fraud incidents.

Schemes employed by fraudsters are often reflective of broader societal trends and current events. From March 2020 to January 2022, the CAFC recorded 32,476 reports of COVID-19-related fraud, totaling a loss of $8.53 million. As pandemic-related fraud declined in 2022, it was replaced by fraud schemes related to other topical events, such as the ongoing conflict between Russia and Ukraine, Hurricane Fiona relief efforts, the July 8, 2022 national outage on Rogers telecom network, fake investments in crypto assets, and others.

Canada's Policy Response

The Canadian Anti-Fraud Centre (CAFC)

The CAFC is the central repository for fraud information and intelligence in Canada, and is jointly operated by the RCMP, the Ontario Provincial Police (OPP), and the Competition Bureau of Canada. As a National Police Service stewarded by the RCMP, the CAFC offers support to all law enforcement agencies across Canada. CAFC core responsibilities include:

- *Prevention:* serving as the primary national source for fraud and identity crime material and education.
- *Disruption:* working with partners, including financial institutions, credit card companies, telecommunications, and Internet providers to disrupt fraud and prevent financial losses.
- *Intelligence:* producing and sharing timely, accurate, and useful fraud-related intelligence and information to educate and assist citizens, businesses, law enforcement, and government institutions in Canada and around the world.
- *Support:* providing direct support to victims of fraud through its Call Centre and Senior Support Unit.
- *Partnerships:* maintaining strong partnerships with the private sector and law enforcement to prevent fraud and assist in investigations.

Most large-scale fraud schemes in Canada are perpetrated by sophisticated criminals, particularly those that are technologically skilled. The high prevalence of social media use, rapid advancement and adoption of crypto assets, DeFi, and AI are enabling criminals to conduct fraud on a broader and faster transnational scale.[51] The Canadian Centre for Cyber Security assesses that fraud and scams are the most common forms of cybercrime impacting Canadians.[52]

[49] RCMP (2024) Fraud Prevention Month 2024: Fighting fraud in the digital era
[50] RCMP (2023) Canadian Anti-Fraud Centre Annual Report 2022
[51] RCMP (2023) Canadian Anti-Fraud Centre Annual Report 2022
[52] Canadian Centre for Cyber Security (2024), National Cyber Threat Assessment 2025-2026

Fraud is associated with multiple money laundering techniques and the exploitation of several business sectors. RCMP analysis has noted that this includes transferring funds to the benefit of a registered company (potentially a shell company) followed by an immediate outbound transfer of funds to unrelated third parties and/or corporate entities in multiple jurisdictions, victims willingly transferring funds, and accounts compromised by fraud actors. Once assets in any fraud are moved outside of the Canadian financial sector, it becomes more difficult to retrieve them, and less necessary for these actors to employ sophisticated money laundering techniques. The successful laundering of proceeds obtained from fraud victims further perpetuates this type of crime and enables criminals to reinvest in advanced technologies and expand their operational capabilities.

Within the broad area of fraud there are several crime sub-types of concern. Table 4 lists fraud sub-types of concern, and summarizes associated money laundering dynamics, and OCG involvement.

Table 4
Common Fraud Types and Money Laundering Dynamics

Mass Marketing Fraud *A type of fraud that uses mass-communication methods – such as telephones, the internet/email, postal mail, television, radio, or personal contact – to solicit and defraud prospective victims.[53] Mass marketing fraud may involve other fraud types discussed in this table (e.g. romance, investment fraud).*	Mass marketing fraud often involves the impersonation of authority figures in the banking, mortgage, legal, crypto assets, and traditional investment industries. While some Canada-based OCGs are involved, foreign actors, sometimes using Canadian associates for payment forwarding, are large players in this activity. Organized foreign-based operations (e.g. scam call centres in Southeast Asia) are growing in popularity.[54] The RCMP has observed proceeds of crime being sent to several markets, including Southeast Asia, the Caribbean, South America, Europe, West Africa, and Oceania. Foreign actors are known to use a range of money laundering methods and techniques, including smurfing, structuring, the use of nominees and money mules, shell and front companies, MSBs (including IVTS), and illicit underground banking systems.
Investment Fraud *A type of fraud (often committed as part of mass marketing fraud operations) which seeks to bait a potential victim with promises of low to no risk investments with high returns that are ultimately non-existent. It can include investments related to real estate and crypto assets, as well as Ponzi and pyramid schemes.*	Investment frauds were one of the top three frauds with the highest levels of reported victim losses in 2023. Approximately 60 per cent of the $310 million reported to the CAFC was tied to crypto asset investment frauds. RCMP analysis has noted that individuals engaging in this activity demonstrate the capability to exploit a variety of business sectors and employ various methods to launder the proceeds of fraud, including the use of crypto assets, high-risk foreign jurisdictions with weak AML/ATF regulations, shell/front companies, and electronic funds transfers inside/outside of Canada. Transactional activity related to proceeds of fraud may also involve structured or smurfed deposits, nominees, and money mules.
Capital Markets Fraud *A type of investment fraud related to the capital markets (stock exchanges, options exchanges, etc.), both domestically and internationally. It includes related misconduct, such as prohibited insider trading, false prospectus, fraud affecting the public market, fraudulent manipulation of stock exchanges, and fraudulent manipulation of stock exchange transactions.*	Capital markets fraud is a highly sophisticated crime. Perpetrators leverage the financial services industry, primarily the banking sector in Canada and abroad, to launder proceeds of crime. Professional money launderers have been observed facilitating the movement of funds. The extent of Canadian OCG involvement in this area is not fully known. Wire transfers, deposits of letters of credit, and bank drafts are common methods to launder proceeds of crime through the banking sector. Additionally, funds transfers to the benefit of a public company followed by an immediate outbound transfer of funds to unrelated third parties and/or corporate entities in multiple jurisdictions have also been observed.
Romance Fraud *A type of fraud (often committed as part of mass marketing fraud operations) where perpetrators express false romantic intentions in order to access a victim's cash, bank accounts, or credit cards.*	Romance fraud schemes often operate from foreign jurisdictions targeting Canadians. According to RCMP data, the laundering of proceeds of romance fraud largely resembles that of other types of mass marketing fraud. Romance fraud victims can also be used as unwitting money mules to launder money, usually acquired from another victim or criminal activity. More than $58 million was reported to the CAFC as lost due to romance frauds in 2024.

[53] US Department of Justice Criminal Division (2023) Criminal Division | Mass Marketing Fraud; Edmonton Police (Accessed 2025) Mass Market
[54] United Nations Office on Drugs and Crime (Accessed 2025) Crushing scam farms, Southeast Asia's 'criminal service providers'

Mortgage Fraud *The deliberate misrepresentation of information to obtain mortgage financing that would otherwise not be granted.*	Mortgage fraud is associated with sophisticated OCGs and predominantly associated with the integration stage of money laundering. Criminals may create fraudulent loan applications and leverage third-party actors, such as straw buyers or shell companies, to obscure and distance themselves from the real estate transaction.[55] Once the loan is approved and funds are advanced, criminals may then pass off illicit funds as legitimate. Mortgage fraud has also been observed to facilitate further organized criminal activity, such as illicit drug production and distribution, or running a bawdy house. OCGs involved in mortgage fraud, and subsequent laundering through real estate, are primarily concentrated in BC and Alberta. OCGs involved in real estate fraud target large Canadian banks, real estate investors, homeowners, or renters.[56]
Identity Fraud *The use of falsified or stolen personal information, often for criminal purposes.*	Identity fraud is associated with sophisticated OCGs, particularly those with access to highly skilled technological abilities. The RCMP has observed that identity fraud often involves unauthorized remote access to financial accounts, resulting in the movement of securities and/or funds out of victims' accounts. These platforms have often implemented several layers of security features and can include the direct deposit banking information of the victims. Identity fraud actors display a sophisticated knowledge and capability of redirecting funds using the formal banking system to accounts under their control and to gain access to those funds generated from fraud. Furthermore, fraud actors often conduct scams remotely across multiple international and domestic jurisdictions, using technology to avoid detection by law enforcement.[57] The CAFC received 9,487 reported instances of identity fraud in 2024.[58]
Payment Card Fraud *A type of fraud that occurs when a credit or debit card, or its associated payment information, is stolen and used to make purchases or withdraw funds.*	OCGs remain involved in payment card fraud. Groups active in this threat activity are also known to be involved in other criminal markets and may use the proceeds from payment card fraud to finance other criminal activities. These groups are primarily based in Ontario and BC but have the potential to commit payment card fraud outside of their respective jurisdictions. Multiple sectors are suspected to be used to launder payment card-related proceeds, including financial institutions, MSBs, and online or brick-and-mortar casinos, through multiple methods, including use of crypto assets, structured bank deposits, smurfing, front companies, and the use of nominees and money mules. Prepaid payment products are attractive for laundering funds involved in fraud due to their ease of use and wide acceptance.[59]

[55] FINTRAC (2024) Operational alert: Laundering the proceeds of tax evasion in real estate
[56] CISC (2020) National Criminal Intelligence Estimate on the Canadian Criminal Marketplace: Money Laundering and Fraud
[57] CAFC (2024) Bulletin: New technology
[58] CAFC (2025) Fraud Prevention Month 2025
[59] CISC (2020). National Criminal Intelligence Estimate on the Canadian Criminal Marketplace: Money Laundering and Fraud

Public-Private Collaboration: Project Chameleon

Launched in June 2017, Project Chameleon is a public-private partnership under the leadership of HSBC Canada[60] that focuses on the laundering of criminal proceeds derived from romance fraud and emergency grandparent scams. It has mobilized businesses, FINTRAC, and law enforcement to identify illicit activity and report suspicious transactions, with a goal of protecting victims and their money. In consultation with the CAFC, FINTRAC published an Operational Alert on laundering the proceeds of romance fraud in 2019.[61]

Enforcement Action Spotlight: Project Déjà Vu

In 2024, the Toronto Police Service made 12 arrests and laid 102 charges in a major identity fraud investigation titled Project Déjà Vu. The investigation began in 2022 following a report from a financial institution that had identified several synthetic accounts that had been opened. The investigation revealed a scheme where the perpetrators allegedly created more than 680 unique synthetic identities and leveraged them to open hundreds of bank and credit accounts at financial institutions across Ontario.

The scheme resulted in losses of approximately $4 million. Police recovered several dozen synthetic identity documents, hundreds of payment cards, and seized approximately $300,000 in Canadian and foreign cash as proceeds of crime. The Toronto Police Service was supported in their investigation by the Halton, Peel, and Waterloo Regional Police Services, CRA, and FINTRAC. In general, accounts obtained under synthetic identities are known to facilitate other serious criminal offences, including the laundering of proceeds derived from human trafficking, drug trafficking, and armed robbery among, other serious crimes.[62]

Enforcement Action Spotlight: Project Atlas

In 2024, the OPP launched Project Atlas, an initiative to combat global cryptocurrency investment fraud affecting people worldwide, including in Ontario. The project focuses on disrupting organized fraud, supporting victims in the recovery of stolen funds and educating the public about cryptocurrency investment scams. As part of the initiative, OPP investigators may proactively reach out to individuals who have sustained losses to support cryptocurrency recovery efforts for the victims and/or to support the prosecution of offenders.

As of November 2024, the initiative has helped prevent more than $70 million in cryptocurrency from being stolen by cybercriminals and frozen over $24 million in fraudulent losses. Working with law enforcement partners around the globe, investigators have identified over 2,000 cryptocurrency wallet addresses linked to fraud victims across 14 countries, including Canada, the US, Australia, Germany, and the United Kingdom.[63]

[60] In March 2024, HSBC Canada was acquired by the Royal Bank of Canada (RBC)
[61] FINTRAC (2019) Operational alert: Laundering of the proceeds of romance fraud
[62] Toronto Police Service (2024) Arrests in Synthetic Identity Fraud
[63] Ontario Provincial Police (2024) Project ATLAS; Ontario Provincial Police (2024) Project ATLAS Overview

ML Threat from Commercial (Trade) Fraud and Trade-Based Money Laundering: Commercial trade fraud involves the intentional misrepresentation of trade and customs-related information. Trade fraud involving the international trade in goods is a designated offence for money laundering and terrorist financing in Canada when the fraud results in a loss of revenue for the Government of Canada (duties and taxes). Trade fraud with a nexus to Canada is carried out through various mechanisms, including mis-invoicing, misdescription of goods, and the use of phantom shipments.

Trade-based money laundering is the process of disguising proceeds of crime from a variety of predicate offences and moving value through trade transactions to legitimize their illicit origin. Trade-based money laundering leverages trade fraud as a primary method to move value with complicit sellers and buyers in different jurisdictions using a variety of techniques to misrepresent the price, value, quantity, or quality of imports or exports.

Table 5
Customs trade fraud techniques

Misdescription of Goods	Incorrectly declaring the type of good or its quality creates a discrepancy between the value of the good declared and what is actually shipped.
Multiple Invoicing	By providing multiple invoices or declarations for the same goods the seller can justify multiple payments for a single shipment either through the same or multiple financial institutions.
Over- and under-valuation	Goods are invoiced and/or declared to customs services above or below their true value. Undervaluing goods allows buyers to gain excess value once a payment is made. Similarly, overvaluing a good allows the seller to gain the excess value upon payment for the goods in question.
Over- and under-shipment	Inflating the true quantity of goods shipped on customs declarations allows the buyer to remit excess value to the seller, while reducing the true quantity of goods shipped on customs declarations allows the seller to remit excess value to the buyer.
Phantom Shipments	Involves the submission and processing of customs and shipping documents and corresponding payments without the shipment of any actual goods.
Financial Phantom Shipments	Involves the payment for goods without making declarations to customs services and without shipping any actual goods.

Significant illicit proceeds are estimated to be laundered through commercial trade fraud and trade-based money laundering in Canada on an annual basis. It is estimated that approximately 80 per cent of the movement of illicit financial flows globally is done through mis-invoicing in trade-based money laundering schemes.[64] The FATF has noted that "open account transactions", an international sale in which the goods are shipped and delivered before payment is due and which are used in around 80 per cent of international trade, are particularly susceptible to trade-based money laundering schemes.[65]

[64] Global Financial Integrity (2021) Trade-Related Illicit Financial Flows in 134 Developing Countries 2009-2018
[65] FATF (2020) Trade-Based Money Laundering: Trends and Developments

Canada's Policy Response

The Trade Fraud and Trade-Based Money Laundering Centre of Expertise

In April 2020, the government created the Trade Fraud and Trade-Based Money Laundering Centre of Expertise ("the Centre of Expertise") within the CBSA. The Centre of Expertise identifies suspected non-compliant customs transactions and produces intelligence that CBSA officers can use to confirm non-compliance and take appropriate action. This can include seizing goods and issuing monetary penalties under customs law, or referring the most serious forms of trade fraud, such as trade-based money laundering, for both customs and criminal investigations.

This work was expanded in 2024 through the creation of the Border Financial Crime Centre as a new division within the CBSA. The new division includes the existing Centre of Expertise in addition to two new capabilities announced in the *Fall Economic Statement* 2023 and Budget 2024 – the development of a Trade Transparency Unit and new cadre of Regulatory Investigators. These Regulatory Investigators will enable CBSA's new authorities under the new PCMLTFA Part 2.1 (Reporting of Goods), which came into force in April 2025 and expands the CBSA's mandate beyond customs concerns to enforce the compliance of goods flows to and from Canada for AML/ATF purposes.

Trade-based money laundering schemes can range in complexity and sophistication, as criminals can abuse any commodity, including those for which a high rate of duty applies. Simple schemes often conceal illicit value through the purchase and onward sale of difficult to value goods, such as art and antiquities, or sought after goods, such as vehicles and luxury products. Conversely, highly complex schemes often integrate professional money laundering techniques, including the use of shell, shelf or front companies, complex and/or opaque financial products, such as trusts, and goods trading methods, such as transit via free trade zones.

Both OCGs and terrorist actors are known to rely on trade-based money laundering techniques, typically facilitated through professional money laundering networks, notably international money controllers. International money controllers are transnational professional money launderers who specialize in moving value through formal and informal means globally on behalf of OCGs and have been particularly prolific in carrying out trade-based money laundering schemes. Their knowledge, expertise and global reach enable them to manipulate multiple trade chains, customs processes and financing mechanisms, often operating under the front or cover of a seemingly legitimate company.

***ML Threat from Tax Evasion and other Tax Crimes*:** Tax evasion is the intentional non-compliance with Canada's tax laws through various actions, such as falsifying or altering records and claims, omitting to enter material in a record book of accounts, hiding income, or inflating expenses. Other tax crimes can include the deliberate understatement of income, and/or the claiming of a false refund, rebate, or benefits. Proceeds generated from tax evasion and other tax crimes are considered proceeds of crime, and thus frequently intersect with money laundering as criminals employ money laundering techniques to conceal the true source of funds.[66] Tax evasion and other tax crimes have serious consequences as they lower government revenue and undermine public trust in Canada's tax system.

[66] FINTRAC (2024) Operational alert: Laundering the proceeds of tax evasion in real estate

The CRA has estimated the potential tax revenue loss resulting from tax non-compliance and this is reflected in the tax gap. The tax gap is estimated in the billions of dollars annually,[67] and is the result of both intentional and unintentional actions. Furthermore, the underground economy, which is closely related to tax evasion, is estimated to be in excess of $72 billion[68] in 2023, or 2.5% of total GDP. It includes economic activities, whether legal or illegal, that are unreported, resulting in failure to comply with tax laws. Based on these estimates, the proceeds of crime from tax evasion or other tax crime is likely to be significant.

Tax evasion is often conducted by specialized criminals, including OCGs, who may also orchestrate other tax crime schemes (e.g., claiming fraudulent duty or tax refunds). RCMP has observed that OCGs involved in tax evasion are highly structured and often launder illicit proceeds through offshore companies and accounts. They have also been linked to large money laundering networks, leveraging the global financial system to hide income and assets. For example, Project Collecteur uncovered a money laundering scheme with ramifications in several countries using an MSB and false invoices. Four taxpayers were found guilty of tax evasion as part of this case.[69]

Approximately 900 Canadian individuals, companies, and trusts were identified in the 2016 Panama Papers leak. Although the presence of a person's name on this list does not necessarily imply non-compliance with Canadian tax law, this is an indicator that complex offshore corporate structures, financial products and services continue to be used to shift profits to low-tax countries and move funds to accounts that are undeclared to tax authorities for tax avoidance and tax evasion purposes.[70] In addition, opaque corporate registries in Canada have historically enabled unscrupulous foreign investors to evade taxes on income via corporate vehicles.

Tax crime methods have evolved in recent years. The launch of Canada's COVID-19 emergency benefits and subsidies in 2020 was followed by an increase in cyber-attacks, identity thefts, and frauds against taxpayers.[71] The extent of the COVID-19 emergency benefit program translated into a significant rise in cases where unauthorized individuals accessed CRA taxpayer accounts, changed taxpayer addresses or direct deposit numbers for the purpose of claiming a benefit on behalf of a legitimate taxpayer and redirecting payments to another address or bank account associated with the unauthorized individual. The CRA has implemented numerous security measures, technologies, processes and controls to ensure the security of taxpayer information to combat these threats.[72]

[67] CRA (2023) Overall federal tax gap report
[68] Statistics Canada (2025) The underground economy in Canada, 2023
[69] CRA (2024) Collecteur Project: Laval intermediary convicted of conspiring to commit tax evasion and money laundering
[70] CRA (2024) How we combat tax evasion and avoidance
[71] RCMP (2020) COVID-19 Related Fraud
[72] CRA (2025) Security measures to protect taxpayer information from external threats; CRA (2025) Security of Taxpayer Information

Canada's Policy Response

CRA Criminal Investigations

The CRA targets promoters of sophisticated tax schemes and investigates significant cases of tax evasion with an international element. The CRA also places priority on:

- Joint investigations with other enforcement agencies, including cases of tax evasion involving money laundering;
- Significant cases involving income tax and/or GST/HST tax evasion, including the underground economy; and
- Significant tax offences targeting benefits, credits, and false refunds.

The threat of money laundering exists in all tax crime cases. The CRA pursues the money laundering aspects of a case for criminal prosecution on a case-by-case basis.

Some providers of tax-related advice – including accountants, lawyers, and financial advisors – can be used, unwittingly or wittingly, by bad actors seeking to avoid or evade taxes or obtain fraudulent refunds using a variety of different techniques. Canada's real estate sector is also a notable mechanism used by criminals to facilitate tax evasion and money laundering. Professionals in the real estate sector can unwittingly or wittingly facilitate tax evasion and money laundering through actions that manipulate the price of a given property, or the use nominees, false identities, corporations, or trusts to hide the identity of the ultimate beneficial owners.[73]

Enforcement Action Spotlight: Tax Evasion Scheme and Laundering Proceeds

A CRA investigation revealed that a resident of Ottawa, Ontario, used their spouse to transfer unreported income from "private contracts". For the years 2008 to 2012, the accused reported income from their dentistry practice on individual tax returns, but then wrongfully deducted the entire amount as a business expense, thereby evading federal tax of over $500,000. The accused pleaded guilty to one count each of tax fraud and laundering proceeds of crime under the *Criminal Code* and was sentenced in 2019 to a conditional jail sentence of two years less a day. This marks the first time in Canada that the *Criminal Code* money laundering provisions have been successfully applied to a tax evasion conviction.

Medium Money Laundering Threats

***ML Threat from Illegal Gambling*:** Under the *Criminal Code*, all forms of gaming and betting (gambling) are prohibited, and various criminal offences may apply depending on the specific activity. Legal gaming and betting activities must fall within one or more of the *Criminal Code* exemptions, such as lottery schemes conducted and managed by a province; betting on horse-racing as regulated by the Canadian Pari-Mutuel Agency; or through other exemptions, such as for private bets between individuals who are not engaged in any way in the business of betting. This general prohibition includes online casinos and sports betting operations. Illegal gambling operators undermine the economic and tax contributions of the legal gaming industry and can expose customers to heightened risk.

[73] FINTRAC (2024) Operational alert: Laundering the proceeds of tax evasion in real estate

Based on the estimated size of the Canadian gambling sector, its importance to organized crime, and the scale of seizures from past enforcement actions, the scale of illegal gambling in Canada is estimated to generate significant proceeds of crime annually. Organized crime is the primary provider of illegal gambling in Canada, mainly through illegal gaming houses. In 2023, the CISC assessed that 39 OCGs active in Canada are involved in illegal gambling schemes. Although the market for illegal gambling in Canada is small, it is highly profitable.

Illegal gambling can both generate proceeds of crime and be used to launder proceeds of crime. Proceeds of crime are typically sourced from various predicate offences, including drug trafficking, human trafficking, and arms trafficking. High betting limits of $20,000 per hand for certain games allows for money to be laundered quickly in high volumes. Illegal gambling den profits are laundered through numbered companies, real estate, and invested into further criminal activity.[74] Illegal gambling operators have also demonstrated their ability to exploit financial entities and MSBs, including payment service providers, to launder proceeds of crime through licensed and unlicensed gambling sites hosted domestically and internationally. [75]

There are also money laundering risks associated with online betting sites known as "sportsbooks" operated by OCGs in Canada. Online sportsbooks have been observed to include complex management structures to insulate those at the top of the organization. Sportsbook betting is done by cash transferred directly from bettor to agent, and the origins and flows of this cash are not traceable. The impact of legal online sports betting in Canada on the illicit sports betting market has not been fully assessed at the time of writing.

Enforcement Action Spotlight: Illegal Gambling

In early 2022, the Combined Forces Special Enforcement Unit of BC's Joint Illegal Gaming Investigation Team started an investigation into a café after receiving reports of illegal gaming activity. In July 2023, the Joint Illegal Gaming Investigation Team arrested 11 individuals and seized multiple items in connection with this investigation, including video lottery terminals, cell phones, and approximately $14,000 in cash.[76]

ML Threat from Corruption (including Bribery and Collusion): Corruption in Canada varies in scope and scale, and in the nature of the activity. It can include small-scale bribe-paying activity to obtain an advantage or benefit, misappropriation by an official of government property for personal ends, and large-scale bribery or collusion schemes aimed at illegally obtaining lucrative public contracts. Attempts to disguise or facilitate corrupt payments or proceeds may in themselves leverage money laundering techniques.[77] In addition to corrupt activities carried out domestically, some Canadian companies have been implicated in paying bribes to foreign officials to advance their company's business interests.[78] While certain schemes may not constitute corruption, they may involve a fraud in a procurement process and generate inflated revenues.

[74] Global News (2020) Suspects in alleged Markham illegal casino mansion linked to B.C. casino suspects
[75] FINTRAC (2024) Special Bulletin on laundering the proceeds of crime through online gambling sites
[76] Combined Forces Special Enforcement Unit of BC (2025) Two People Charged for Keeping an Illegal Gaming House
[77] FATF (2012) Specific Risk Factors in Laundering the Proceeds of Corruption: Assistance to Reporting Institutions
[78] Government of Canada (2024) Canada's Fight against Foreign Bribery - twenty-fifth Annual Report to Parliament

Corruption and the laundering of proceeds generated from such crimes have severe economic and social consequences for Canada and Canadians. Corruption erodes trust in institutions, fosters unfair competition, and often leads to the diversion of public resources away from essential services or investments that promote sustainable development and long-term prosperity.

Corruption cases can be complex, involving multiple actors including public officials at all levels, and/or contractors. Actors can be part of complicated and highly structured networks that are capable of layering and obscuring the sources of illegal funds, including through association with seemingly credible and established companies. Such transactions may be hidden as legitimate transfers, and as such, investigations may be unable to appropriately trace funds moving quickly or through opaque structures. Advances in technology, such as encrypted messaging apps and disappearing messages, continue to help facilitate corruption and collusion schemes.

The CISC assesses that a relatively small share of OCGs are involved in corruption and bribery and associated money laundering activities within Canada. Transparency International's Corruption Perception 2024 Index also ranks Canada 15th of 180 in terms of least corrupt countries ahead of most of its peers and second highest in the G7.[79]

Canada's Policy Response

Politically Exposed Persons and Heads of International Organizations

Politically exposed persons (PEPs) and heads of international organizations (HIOs) hold positions at risk for money laundering and terrorist financing. PEPs and HIOs may be exploited by criminals – who use their status and power to carry out money laundering or terrorist financing – or may be criminals themselves who seek to employ their networks and resources to launder proceeds from their crimes, such as bribery or corruption. Family members and close associates of PEPs and HIOs are also potential targets, as they can more easily avoid detection.

While Canadian officials are not immune to bribery and corruption, the Cullen Commission noted the greater risk to Canada stems from foreign corrupt officials who attempt to safeguard the proceeds of their unlawful activities by transferring them to Canada. Sectors of the economy considered most vulnerable to abuse by PEPs and HIOs for money laundering include real estate, banking, casinos, company service providers, and the legal profession.

[79] Transparency International (2024) Corruption Perception Index

Enforcement Action Spotlight: Project "Assistance"

The RCMP Sensitive and International Investigations Unit in Ottawa, successfully investigated SNC-Lavalin and its subsidiaries as part of Project "Assistance" for providing over $47 million to foreign public officials to obtain contracts in Libya. In 2020, one of the SNC-Lavalin executives was sentenced to 8 years and 6 months imprisonment for fraud, corruption of a foreign public official, laundering proceeds of crime, and two counts of possession of proceeds of crime in the Québec Superior Court.

The Court ordered the forfeiture of the executive's assets, which are worth over $4 million related to the conviction. The executive was also fined $24.6 million in lieu of the seizure of additional proceeds of crime.

SNC-Lavalin as a company was also fined $280 million and issued a three-year probation order, with conditions that cause the group to maintain, and as required, further strengthen its compliance program, record keeping, and internal control standards and procedures.[80]

ML Threat from Cross-Border Smuggling of Illicit Tobacco and Firearms: Canada continues to see cross-border smuggling of illicit tobacco and firearms. Illicit tobacco (also referred to as contraband tobacco) refers to any tobacco product, including raw tobacco, that does not comply with Canada's tobacco regulations regarding importations, manufacturing, distribution, and taxation. Contraband tobacco undermines the government's efforts to reduce smoking rates, generates profits that fuel other criminal activity, and results in loss of tax revenue.

The illicit tobacco market in Canada includes counterfeit cigarettes imported from overseas; illegal cigarettes manufactured in Canada and the US on Indigenous reserves and sold in Canada; cigarettes produced legally in Canada, the US, or abroad, and sold tax-free to non-Indigenous people; and "fine cut" tobacco imported illegally, mostly by Canadian-based manufacturers. The largest quantity of illicit tobacco found in Canada continues to originate from the manufacturing operations based on Indigenous reserves that straddle Québec, Ontario, and New York state.

[80] RCMP (2020) More than $4 million seized following an RCMP corruption investigation; Global Affairs Canada (2020): Canada's Fight against Foreign Bribery

Enforcement Action Spotlight: Contraband Tobacco Seizure

In 2024, CBSA criminal investigators launched an investigation into a cigarette smuggling operation after CBSA officers intercepted numerous contraband cigarette shipments at Vancouver International Airport Commercial Operations and the Vancouver International Mail Centre. Following an investigation, in November 2024, CBSA criminal investigators executed a search warrant at a Vancouver residence. The following items were seized:

- 3,826 cartons of contraband cigarettes;
- 4.2 kilograms of illegal cannabis; and
- $51,915 in cash and casino chips.

CBSA officers arrested a 34-year-old Vancouver resident for their suspected involvement in the cigarette smuggling operation. The investigation is ongoing.

Financial intelligence has confirmed that OCGs active in the illicit tobacco smuggling and trafficking trade have the sophistication and capability to use a variety of sectors and methods (e.g., commingling proceeds of crime with lawfully obtained revenues, structuring, and smurfing) to launder the large amount of cash proceeds generated from these crimes.

The illegal firearms market in Canada continues to attract OCGs of all levels of sophistication, primarily street gangs operating in metropolitan cities, as well as criminally inclined individuals. The CISC estimates that over 70 OCGs are involved in smuggling illicit firearms from the US. Increasingly, OCGs are specializing in manufacturing privately made firearms and smuggling the necessary components. In general, OCGs use firearms to strengthen their position within other criminal markets, such as the illegal drugs market.

In terms of money laundering risk, individual actors tend to launder proceeds of crime for personal use following the transaction, using simple methods and techniques, such as structuring deposits, purchasing casino chips, or using electronic funds transfers. A small network of associates may also be relied on to launder proceeds. These actors are assessed to pose a low level of sophistication, capability, and scope. RCMP has observed that most of the transactions appear to be for one-off sales rather than for larger shipments of firearms.

For sophisticated actors, the trafficking of firearms is likely to be just one aspect of their illegal activities and as such the proceeds from firearms trafficking would be one part of their overall larger money laundering activities. These actors may also use the services of professional money launderers.

ML Threat from Human Smuggling and Human Trafficking: Canada remains a target for increasingly sophisticated global human smuggling and human trafficking networks. Human trafficking, also known as trafficking in persons, involves the recruitment, transportation, harbouring, and/or exercising control, direction, or influence over the movements of a person in order to exploit that person or to facilitate their exploitation, typically through sexual exploitation or forced labour. Human smuggling involves facilitating the illegal entry of a person into a country by air, land, or sea where the person being transported is not a national or resident.[81]

[81] RCMP (2024) Migrant Smuggling

Due to the underreporting of this criminal activity, it is difficult to reliably determine the magnitude of proceeds of crime being generated by human trafficking. Globally, it is estimated that human trafficking generates US$150 billion per year.[82] In Canada, the financial gains derived from human trafficking are considered materially significant. Human trafficking and human smuggling inflict profound and enduring trauma on victims through both physical and psychological harm.

Within Canada, the most detected form of human trafficking by law enforcement is trafficking for sexual exploitation. Indicators that a victim is being trafficked include online pages created on their behalf to solicit clients, unusual transfers to an unknown third party, depositing of cash into accounts by third parties, e-transfers with sexually explicit messages, and the purchase of unusual amounts of hotels and fast food.[83]

Human trafficking actors demonstrate a moderate level of sophistication in their money laundering operations. However, the involvement of OCGs in human trafficking indicates a potential to enhance the sophistication of money laundering activities, as they may comingle proceeds from other criminal activities. The CISC notes that there has been a 24 per cent increase in OCG involvement in human trafficking since 2020, with domestic sexual exploitation remaining the most common form of trafficking.[84] Human traffickers are commonly known to use cash, prepaid cards, e-mail money transfers, and crypto assets. They often also use money mules or other nominees to launder proceeds of crime, typically through personal accounts. They also leverage business accounts, front companies, and legitimate business ventures.[85]

Unlike with human trafficking, a smuggled person generally willfully consents to be smuggled. Human trafficking can occur entirely within the same country, whereas human smuggling only occurs where there is transportation between countries. The source of profit for human smuggling is the fee the person pays to be smuggled. In trafficking cases, profits are made through the exploitation of the victim. [86] Smuggled persons may ultimately become trafficking victims, as many are vulnerable to exploitation after having entered a new country through an irregular fashion without many social connections or full knowledge of their rights.

According to CISC analysis, human smuggling is believed to be carried out by a limited number of OCGs in Canada. Given the sophistication, logistical planning, and finances needed to conduct human smuggling operations, OCGs engaged in this activity are suspected to be highly capable in laundering the proceeds of their crimes. Large amounts can be generated by individual smuggling actions, for example up to $65,000 per person for illicit passage to Canada through the Caribbean and the US.[87]

A 2022 FATF report found that IVTS are the most common method of transferring funds generated from migrant smuggling between jurisdictions. This can make it difficult for law enforcement agencies to perform financial investigations. Other methods include the physical transportation of funds via cash couriers or money mules.

[82] CISC (2022) Public Report on Organized Crime in Canada
[83] Statistics Canada (2024) Trafficking in persons in Canada, 2023; Statistics Canada (2024) Preliminary national estimates on police-reported human trafficking incidents, 2024; US Department of State (2024) 2024 Trafficking in Persons Report: Canada
[84] CISC (2024) Public Report on Organized Crime in Canada
[85] FINTRAC (2021) Updated Indicators: Laundering of proceeds from human trafficking for sexual exploitation
[86] Public Safety Canada (2025) About Human Trafficking
[87] Global News (2020) Canadian human smuggler allegedly charged migrants up to $65K for transport to Canada

Canada's Policy Response

Canada's Efforts to Combat Human Smuggling

The Government of Canada combats human smuggling through its Migrant Smuggling Prevention Strategy. Renewed in March 2024 for five years, the Migrant Smuggling Prevention Strategy aims to prevent and disrupt maritime human smuggling operations and dismantle organized criminal smuggling networks that target Canada as a destination. This whole-of-government strategy, coordinated by GAC and executed by the RCMP and IRCC, facilitates intelligence gathering and outreach in countries of origin and transit.

Additionally, to help in global efforts to combat human smuggling, Canada is implementing the ***G7 Action Plan to Prevent and Counter the Smuggling of Migrants*** that was jointly adopted by G7 countries in October 2024. The Plan outlines five pillars of action:

1) Strengthening the capacities of law enforcement agencies against migrant smuggling groups;
2) Strengthening international cooperation between police, judicial, and border officials;
3) Strengthening cooperation with countries of origin and transit of irregular migration flows;
4) Prevention and awareness raising; and
5) Increasing knowledge and monitoring of migrant smuggling.

Through this action plan, the G7 confirms their commitment to intensify efforts to prevent, counter, and eradicate OCGs engaging in human smuggling and stripping them of the proceeds generated by these crimes.

Canada's Policy Response

Canada's Efforts to Combat Human Trafficking

The **National Strategy to Combat Human Trafficking** guides Canada's response to human trafficking. Since 2019, this whole-of-government approach is led by the federal government, in collaboration with the provinces and territories, non-government organizations, and Indigenous communities. The strategy is built around five pillars: empowerment, prevention, protection, prosecution, and partnerships. The Strategy supports efforts to prevent trafficking, empower and support survivors, bring perpetrators to justice, and strengthen community safety through targeted investments and coordinated federal action.

Public-Private Collaboration: Project Protect

Project Protect is a public-private partnership led by the Bank of Montreal (BMO), with the assistance of other banks, Canadian law enforcement agencies, and FINTRAC. First launched in 2016, Project Protect targets human trafficking for sexual exploitation by focusing on the money laundering aspect of the crime. FINTRAC's 2021 Operational Alert, Updated Indicators: Laundering of Proceeds from Human Trafficking for Sexual Exploitation, provided 58 additional indicators to assist businesses in better identifying and reporting suspicious transactions associated with human trafficking for sexual exploitation.

The objective of the project is to improve the collective understanding of the crime, and to improve the detection of the laundering of proceeds from human trafficking for sexual exploitation. FINTRAC generated 147 financial intelligence disclosures related to human trafficking in 2023-2024. Project Protect was expanded in 2023-2024 to include the laundering of proceeds associated with labour trafficking.

Enforcement Action Spotlight: Human Trafficking

In 2023, the RCMP's Trafficking Response Team in Swift Current Saskatchewan utilized FINTRAC financial intelligence during an investigation into a human trafficking operation that used a popular job bank to recruit an adult female from Bangladesh staying in Canada on a visitor's permit. After providing her a working permit, the accused forced the woman to work 10 to 12 hours a day, seven days a week, for several months at various restaurants. When not working, she was forced to stay in an unfinished, concrete basement, which was dimly lit and heavily water damaged. As a result of the investigation, two people were charged with trafficking a person. One individual was also charged with three counts of sexual assault.[88]

Enforcement Action Spotlight: Human Smuggling

In June 2024, the RCMP and the Cornwall Regional Task Force dismantled an international human smuggling ring that allegedly funneled hundreds of migrants into the US in the area around Cornwall, Ontario between July 2022 and June 2023. Migrants were allegedly charged thousands of dollars by the smugglers. Dangerous night-time crossings cost some migrants their lives. The RCMP identified and charged eight people associated with these activities, including the primary leader of the criminal operation.[89]

[88] RCMP (2023) Saskatchewan RCMP STRT charges two males after investigation into forced labour at Saskatchewan restaurants

[89] RCMP (2024): International human smuggling ring dismantled

ML Threat from Extortion and Ransomware: Extortion occurs when money, property, or services are unlawfully obtained from a person, entity, or institution through coercion.[90] Incidents of extortion have grown significantly in Canada over the past decade with nearly 14,000 cases reported in 2023.[91] Key types of extortion affecting Canadians include ransomware and financial sextortion.

Extortion disrupts business operations and increases business costs associated with implementing security systems or paying ransoms to protect assets. For individuals, extortion often results in financial losses, compromised personal data, and psychological harm. Proceeds of extortion allow criminals to reinvest in the infrastructure and resources needed to further perpetuate these crimes.

Criminal actors involved in extortion can range from individuals to OCGs, and therefore display varying levels of sophistication, capability, and scope for laundering extortion-related proceeds. Structuring and smurfing, commingling, and casino refining activities may be used to launder proceeds of extortion, particularly proceeds in cash.

There has been an increase in the sophistication of laundering the proceeds of crime as cyber-related forms of extortion grow. Cyber-related forms of extortion that leverage crypto assets – or convert proceeds of crime into crypto assets – tend to leverage more sophisticated techniques to move funds and are committed by threat actors who possess technological expertise to commit their crimes and to conceal their identity and physical location.[92]

Ransomware occurs when a perpetrator compromises a victim's device, encrypts their data, and demands a ransom to provide a decryption key. Ransomware actors often exfiltrate files before encrypting them and threaten to leak sensitive information publicly if the ransom is not paid.[93] Since 2020, ransomware attacks have increased in scope, frequency, and complexity. A 2023 study by cybersecurity firm Palo Alto Networks and polling firm Angus Reid Institute found that the average ransom paid by Canadian businesses was $1.13 million, an increase of almost 150 per cent in two years.[94]

Ransomware-as-a-Service model, available for lease or purchase on the dark web, has lowered technical barriers to entry for threat actors, contributing to the overall rise in ransomware incidents. Similarly, phishing attacks in Canada are becoming more prevalent and sophisticated due to new tools and services, including Phishing-as-a-Service kits available online to cybercriminals. Collectively, such attacks can have a significant impact on the integrity of key business sectors and the Canadian financial system.

The impact of ransomware can be extensive, and often includes core business disruptions, data loss and potentially significant recovery costs. In critical infrastructure sectors, such as healthcare, ransomware could cause physical harm to individuals or even result in loss of life. Due to its impact on individuals and an organization's ability to function, ransomware is one of the most disruptive forms of cybercrime facing Canada.[95]

[90] CAFC (2023) Extortion
[91] Statistics Canada (2024) Incident-based crime statistics, by detailed violations, Canada, provinces, territories, Census Metropolitan Areas and Canadian Forces Military Police
[92] FATF (2023) Countering Ransomware Financing
[93] TELUS (2022) TELUS Canadian Ransomware Study
[94] Global News (2023) Canadian firms paying 'significantly' more in ransomware attacks: data.
[95] Canadian Centre for Cyber Security (2024) National Cyber Threat Assessment 2025-2026

Ransomware threat actors almost exclusively demand payment in the form of cryptocurrency, which is often laundered through techniques and services such as peel-chains (where cryptocurrency is transferred through a series of digital wallets, with small amounts of funds "peeled off" and cashed out at each step to obfuscate the trail), mixers (a service that mixes potentially identifiable or "tainted" cryptocurrency funds with others), online gambling platforms, and DeFi platforms, before being exchanged to fiat currency at crypto asset exchanges located in foreign jurisdictions with weak AML/ATF controls.[96] The speed at which the funds are moved and then exchanged to fiat currency may make it difficult to detect ransom payments in real time.

Quick Definitions

Phishing is an attack where a scammer calls, texts, or emails a victim, or uses social media to trick a victim into clicking a malicious link, downloading malware or sharing sensitive information, usually for financial gain. Phishing attempts are often generic mass messages, but the message appears to be legitimate and from a trusted source, such as a bank or courier company.

Enforcement Action Spotlight: Project Cipher

In 2021, the RCMP conducted a reverse hack of criminally controlled servers that halted a piece of malicious software that was designed to exploit computer networks for money and supported international cyberattacks for years. The malicious software that the RCMP helped take down was used in high-profile ransomware cases where computer-network owners – usually large institutions such as private businesses, government departments, or universities – were prevented from accessing their own data until a large ransom was paid to criminal actors.[97]

Sextortion is a form of online blackmail where the victim is convinced to send sexual images or videos of themselves which are then threatened to be shared with others unless the victim pays the offender or sends more images. The perpetrator may then threaten to share the content publicly on social media or send it to friends and family of the victim. Although sextortion can affect anyone, this online crime particularly impacts Canadian youth aged 14 to 24.[98]The psychological impacts of sextortion on victims can be severe and long-lasting. In some cases, these impacts can result in extreme outcomes, such as self-harm or even suicide.

The Canadian Centre for Child Protection reports that it receives an average of seven sextortion reports per day, and that demands for money are often linked to international OCG networks.[99] Payments are conducted through various means, including cryptocurrencies, e-transfers, and the use of MSBs. Typically, once the funds are out of the victims' control, the value is transferred quickly in an attempt to mask the illicit source of funds.

[96] Chainalysis (2022) The 2022 Crypto Crime Report
[97] RCMP (2021) RCMP helps stop malware that stole millions from Canadians
[98] RCMP (2024) Sextortion
[99] Cybertip.ca (Accessed 2025) Online Harms: Sextortion

In addition to the practice of sextortion, another area of significant concern is the production and distribution of child sexual abuse material. FINTRAC analysis related to online child sexual exploitation indicates that the senders of payment (i.e. suspected purchasers) were typically males aged 40-60, and transfers were generally under $100 (though higher for certain Eastern European destinations). The collection of payments for these materials are conducted by sending cryptocurrency either directly or indirectly to a darknet marketplace where these materials are sold. Transactions have also been documented using MSBs, including payment processors.[100]

Canada's Policy Response

Canada's National Strategy for the Protection of Children from Sexual Exploitation on the Internet

The National Strategy for the Protection of Children from Sexual Exploitation has guided Canada's response to online child sexual exploitation since 2004. The Strategy addresses online child sexual exploitation through a multi-faceted approach with activities under four pillars: prevention and awareness; pursuit, disruption and prosecution; protection; and partnerships, research and strategic support.

Public-Private Collaboration: Project Shadow

Project Shadow is a public-private partnership co-led by Scotiabank and the Canadian Centre for Child Protection, supported by Canadian law enforcement agencies and FINTRAC to combat online child sexual exploitation. The objective of the project is to improve the collective understanding of the threat, and to improve the detection of the facilitation and laundering of the proceeds from online child sexual exploitation. FINTRAC generated 45 financial intelligence disclosures related to online child sexual exploitation in 2023-2024. Financial intelligence disclosures included 127 unique suspicious transaction reports on 320 subjects of interest from all 10 provinces and two territories.

ML Threat from Robbery and Theft: Robberies and thefts in Canada are undertaken by a diverse range of threat actors. While small-scale robberies and thefts are primarily conducted by opportunistic individuals and petty thieves, robberies and thefts at a larger scale are frequently associated with OCGs. This assessment focuses on more serious robbery and theft, including auto theft.

Victims of robbery and theft experience financial loss, emotional distress, and, in some cases, physical harm. Businesses incur revenue losses and increased security spending, which impacts their profitability and growth.

The rate of large-scale theft in Canada above $5,000, not including auto theft, rose 49 per cent between 2013 and 2023.[101] In particular, cargo theft – when goods are stolen during transportation – rose 59 per cent in Canada and the US in 2024, according to CargoNET, a cargo theft prevention and recovery network.[102] OCGs are also believed to target heavy machinery, such as farm or construction equipment. After doubling from 2022 to 2023, CISC reports that OCG involvement in vehicle theft remained steady in 2024; however, OCG involvement is increasingly reported in Western Canada, as a response to the increased law enforcement focus on Eastern Canada. The most sophisticated and capable OCGs involved in vehicle theft in Canada have well-established transnational networks that supply foreign markets with stolen Canadian vehicles.

[100] FINTRAC (2020) Operational alert: Laundering of proceeds from online child sexual exploitation
[101] Statistics Canada (2024) Police-reported crime for selected offences, Canada, 2022 and 2023
[102] Verisk (2024) Cargo Theft Data | CargoNet

Canada's Policy Response

Canada's National Action Plan on Combatting Auto Theft

In 2024, the Government of Canada released a National Action Plan on Combatting Auto Theft, outlining actions focused on disrupting, dismantling, and prosecuting implicated OCGs.

The National Action Plan includes legislative and regulatory changes, including to the *Criminal Code*, to strengthen penalties for auto theft with ties to violence, organized crime and money laundering; a new aggravating factor applicable at sentencing where there is evidence that an offender involved a young person in committing an office; and changes to the *Radiocommunication Act* to regulate devices used to steal cars.

Additional measures include enhanced intelligence and information sharing among municipal, provincial, federal, and international police and customs officials. These measures aim to support criminal investigations, charges, and prosecutions, building on joint efforts already underway. The Government also announced intervention improvements that would enable the examination of more shipping containers through increased capacity at the CBSA and the integration of new targeting tools.

Statistics Canada data on police-reported theft (excluding auto theft) suggests the total proceeds of crime to be in the hundreds of millions of dollars in 2023. Auto theft, in particular, is an evolving threat issue that is believed to generate significant proceeds of crime. A large portion of this profit goes to the buyers and exporters of stolen vehicles, and another substantial portion is realized at the final point of sale in a foreign jurisdiction.

FINTRAC financial intelligence and the sophistication of theft operations observed by law enforcement suggests that OCGs involved in auto theft in Canada have sophisticated money laundering capabilities, utilizing trade fraud and related techniques to disguise the illicit origin of the automobiles and to move the proceeds of crime within Canada, internationally, and back to Canada. Professional money launderers may also be used to conduct intricate money laundering schemes, including trade-based money laundering, given the large amounts of proceeds of crime that may be realized outside of Canada.

The methods employed to obscure the flow of proceeds of crime include cash smuggling, international electronic funds transfers, the use of nominees, and the establishment of front and shell companies. In addition, financial intelligence suggests that individuals or entities suspected of having a significant role in a car trafficking ring are consistently observed owning or frequently transacting with freight transportation and logistics companies, used car dealerships, auto-parts companies, import/export companies, and towing companies located within the Greater Toronto Area and Greater Montréal Area.

Enforcement Action Spotlight: Canada Border Services Agency (CBSA)

The CBSA provides critical support to law enforcement partners to disrupt, investigate and ultimately prosecute these crimes. In 2024, the CBSA intercepted 2,277 stolen vehicles, which represents an increase of 26 per cent in interceptions from 2023 and about 83 per cent from 2020. Additionally, the CBSA has implemented a request for information protocol to consolidate and expedite the sharing of customs information to police of jurisdiction and addressed 2,758 requests received in 2024.

Enforcement Action Spotlight: Project Big Rig

In 2023, the Peel Regional Police used financial intelligence in a joint force operation investigating a series of tractor trailer and cargo thefts across the Greater Toronto Area. The investigation resulted in the disruption of a criminal ring. Project Big Rig resulted in a total of 15 arrests and 73 charges laid, along with the recovery of $6,990,000 in stolen cargo and $2,250,000 in stolen tractor trailers.[103]

Low Money Laundering Threat

ML Threat from Environmental Crimes: Environmental crimes of concern from a money laundering perspective in Canada include pollution crime, wildlife crime, and illegal and unregulated fishing. The amount of proceeds of crime generated in Canada from each of these environmental crimes varies. These crimes cause lasting harm to Canada's people, economy, and ecosystems by threatening public health, damaging wildlife and habitats, reducing marine biodiversity, and contributing to the effects of climate change. They also undermine the livelihoods of Canadians, particularly those living in rural communities or working in industries dependent on natural resources.

Pollution crime in Canada includes the trafficking of electronic waste, importation of counterfeit products that do not meet Canada's environmental standards (e.g., counterfeit engines), and the use of deceptive practices to undermine emissions regulations, such as dumping or using third parties to dump waste illegally.

Wildlife crime in Canada includes the trafficking of Canadian species, such as narwhal tusks, polar bear hides, peregrine falcon eggs and wild ginseng, through established illicit markets. Illegally trafficked wildlife are being increasingly transported with legal flora and fauna products, which makes identification and interception of illegally acquired goods more difficult. Threat actors in this area are often opportunistic, criminally inclined individuals who exhibit low levels of sophistication. However, transnational OCGs appear to be increasingly involved.

Illegal fishing refers to fishing by national or foreign vessels without permission or undertaking fishing activities that contravene the country's laws, regulations, or its international obligations.[104] Coastal areas are vulnerable to illegal fishing by small- and medium-scale enterprises, as well as opportunistic and organized individuals. These actors may perpetrate fraud through the under-reporting and/or misreporting of legally and illegally caught fish. Methods may also include corrupting officials at ports; using vertically integrated business lines; misrepresenting illegal catches as legitimate when sold in commercial markets; bribing Indigenous fishers holding special Indigenous licenses, and over-packing and subsequently under-reporting catches. A lack of transparency over the ownership of certain fishing quotas also makes the markets on Canada's West Coast vulnerable to abuse for money laundering, tax evasion, and sanctions evasion by criminals. The main actors involved in illegal fishing are harvesters, buyers, shippers and processors attempting to bypass catch reporting and regulatory requirements, with some suspected OCG involvement.

[103] Peel Regional Police (2023) PRP Joint Force Operation Results in significant cargo theft recovery
[104] Fisheries and Oceans Canada (2019) Illegal, Unreported and Unregulated (IUU) Fishing

Proceeds generated by wildlife crime have increased since 2023. Methods used to launder proceeds derived from wildlife crime can vary depending on the destination country and type of commodity being illegally trafficked. FINTRAC has identified several typologies employed in money laundering schemes associated with illegal wildlife trafficking, including the use of nominees, front companies owned by traffickers or their associates, and funds layered between related accounts. Cash transactions, wire transfers, and email money transfers were the primary transactions in suspicious transaction reports submitted to FINTRAC related to wildlife trafficking.[105] Laundering methods for illegal fishing can be relatively simple with proceeds mostly used for direct spending or immediate placement. This may include placement in vertically integrated family business structures, such as family-owned restaurants located near the point of catch. Wiring of proceeds between multiple corporate banks accounts to obfuscate the original source of funds is also a possibility.

Public-Private Collaboration: Project Anton

Project Anton, launched in 2023, is a first-of-its-kind international public-private partnership led by Scotiabank and supported by FINTRAC, The Royal Foundation's United for Wildlife Network, and other domestic and international partners working to combat the illegal wildlife trade.

The project is named after Anton Mzimba, head of security at the Timbavati Private Nature Reserve in South Africa and a Global Conservation Technical Advisor, who was murdered for his commitment to protecting and conserving wildlife. In his memory, Project Anton aims to improve the collective understanding of illegal wildlife trade and to improve the detection of the laundering of proceeds from this crime.

Since the launch of Project Anton, FINTRAC has generated more than 25 disclosures of actionable financial intelligence related to illegal wildlife trade for Canada's law enforcement agencies and international partners.

***ML Threat from Loan Sharking*:** Loan sharks are illegal lenders who operate outside any regulatory framework and lend in contravention of the *Criminal Code*, section 347 (1)[106] on "Criminal interest rate." Loan sharks are often associated with organized crime, and appear to target wealthy high-rollers, low-income individuals, problem gamblers playing in legal or illegal gambling establishments (including online), illicit drug users, and entrepreneurs who need capital to start a business or to keep it operational. Loan sharking traps vulnerable individuals in cycles of debt, draining families and communities. It also enables OCGs to fund and expand their operations through illegal gambling, the drug trade, and other crimes.

Loan sharking can be part of larger operations backed by OCGs and may involve threat actors with a relatively high level of sophistication in laundering proceeds generated from criminal lending activities. Loan sharking appears to be limited to a small number of more sophisticated OCGs in Canada, as well as a small number of independent operators.

[105] FINTRAC (2022) Operational alert: Laundering the proceeds of crime from illegal wildlife trade

[106] On January 1, 2025, the criminal rate of interest under *Criminal Code* s.347(1) was lowered, and came into effect: Canada Gazette, Part 2, Volume 158, Number 13: Order Fixing January 1, 2025 as the Day on Which Sections 610 to 612 of the Budget Implementation Act, 2023, No. 1 Come into Force Additional amendments broaden the application of the *Criminal Code* to prohibit the 'offering or advertising' of credit at a rate exceeding the criminal interest rate: Canada Gazette, Part 2, Volume 159, Number 1: Order Fixing January 1, 2025 as the Day on Which Certain Provisions of the Budget Implementation Act, 2024, No. 1 Come into Force

Loan sharking in Canada is estimated to to generate relatively lower proceeds of crime. Due to the associated stigma, as well as the expected high interest rates and risks of borrowing money from criminal organizations, the actual level of proceeds of crime from loan sharking may be significantly under-reported. Loans sharks are believed to use a variety of money laundering methods, including laundering funds through casinos and financial institutions, as well as through the real estate and construction industries.

ML Threat from Counterfeiting: Counterfeiting in the Canadian context pertains primarily to counterfeit goods and counterfeit currency. With respect to goods, a broad range of counterfeit and pirated products are sold in Canada, primarily online, with Toronto, Montreal, and Vancouver remaining as the key entry points for these products into the Canadian marketplace. China is the primary source of counterfeit goods imported into Canada.

Counterfeit goods undermine legitimate industries, reduce government tax revenues, and potentially pose health and safety risks to Canadians. Counterfeit currency results in financial losses for Canadians and businesses. Counterfeit currency can also undermine public confidence in the Canadian dollar.[107]

According to CISC data, OCGs active in the counterfeit and forgery criminal market are primarily based in BC and Ontario, with smaller concentrations in Québec and the Maritime provinces. OCGs appear to have established links with illicit global distribution channels, allowing them to bring increasing volumes of counterfeit products into Canada. Clients buying these products may not know that they are counterfeit.

Most goods counterfeiting threat actors who target customers in Canada exhibit a low level of sophistication with respect to money laundering. FINTRAC analysis suggests varying levels of complexity in money laundering operations by counterfeiters. Counterfeiters may exploit online marketplaces, use front companies, and misuse the services offered by payment processors to launder and reintegrate illicit funds into the financial system before rapidly transferring them offshore or to other corporations.

In contrast, the volume of counterfeit banknotes passed in Canada has declined by approximately 50 per cent in recent years.[108] The introduction of polymer notes in the early 2010s has substantially affected the currency counterfeiting market and contributed to the decline of currency counterfeiting rates over the last decade.[109] The money laundering risks arising from this activity are low compared to other predicate offences.

[107] Bank of Canada (2017) The Economic Impact of Counterfeiting in Canada
[108] RCMP (2024) Statistics on counterfeit Canadian bank notes - Total number passed and seized
[109] Blueline (2023) Counterfeit currency: How the RCMP, law enforcement and the Bank of Canada combat fake money

Chapter 4: Assessment of Terrorist Financing Threats

Overview

The terrorist financing threat assessment indicates that Canada's terrorist financing landscape is largely low volume, characterized by low value transactions and limited financial flows. There is little evidence to suggest that terrorist funds are flowing into or returning to Canada to finance domestic terrorism.

Where there is a terrorist financing nexus to Canada, funds originate from Canada and are either (i) directed to domestic terrorists, who primarily use self-financing methods to support attacks; or are (ii) destined to foreign jurisdictions where terrorists are known to operate or have financing links with international terrorist groups. In the Canadian context, terrorists can range from individual lone actors to organized terrorist groups.

Given the grave consequences of terrorist activity both in Canada and abroad, Canada must remain vigilant to protect its national security from terrorists and violent extremists, including their financing.

Quick Definitions

What is Terrorist Financing?

Terrorist financing is the use of funds, property or other services to encourage, plan, assist, or engage in acts of terrorism, where the primary motivation is not financial gain.

Two main differences distinguish terrorist financing from money laundering:

- Funds can be from lawful sources, not just criminal acts; and
- Money is the means, not the end – the goal is to use funds to facilitate or carry out terrorist activities.

Canada is a diverse, multicultural society with many individuals maintaining ties to communities around the world. This contributes to financial flows from Canada to many jurisdictions abroad, which can be important and legitimate sources of financing for economic development and other social purposes. Measures taken by the government or private sector entities, intended to mitigate risks related to terrorist financing, should be considered on a case-by-case basis. This assessment should not be used as a justification for discriminatory behaviour or actions toward specific communities in Canada or abroad. The vast majority of funds leaving Canada via remittances do not support terrorist financing activities.

Terrorist Financing Threat Assessment Methodology

Terrorist financing threats in Canada are determined based on updated intelligence on the Canadian and international threat environment, including known or suspected cases of terrorist financing investigated or observed by Canadian law enforcement and intelligence services.

Terrorist financing threats are assessed against three criteria on the basis of ideologically, politically, or religiously motivated violent extremism:

1) Level of threat actor sophistication, including established financing networks and ability to have resilient, sustainable, and long-term funding;
2) Level of threat actor capability in undertaking terrorist financing operations in Canada, including access to facilitators, networks, and links to organized crime; and
3) Linkages with Canada, including suspected terrorist financing from, within, and, to Canada.

Specific threat ratings are not assigned to the groups identified in this assessment. The terrorist groups or movements named in this report have been identified as being active in raising and moving funds through Canada and the Canadian financial system.

Terrorist Financing Methods

Terrorist financing methods vary depending on the terrorist actor's structure, motivations, geopolitical context, and connections. Terrorists are adaptable and will exploit both legal and illegal channels to secure funding. Terrorists raise, move, and use funds through a variety of methods, often adapting their financing strategies in response to law enforcement efforts and regulatory controls.

The cost of conducting a terrorist attack varies widely, depending on the sophistication of the terrorist group or individual involved and the nature of the attack. Impactful terrorist attacks can require minimal funds adding further complexity to national security investigations. Funds tend to be raised and moved in smaller amounts, making detection and tracking difficult.[110] The degree to which a terrorist actor is sophisticated in their origination and operations may also determine the extent to which various techniques are used and how much funding is required. Lone actors are less likely to use sophisticated techniques to fund their activities, relying instead on personal income and/or other legitimate sources.

While there is little evidence that terrorist funds flow into or return to Canada, domestic fundraising and self-financing are areas of concern, with funds often moving to international jurisdictions that are high-risk for terrorist financing, which include areas where listed terrorist entities are known to operate, or jurisdictions with identified deficiencies relating to the implementation/enforcement of anti-terrorist financing measures.

Quick Definitions

Types of Violent Extremism

Three classifications of violent extremism can be derived from definitions included in Canadian law, including the *Criminal Code* and *CSIS Act*. While none of these categories are necessarily mutually exclusive, CSIS identifies the following types of violent extremism in their 2025 publication titled *Protecting National Security in Partnership with all Canadians*:

Ideologically Motivated Violent Extremism (IMVE)

IMVE actors are driven by a range of influences rather than a singular belief system. Radicalization is more often caused by a combination of ideas and grievances resulting in a personalized worldview that is inspired by a variety of sources. IMVE includes gender-driven, xenophobic, anti-authority, and other grievance-driven violence.

Politically Motivated Violent Extremism (PMVE)

PMVE encourages the use of violence to establish new political systems, or new structures and norms within existing systems.

Religiously Motivated Violent Extremism (RMVE)

RMVE encourages the use of violence as part of a spiritual struggle against a perceived immoral

[110] FINTRAC (2022) Operational alert: Terrorist activity financing

Table 6
Common terrorist financing methods

Criminal Activity	Many terrorists supplement their financing through illicit activities, including drug trafficking, kidnapping for ransom, arms smuggling, and extortion. Some terrorist groups engage in human trafficking, counterfeiting, and cybercrime to diversify their revenue streams.
Crowdfunding	Crowdfunding platforms allow individuals or groups to appeal for funds online directly from members of the public who may be geographically dispersed. Terrorists have been observed to co-opt crowdfunding platforms to reach global audiences to solicit funds and donations to support terrorist activity.
Cryptocurrencies	Cryptocurrencies are becoming increasingly attractive for terrorist financing due to the nature of their pseudonymous, decentralized networks that allow individuals to send or receive funds anywhere in the world.
Informal Value Transfer Systems (IVTS)	IVTS, such as *hawalas*, *hundi*, and *fei'chen*, involve dealers who facilitate the transfer of value to a third party in another jurisdiction without having to physically move the items. Terrorist groups have been observed to use IVTS to sidestep formal banking channels to transfer funds across borders.
Non-Profit Organizations (NPOs) and Charitable sector abuse	Terrorist groups operating overseas in conflict areas and/or territories controlled by terrorist groups have been known to use and/or abuse NPOs, both sham and legitimate (unwitting diversion of funds), to raise and move funds.
Self-financing	Self-financing refers to strategies and techniques, both legal and illicit, used by terrorist actors to generate their own financial resources to fund their violent activity. Lone terrorist actors typically leverage self-financing methods to support their terrorist acts.
State Sponsorship	Certain terrorist groups rely on financial support from national governments. Notably, funding from Iran is a key source of financing for Hamas and Hezbollah. Iran is known to use trade-based money laundering techniques, front companies, financial institutions, correspondent banking, and crypto assets to support these terrorist groups.

Evolution of the global terrorist landscape

The nature of the global terrorist threat has evolved since the early 2000s. At that time, terrorist activity was largely driven by religiously motivated groups, such as Al-Qaida and the Taliban. The rise of Daesh after 2013, in particular, inspired individuals from around the world – including Canada – to travel to Syria and Iraq to engage in violent extremist activity. Commonly referred to as 'foreign terrorist fighters,' or 'Canadian extremist travellers' in the domestic context, these individuals have been involved in a variety of activities, including frontline combat, fundraising, operational planning, and disseminating online propaganda. While foreign terrorist fighters emanating from Canada was not a new phenomenon, the volume and speed at which individuals left Canada to travel to Syria to join Daesh became significant.

While the threats posed by these groups persist, the current terrorist threat landscape is more complex. There has been a global rise in ideologically and politically motivated violent extremists, who are fueled by a range of factors, such as social isolation, anti-government sentiment, and mis-and dis-information. These groups and individuals have found likeminded networks that perpetuate their radicalization, which, in some cases, can lead to violence. These largely online and diffuse activities have made it increasingly difficult for intelligence and law enforcement agencies to detect, disrupt, and prevent these threats.

Adding to this complexity is a growing nexus between terrorism and transnational organized crime, creating a bond of mutual interest. Terrorists can leverage organized crime for various purposes, furthering their ideological, religious, or political objectives.

Spotlight: Transnational OCGs and Terrorist Financing

Canada recognizes that transnational OCGs can form alliances with terrorist groups to secure routes, finance operations, and support their objectives, leading to a complex network of illicit financial flows. The links between these criminal organizations and terrorist networks pose a challenge to international security, as they enable both groups to expand their operations. Countering these financial networks is important to disrupt their funding channels and weaken their influence.

In February 2025, Canada listed seven transnational OCGs as terrorist entities under the *Criminal Code,* including Cártel del Golfo, Cártel de Sinaloa, La Familia Michoacana, Cárteles Unidos, La Mara Salvatrucha, Tren de Aragua, and Cártel de Jalisco Nueva Generación.

These seven organizations are now considered terrorist entities under Canadian law. Listing these organizations as terrorist entities assists Canadian security, intelligence, and law enforcement agencies in combatting terrorism and plays a key role in countering domestic financing activities.

Terrorist Financing Threat Actors Relevant to Canada

The Government of Canada groups terrorist threats into three broad categories: ideologically motivated violent extremism (IMVE), politically motivated violent extremism (PMVE), and religiously motivated violent extremism (RMVE). While there are some common financing methods employed by terrorists regardless of primary motivation, there are some distinct financing methods associated with each of IMVE, PMVE, and RMVE.

In the past decade, the most common perpetrators of attacks in Canada, resulting in the most fatalities, have been lone actors motivated by a range of grievances, the majority of which fall under the IMVE category. These actors tend to be inspired by diffuse networks, carry out their attacks using low sophistication methods, such as bladed weapons or vehicles, which generally require fewer resources. PMVE and RMVE groups typically have sophisticated international financing networks and larger funding portfolios and revenue streams due to their longstanding activities.

The top threat groups that continue to have financial links to Canada are discussed below.

Quick Definitions

***Criminal Code* Terrorist Listing Regime**

Canada's *Criminal Code* listing regime provides the legal framework to designate an individual or group as a terrorist entity.

A group or individual may be listed if there are reasonable grounds to believe that it has knowingly carried out, attempted to carry out, participated in, or facilitated a terrorist activity, or has knowingly acted on behalf of, at the direction of, or in association with a terrorist entity. Legal thresholds for listing an entity are set out under *Criminal Code* section 83.05.

Being listed as a terrorist entity carries significant consequences. It is a *Criminal Code* offence for any person in Canada or Canadian abroad to knowingly deal in property owned or controlled by a terrorist entity. To avoid criminal liability, banks and brokerages may freeze the entity's assets, which can then be the subject of seizure, restraint, and/or forfeiture under the *Criminal Code*.

The Minister of Public Safety and Emergency Preparedness is responsible for maintaining the list and publishes this information online: Currently listed entities

Ideologically Motivated Violent Extremism

IMVE is a growing threat to Canada's national security and draws from a complex range of ideas from across the traditional "left-right" ideological spectrum. This includes anti-authority, xenophobic, gender-driven, and other types of violent extremist views. According to CSIS, between 2014-2024, IMVE-related attacks in Canada resulted in 26 deaths and more than 40 injuries.[111]

CSIS has divided the violence carried out by IMVE threat actors in Canada into four main categories:

- *xenophobic violence*: racially or ethnically motivated violence based on fear or hatred of what is perceived to be foreign, strange, or different;
- *anti-authority violence:* violence against the authority of state and law-enforcement entities;
- *gender-driven violence*: violence motivated by hatred of those with a different gender or sexual orientation; and
- *other grievance-driven violence*: violence committed by individuals with no clear association with an organized group or any external guidance.

[111] CSIS (2025) Protecting National Security in Partnership with all Canadians

IMVE radicalization is often caused by a combination of ideas and grievances resulting in a personalized worldview that is inspired by a variety of sources including books, videos, online discussions, and conversations. Those holding violent extremist views often attempt to create a culture of fear, hatred, and mistrust that can result in an individual's willingness to incite, enable, or mobilize to violence.[112]

As of December 2024, Canada has listed eight IMVE-related groups and one individual as terrorist entities under the *Criminal Code,* including the Proud Boys, Atomwaffen Division, the Base, the Russian Imperial Movement, Blood and Honour, Combat 18, Three Percenters, Aryan Strikeforce, and American neo-Nazi James Mason.

IMVE movements and IMVE groups are distinct. IMVE movements are often informal networks, or loose coalitions of like-minded individuals with no clear structure or direction. They can dissolve and reformulate at any given time on any given issue. Nevertheless, IMVE groups, like the Atomwaffen Division and The Base, have a more structured leadership hierarchy with more clearly defined objectives. This includes individuals driven by a belief in the superiority of the white race and who have targeted their violence towards non-white communities.

Misogyny has also been a significant feature of IMVE attacks in Canada. The involuntary celibate movement, dubbed 'incel' for short, is a prominent, largely online network of individuals who hold extreme misogynistic views that focus on members' perceived inability to find romantic or sexual partners.[113] Themes of the incel community focus on perceived failure and frustration, along with loneliness, anger, and hate.[114]

IMVE Financing Methods

FINTRAC's December 2022 Operational Alert on Terrorist Activity Financing identified three sub-categories of IMVE actors in Canada: lone-actors, cross-border networks, and organized groups.[115]

Lone IMVE actors who conduct terrorist attacks tend to be self-funded, using their savings, employment income, or money from family and friends.[116] Terrorist attacks committed by lone actors tend to be unsophisticated and require limited financing.

[112] CSIS (2023) CSIS Public Report 2022
[113] Centre for Research and Evidence on Security Threats (2021) A Short Introduction To The Involuntary Celibate Sub-Culture; Southern Poverty Law Center (2018) "I laugh at the death of normies": How incels are celebrating the Toronto mass killing; NBC26 (2018) What Is 'Male Supremacy,' According To Southern Poverty Law Center?
[114] BBC (2021) Incels: Inside a dark world of online hate
[115] FINTRAC (2022) *Operational alert: Terrorist activity financing
[116] FINTRAC (2021) Special Bulletin on Ideologically Motivated Violent Extremism: A Terrorist Activity Financing Profile

IMVE Lone Actor Attacks in Canada

Self-financing methods were observed in two prominent terrorist attacks in Canada conducted by lone actors radicalized by IMVE.

In 2020, a 17-year-old male radicalized by the incel ideology killed one woman and injured another at a massage parlour in Toronto using only a sword to conduct the attack.

In 2021, four members of a Muslim family were killed when an individual drove a pickup truck onto a pedestrian crosswalk in London, Ontario. In 2024, the individual was sentenced to life imprisonment for committing first degree murder and attempted murder amounting to terrorism.

Cross-border networks and organized IMVE groups differ from lone actors in their financing. Organized groups often rely on online communities and cross-border networks to raise funds and have been observed to rely on a host of financing methods, including commercial activities, such as merchandise sales; hosting paid events, such as talks and concerts; crowdfunding; charging membership fees; and accepting donations.

Cross-border networks use large MSBs and electronic money transfers to transfer funds, often to third parties in locations of concern for IMVE activity, such as Eastern Europe or other geographic regions where the IMVE group in question is known to operate. Organized groups, in contrast, tend to raise funds through a variety of methods including electronic money transfers, merchandise sales and frequent cash deposits. Some groups have also been known to engage in drug trafficking, weapons trafficking, and theft to fund their operations.

Crowdfunding and social media platforms have been increasingly working to prevent IMVE fundraising across their networks, leading IMVE threat actors to seek alternative funding methods, including sending cash via mail, cheques, or money orders, as well as increasingly turning to cryptocurrency.

Politically Motivated Violent Extremism

PMVE encourages the use of violence to establish new political systems, or new structures and norms within existing systems. While PMVE may include religious elements, actors are more focused on political self-determination or representation, rather than racial or ethnic supremacy.[117]

Several terrorist entities listed under the *Criminal Code* in Canada that fall under the PMVE category, such as Hamas, Hezbollah, and the Khalistani violent extremist groups Babbar Khalsa International and the International Sikh Youth Federation, have been observed by law enforcement and intelligence agencies to receive financial support originating from Canada.

FINTRAC's 2022 Operational Alert on Terrorist Activity Financing identified Hezbollah as the second most frequently identified international terrorist entity to receive outgoing Canadian funds.[118]

PMVE Financing Methods

Hamas and Hezbollah are established and well-resourced groups that fall under the PMVE category. These groups use diverse funding methods to sustain their operations, including the abuse of the MSB and banking sectors; use of cryptocurrencies; state financing; abuse of the charitable and NPO sector; and criminal activity.

[117] CSIS (2020) CSIS Public Report 2019
[118] FINTRAC (2022) Operational alert: Terrorist activity financing (canada.ca)

Khalistani extremist groups supporting violent means to establish an independent state within Punjab, India are suspected of raising funds in a number of countries, including Canada. These groups previously had an extensive fundraising network in Canada but now appear to consist of smaller pockets of individuals with allegiance to the cause but seemingly no particular affiliation to a specific group.

Financial sector abuse: Both Hamas and Hezbollah are known to use MSBs, especially IVTS, such as hawalas, to move money across borders. Hezbollah, in particular, is known to use Lebanon's banking sector to maintain their account holdings. A lawsuit in New York court, *Lelchook v. Société Générale de Banque au Liban SAL*, highlights how a now defunct Lebanese bank provided financial services to Hezbollah, including through correspondent banking relationships in the US.[119] Canada's financial sector may also be exposed to risks emanating from correspondent banking relationships with institutions known or suspected of servicing Hezbollah in Lebanon.

Cryptocurrencies: Cryptocurrencies, such as Bitcoin and Tether, have emerged as part of Hamas and Hezbollah financing strategies, although these tend to be low value donations. Both Hamas and Hezbollah use online platforms and social media to solicit donations in the form of cryptocurrencies. Hamas in particular has been an early adapter of cryptocurrencies to raise and move funds, with the group reportedly first beginning to solicit Bitcoin donations in 2019.[120] To convert cryptocurrency into cash, Hamas has used currency exchanges, MSBs, and IVTS in Lebanon, Türkiye, and Syria.[121] However, the full scale and effectiveness with which these groups have successfully been able to raise and use cryptocurrency to support their operations remains unclear.[122]

State sponsorship: State sponsorship, particularly from Iran, is a significant source of revenue for Hamas and Hezbollah, enabling them to maintain their activities. In May 2024, the US Financial Crimes Enforcement Network (FinCEN) issued an Advisory to Financial Institutions to Counter the Financing of Iran-Backed Terrorist Organizations, which provides substantive analysis on the methods Iran uses to circumvent international sanctions to raise and move funds to Hamas and Hezbollah. This includes the sale of oil and weapons, the use of front companies, financial institutions, correspondent banking connections, and cryptocurrencies.[123] Canada has observed similar patterns used by Iran to support Hezbollah and Hamas activities.

Abuse of non-profit and charitable activities: The misuse of the charitable and NPO sectors has been observed as a prominent financing method used by Hamas and Hezbollah. Khalistani violent extremist groups have also been known to use networks to solicit donations from diaspora communities to raise and move funds, including through NPOs. Despite these observations, it is estimated that revenue generation through NPO abuse represents a relatively small percentage of operational budgets of terrorist groups overall.[124] In 2024 the Egmont Group, a united body of 174 Financial Intelligence Units, published an overview of NPO abuse typologies and ways for financial intelligence units to make the best use of international cooperation by sharing financial information and intelligence to enhance detection and achieve better results in disrupting the abuse of NPOs to finance terrorism.[125]

---

[119] JUSTIA (2024) Lelchook v Société Générale de Banque au Liban SAL :: 2024 :: New York Court of Appeals Decisions
[120] TRM (2023) In Wake of Attack on Israel, Understanding How Hamas Uses Crypto
[121] Washington Post (2024) Seeking cash, Hamas turns to allies experienced in 'financial jihad'
[122] Chainalysis (2023) Correcting the Record: Inaccurate Methodologies for Estimating Cryptocurrency's Role in Terrorism Financing; Elliptic (2023) Setting the record straight on crypto crowdfunding by Hamas
[123] FinCEN (2024) FinCEN Advisory to Financial Institutions to Counter the Financing of Iran-Backed Terrorist Organizations
[124] Insight Monitor (2023) Hamas Fundraising & Revenue-Generation
[125] Egmont Group (2024) Report on FIUs' Role in the Fight against the Abuse of NPOs for TF Activities

Criminal activity: Criminal activity is also a means of financing for PMVE purposes, particularly for Hezbollah which has strong partnerships with international and domestic OCGs. Hezbollah remains a highly active global player in the cocaine, heroin, fentanyl, and captagon trades,[126] with trafficking networks spanning Latin America,[127] Canada, and the US.[128] Hezbollah has also employed trade-based money laundering techniques. For instance, FINTRAC has reported that funds suspected of supporting Hezbollah were sent or received related to the used car trade.[129]American officials have observed Hezbollah buying used cars in North America and shipping them for resale through jurisdictions such as the United Arab Emirates, South Africa, Angola, Côte d'Ivoire, the Democratic Republic of the Congo, Belgium, the United Kingdom, Hong Kong, Tanzania, Kenya, and Yemen, after which the proceeds are transported to Lebanon by way of couriers.[130] The Port of Montréal is a known link where luxury vehicles are shipped to Lebanon, financially supporting Hezbollah.

Religiously Motivated Violent Extremism

RMVE encourages the use of violence as part of a spiritual struggle against a perceived immoral system. Followers believe that salvation can only be achieved through violence. Many of the listed entities under the *Criminal Code* terrorist listing regime are captured in the RMVE category. Daesh and the Taliban are identified as the top RMVE groups that pose terrorist financing threats to Canada. Notably, FINTRAC's 2022 Operational Alert on Terrorist Activity Financing identified Daesh as the most frequently identified international terrorist entity to receive outgoing Canadian funds.[131]

The RMVE threat to Canada increased in 2023 from inspired lone actors who attempted attacks or, in one case, successfully conducted an attack. This escalating trend is expected to continue and is likely to use unsophisticated methods that are largely self-funded. Charismatic RMVE leaders in Canada continue to use international events to amplify their propaganda to radicalize and recruit vulnerable individuals while encouraging both domestic acts of violence and international travel to conflict zones.[132]

RMVE Financing Methods

Daesh and the Taliban are established and well-resourced groups that fall under the RMVE category. While these groups operate in different contexts that present distinct terrorist financing challenges, both groups use diverse funding methods to sustain their operations, including reliance on international financing networks, drug trafficking, cash smuggling, exploitation of humanitarian appeals, and IVTS. These groups also rely on money laundering techniques and professional money laundering services, including proxies, layering, and cash smuggling to obfuscate the origin of funds.[133]

[126] RUSI (2024) Syria, Captagon and Geopolitics: From Magic Bullet to Placebo
[127] OilPrice.com (2024) How Hezbollah Is Exploiting Cocaine, Corruption, and Chaos in Venezuela
[128] Global News (2019) From Colombia to Lebanon to Toronto: How a DEA probe uncovered Hezbollah's Canadian money laundering ops
[129] The Washington Institute (2020) The DEA's Targeting of Hezbollah's Global Criminal Support Network; FINTRAC (2022) Operational alert: Terrorist activity financing
[130] US Department of Treasury (2023) Treasury Disrupts International Money Laundering and Sanctions Evasion Network Supporting Hizballah Financier; United States House of Representatives House Committee on Foreign Affairs (2017) Attacking Hezbollah's Financial Network: Policy Options. Statement of Derek S. Maltz
[131] FINTRAC (2022) Operational alert: Terrorist activity financing
[132] CSIS (2023) Public Report
[133] RUSI (2023) The Islamic State in Afghanistan: A Golden Opportunity for a 'Golden Child'

As the de facto authorities of Afghanistan since 2021, the Taliban are in control of the national economy, including revenue generation through taxes, customs tariffs, and government agency fees collected in return for services provided. Furthermore, Afghanistan under the Taliban has once again become a safe haven for transnational terrorist groups, including groups with linkages to Canada. The Taliban operates largely in Afghanistan and are known to use front companies and cash storage sites around the world, including in Dubai.[134]

In comparison, Daesh, once concentrated in Syria and Iraq, has splintered and spread-out, adopting more localized strategies to finance operations globally through its so-called 'provinces'.[135] The Taliban and Daesh are both known to rely heavily on IVTS as a means to move and obscure funds. From Canada, Iraq, Lebanon, Pakistan, Syria, Türkiye, United Arab Emirates, and Yemen are the most likely locations where funds or goods would be received. [136]

RMVE actors, particularly Daesh, also inspire foreign terrorist fighters to travel overseas and support their cause. However, there has been a sharp decline in the number of foreign terrorist fighters, including Canadian extremist travelers, since the collapse of Daesh's so-called territorial caliphate in 2019. The scale of funds to support foreign fighter travel has thus decreased in line with fewer individuals participating in offshore conflicts. For those Canadians who do attempt to travel overseas, Canadian law enforcement and intelligence agencies have tools to monitor and lay relevant terrorism charges from the *Criminal Code*.

Enforcement Action Spotlight: Terrorist Financing

In 2022 the RCMP arrested a Canadian citizen upon their arrival to Canada, after the individual, along with their children and another adult, were released from a camp for Daesh detainees in Syria. The individual had been the subject of an investigation by the Integrated National Security Enforcement Team since November 2014. Pursuant to the *Criminal Code*, four terrorism charges were laid including one terrorism financing charge.[137]

In 2023, a Toronto resident was charged by the RCMP Integrated National Security Enforcement Team for their role in raising funds for Daesh. The individual was alleged to have helped raise funds for Daesh fighters through crowdfunding. The investigation further revealed that the individual made and disseminated pro-Islamic State propaganda on social media for the purposes of radicalizing and recruiting people to the terrorist group. It is alleged that the individual also conspired with an overseas member of the Islamic State to commit terrorist attacks against foreign embassies in Afghanistan as well as providing propaganda and research related to attacks conducted in Afghanistan against foreign nationals.[138]

[134] LAWFARE (2021) The Challenges of Understanding Taliban Finance; US Department of Treasury (2024) Fact Sheet: Countering ISIS Financing
[135] The Insider (2024) You name it, we've got it: Exploring the finances of the ISIS, Hamas, and Hezbollah terrorist empires
[136] FINTRAC (2022) Operational alert: Terrorist activity financing
[137] RCMP (2022) Arrest of Canadian citizen returning from Syria
[138] RCMP (2023) Charges laid against Islamic State financier in Canada's terrorist financing investigation

While the Taliban are less likely to use cryptocurrencies, Daesh has been increasingly leveraging this financing tool, with funds solicited through social media platforms, including Telegram, WhatsApp, and Facebook, but to a lesser degree than traditional methods, like hawalas and other types of MSBs.[139] For example, Daesh-West Africa has been observed making payments using Tether[140] and Daesh factions in Somalia regularly channel tens of thousands of dollars back to the Middle East via cryptocurrency each month.[141] Canada has also seen Daesh exploit conflicts, natural disasters, and humanitarian appeals to solicit cryptocurrency donations, from both unwitting and witting donors. In particular, Daesh has exploited the dire humanitarian and security conditions in displaced persons camps in Northeast Syria.[142]

Mitigating Canada's Terrorist Financing Threats

Combatting terrorist financing requires a multifaceted approach with collaboration between governments at the federal, provincial, territorial, and municipal levels, the private sector, and civil society. Canada's legislative and regulatory framework sets out obligations to safeguard the integrity of Canada's financial system from terrorist financing abuse.

Canada maintains a robust anti-terrorism and anti-terrorist financing policy response informed by a comprehensive legislative framework and various policy and operational programs. The legislative and regulatory framework is informed by several federal statutes, including the PCMLTFA, *Anti-terrorism Act, Criminal Code,* and *Income Tax Act*. Various regulations, including the *Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism* and the United Nations Security Council Resolution 1267 on *Taliban, ISIL (Daesh) and Al-Qaida,* also inform the framework.

Terrorism financing offences

It is an offence for any person in Canada or any Canadian abroad to knowingly deal in property, including funds, owned or controlled by a listed terrorist entity. Under subsection 83.1(1) of the *Criminal Code,* and subsection 8(1) of the *Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism,* the existence of any property in the possession or control of a person in Canada or Canadian abroad that they know is owned or controlled by or on behalf of a listed terrorist entity must be disclosed without delay to the RCMP or to CSIS, along with information about any transactions or attempted transactions in respect of that property.

Under the PCMLTFA and associated Regulations, reporting entities are also required to report terrorist

Quick Definitions

Criminal Code Terrorist Financing Offences

Sections 83.02 to 83.04 of the *Criminal Code* are Canada's core terrorist financing offences. Under these sections, it is an offence to provide, collect, make available, use or possess property or services for terrorist purposes, knowing that they will be used, or intending that they be used, in whole or in part for terrorist activity or to benefit a terrorist group.

"Terrorist group" is defined in the *Criminal Code* to include a listed entity. "Entity" includes a person, group, or

[139] Homeland Security Today (2023) ISIS-Affiliated Financial Networks Double Down on Efforts to Exfiltrate Loyalists, Particularly Young Boys, from Camp Al-Hol
[140] US Department of Treasury (2024) Fact Sheet: Countering ISIS Financing
[141] The Insider (2024) You name it, we've got it: Exploring the finances of the ISIS, Hamas, and Hezbollah terrorist empires
cted_2022_cft_gaps_assessment_final.pdf (un.org); Insight Monitor (2024) Financing Terrorism throughout Africa: ISIL Somalia and the Al-Karrar Office
[142] Combatting Terrorism Center (2021) Cash Camps: Financing Detainee Activities in Al-Hol and Roj Camps

property in their possession to FINTRAC.[143] Reporting entities must also file suspicious transaction reports to FINTRAC if they have reasonable grounds to suspect that a transaction or attempted transaction is related to the commission of a terrorist activity financing offence.[144]

To facilitate the delivery of humanitarian assistance in terrorist-controlled areas, Parliament amended the *Criminal Code* in 2023 to establish a statutory exception to criminal liability for humanitarian assistance (subsection 83.03(4)). The amendments also established an authorization regime to shield Canadians from criminal liability where the provision of international assistance and other needed activities would incur an incidental but unavoidable benefit to a terrorist group.[145]

Response to Foreign Terrorist Fighters

Canadian extremist travelers are individuals with a nexus to Canada through citizenship, permanent residency, or a valid visa, who are suspected of having travelled abroad to engage in terrorism-related activities. These individuals may leave Canada to support, facilitate, or participate in violent extremist activities.

Since 2001, at least 200 Canadian extremist travellers[146] journeyed overseas to join or support Daesh and other terrorist groups in Afghanistan, Pakistan, and parts of north and east Africa. For those who return home, Canadian authorities have the mandate to pursue criminal prosecutions, or other threat reduction methods. Several *Criminal Code* offences related to leaving or attempting to leave Canada for the purposes of committing certain terrorism offences were enacted in the *Criminal Code* in 2013.

Since 2013, 17 Canadian individuals have been charged with travel-related terrorism offences and seven individuals have been convicted. Charges have also been laid in six other cases, involving nine individuals not currently in Canada. In early 2023, the Government of Canada repatriated six Canadian women and their children from camps in northeast Syria, with a further six Canadian children repatriated from the region in 2024. CSIS disclosed information that supported the RCMP's investigative efforts and led to PPSC's ability to press charges and issue peace bonds upon the individuals' return to Canada.

Canada deploys a variety of tools to ensure individuals do not travel to conduct terrorist or violent extremist activities abroad, including the Canadian Passport Order, Terrorism Peace Bonds, or listing under the *Secure Air Travel Act*. In the event individuals do travel, Canadian authorities take efforts to monitor their threat-related activities while abroad, as well as upon their return to Canada, to mitigate the threat they may pose.

The government also works with provincial authorities, NPOs, and social services to facilitate rehabilitation and reintegration where possible. The Canada Centre for Community Engagement and the Prevention of Violence, housed in Public Safety Canada, funds initiatives for front-line workers to support the disengagement of extremist travelers and their families from violent extremist ideologies.[147]

[143] FINTRAC (2025) Reporting terrorist property to FINTRAC
[144] FINTRAC (2024) Reporting suspicious transactions to FINTRAC
[145] Public Safety Canada (2024) About the authorization regime and humanitarian exception
[146] National Security and Intelligence Committee of Parliamentarians (2020) Annual Report
[147] Public Safety Canada (2023) Canada Centre for Community Engagement and Prevention of Violence

Chapter 5: Assessment of Money Laundering and Terrorist Financing Vulnerabilities

Overview

A broad range of financial and non-financial businesses and services in Canada are exposed to money laundering and terrorist financing risks, with large banks, MSBs, crypto assets, and certain corporations and express trusts assessed as being the most vulnerable. The assessment of inherent sector and product vulnerabilities remains largely stable since 2023. Many of the changes in vulnerabilities are technology driven, for example by crypto assets, crowdfunding platforms, and online casinos, where risks are more rapidly evolving and increasing overall. Most of the sectors assessed as posing the highest vulnerabilities are subject to robust mitigation measures, including regulation, supervision, and enforcement.

Business sectors, professions, corporate structures, and financial products were assessed using the following criteria:

1. *Inherent Characteristics:* the extent of the sector or profession's economic significance, complexity of operating structure, integration with other sectors, and scope and accessibility of operations to clients.
2. *Nature of Products and Services*: the nature and extent of the vulnerable products and services offered by the sector or profession and the volume, velocity, and frequency of client transactions associated with these products and services.
3. *Nature of Business Relationships*: the extent of transactional versus ongoing business, direct versus indirect business relationships, and exposure to high-risk clients such as PEPs or other clients assessed to be high-risk in the sectoral context.
4. *Geographic Reach*: the exposure to jurisdictions identified as high-risk by the FATF and other locations of concern.
5. *Nature of Delivery Channels:* the extent to which the delivery of products and services can be conducted anonymously (i.e., use of face-to-face and/or non-face-to-face identity verification methods, use of third parties) and with complexity (e.g., multiple intermediaries with few immediate controls).

Ratings of "low," "medium," "high" or "very high' were applied to each rating criterion, with individual ratings then aggregated to arrive at an overall rating for each business sector, profession, or product. While the vulnerability dynamic for each assessed area is unique, the characteristics of each vulnerability rating is summarized in Table 7.

Table 7

Inherent Vulnerability Ratings

Very High	Sector or profession has a very high volume, velocity and/or value of transactions and assets under management, offers a large variety of vulnerable products and services, is integrated with many other vulnerable sectors and is highly accessible by Canadian and international clients. Business relationships are highly transactional, include higher-risk clients, such as PEPs, cash-intensive businesses or complex corporate entities. Sector or profession conducts significant cross-border transactions, including to high-risk jurisdictions and/or often uses complex delivery channels that offer a high degree of anonymity.
High	Sector or profession has a high volume, velocity and/or value of transactions and assets under management, offers some vulnerable products and services, is integrated with some other vulnerable sectors and is highly accessible throughout Canada. Business relationships can be transactional, include higher-risk clients, such as PEPs, cash-intensive businesses or complex corporate entities. Sector or profession often conducts cross-border transactions, including to high-risk jurisdictions, and/or may use complex delivery channels that offer a high degree of anonymity.
Medium	Sector or profession has a low volume, velocity and/or value of transactions and assets under management, offers a few vulnerable products and services, may be integrated with a few other vulnerable sectors, and somewhat limited location of operations. Business relationships are largely ongoing and direct, rarely include higher-risk clients, such as PEPs, cash-intensive businesses or complex corporate entities. Sector or profession conducts limited cross-border transactions, with limited exposure to high-risk jurisdictions, and/or occasionally use complex delivery channels that offer a high degree of anonymity.
Low	Sector or profession has a low volume, velocity and/or value of transactions and assets under management, offers limited services, including limited cash transactions. Business relationships are almost entirely ongoing and direct, rarely or never include higher-risk clients, such as PEPs, cash-intensive businesses or complex corporate entities. Sector or profession conducts exclusively domestic transactions, with no exposure to high-risk jurisdictions, and/or rarely or never uses complex delivery channels that offer a high degree of anonymity.

The 2025 Report discusses sectors and products rated from “very high” to “medium” in terms of their inherent vulnerability to money laundering and terrorist financing, as these represent the segments of the Canadian economy most susceptible to misuse. The top sectors and products with elevated risk are categorized as “very high” or “high” to reflect the differences in materiality such as sector size, transaction volume, and product diversity.

Sectors and products with low vulnerability are still assessed under Canada’s AML/ATF Regime but are not

highlighted in the Report.

Table 8
Overall ML/TF Vulnerability Rating Results

Very High Vulnerability Rating	
Corporations*	Express Trusts*
Domestic Systemically Important Banks (D-SIBs)	Money Services Businesses (MSBs)
	Crypto Assets
High Vulnerability Rating	
Armoured Car Companies	Lawyers & Québec Notaries
Brick-and-Mortar & Online Casinos	Mortgage Lenders
Credit Unions & Caisses Populaires	Other Domestic Banks
Crowdfunding Platforms	Payment Service Providers
Dealers in Precious Metals & Stones	Real Estate Brokers, Sales Representatives & Developers
Foreign Bank Branches	
Foreign Bank Subsidiaries	Securities Dealers
Import/Export Companies	Trust & Loan Companies
Medium Vulnerability Rating	
Accountants	Financing & Leasing Companies
British Columbia Notaries	Life Insurance Companies
Cheque Cashing Businesses	Mortgage Brokers
Company Service Providers	Non-Profit Organizations
Customs Brokerages & Freight Forwarders	Partnerships*
Factoring Companies	White-Label ATMs

* The vulnerability relates to the ability of these entities to be used to conceal beneficial ownership, therefore facilitating the disguise and conversion of illicit proceeds.

Mitigating Canada's Inherent Money Laundering and Terrorist Financing Vulnerabilities

The 2025 Report builds on the analyses published in 2015 and 2023 to include the application of a 'residual risk lens' to the assessment of Canada's inherent money laundering and terrorist financing vulnerabilities. This update highlights the mitigating measures taken to address vulnerabilities for each assessed sector and product along three criteria: the legislative and regulatory framework, the supervisory and enforcement response, and private sector engagement.

Legislative and regulatory framework

Canada maintains a robust AML/ATF legislative framework which consists of several federal statutes, including the PCMLTFA and the *Criminal Code*. This framework is supported by regulations and guidance and implements treaties and conventions that shape international efforts to combat money laundering, terrorist financing, and the proliferation of weapons of mass destruction. Other federal statutes, such as the *Bank Act, Canada Business Corporations Act*, and *Income Tax Act,* complement the federal AML/ATF

framework and contribute to deterring illegal activities in specific sectors. Provincial and territorial legislative and regulatory frameworks are also complementary and deter illegal activities.

The PCMLTFA identifies the business sectors and professions subject to federal AML/ATF legislative and regulatory requirements, referred to as "reporting entities", and establishes FINTRAC as Canada's AML/ATF supervisor and financial intelligence unit.

PCMLTFA reporting entities include:

- Financial entities, such as banks, savings and credit unions, and trust and loan companies;
- Life insurance companies, brokers, and agents;
- Securities dealers;
- MSBs, including virtual currency dealers and armoured car companies;
- Accountants and accounting firms;
- Casinos;
- BC notary corporations and notaries public;
- Real estate brokers, sales representatives, and developers;
- Mortgage administrators, brokers, and lenders; and
- Dealers in precious metals and stones.

In 2025 the scope of reporting entities covered by the PCMLTFA will expand to additional sectors assessed as posing heightened vulnerabilities to money laundering and terrorist financing. Notably, factoring companies, financing and leasing companies, and cheque cashing businesses became covered as reporting entities as of April 1, 2025. Title insurers and white label ATM acquirers will also be subject to the PCMLTFA as of October 1, 2025.

While precise obligations vary from industry to industry, the PCMLTFA imposes four fundamental requirements. First, reporting entities are required to fulfill client due diligence requirements to ensure they have a sound understanding of who their client is in advance of performing certain financial activities or opening an account. This includes requirements for client identity verification, business relationships, ongoing monitoring, beneficial ownership, third-party identification, and PEP assessment.

Second, reporting entities are required to maintain certain records related to the services provided to clients. For instance, deposit taking financial entities, such as banks and credit unions, are required to maintain detailed records on the accounts they open, as well as the transactions conducted through those accounts.

Third, reporting entities are required to file transaction reports with FINTRAC in prescribed circumstances. These reports include:

- **Suspicious transaction reports**, which must be filed as soon as practicable where there are reasonable grounds to suspect that a transaction is related to the commission or attempted commission of a money laundering, terrorist financing, or sanctions evasion offence;

- **Listed Person and Entity Property Reports**, which must be filed immediately when a reporting entity is required to make a disclosure under the *Criminal Code* or an order or regulation made under the *United Nations Act*. Additional reporting requirements for property sanctioned under the *Special Economic Measures Act*, and *Justice for Victims of Corrupt Foreign Officials Act (Sergei Magnitsky Law)* will come into force in fall 2025. Reporting entities are in most cases required to notify the RCMP and CSIS if they determine they are in possession of such property.
- **Large cash transaction reports**, which must be filed when a reporting entity receives an amount of $10,000 or more in cash in a single transaction, or in two or more transactions over the course of a 24-hour period;
- **Large virtual currency reports,** which must be filed when a reporting entity receives an amount in virtual currency equivalent to $10,000 or more in a single transaction, or in two or more transactions over the course of a 24-hour period;
- **Electronic funds transfer reports**, which must be filed when a financial entity, MSBs, or casino processes an international funds transfer of $10,000 or more in a single transaction, or in two or more transactions over the course of a 24-hour period; and
- **Casino disbursement reports**, which must be filed when a casino makes a disbursement of $10,000 or more in the course of a single transaction or in two or more transactions within a 24-hour period.

Finally, each reporting entity is required to establish and implement a compliance program. The program must include the development and application of policies and procedures for the reporting entity to assess the risk of a money laundering or terrorist activity financing offence in the course of their activities.

In order to ensure compliance, the PCMLTFA sets out a framework for administrative penalties that can be applied to persons or entities regulated under the Act. Specific violations and classifications of those violations as minor, serious or very serious are set out in associated regulations. Offences and criminal charges for cases of criminal non-compliance are also included in the Act.

Supervisory & Enforcement Response

All reporting entities are supervised by FINTRAC. As part of its core mandate, FINTRAC administers a comprehensive, risk-based supervision program to ensure that businesses fulfill their obligations under the PCMLTFA and associated regulations.

Compliance with the legislation ensures that regulated businesses and professions are mitigating money laundering and terrorist financing risks. It also ensures that FINTRAC receives the information it needs to generate actionable financial intelligence for Canada's law enforcement and national security agencies.

To maximize reporting entity compliance, FINTRAC conducts industry outreach to help regulated businesses better understand their obligations, assesses levels of compliance through examination and other supervisory functions, performs post-assessment follow-ups to ensure that identified compliance gaps are addressed, and/or enforces compliance through the application of different enforcement tools.

FINTRAC also has the legislative authority to disclose information to law enforcement when it suspects on reasonable grounds that the information would be relevant to investigating or prosecuting a criminal non-compliance offence under the PCMLTFA. Disclosures may occur when FINTRAC has identified reporting entity criminal non-compliance, or when it has received voluntary information from law enforcement on criminal non-compliance.[148] In 2023-24, FINTRAC disclosed 14 such cases to law enforcement.[149]

[148] FINTRAC (2024) Criminal Non-Compliance Offences
[149] FINTRAC (2024) Annual Report 2023-24

Other federal regulators, including OSFI, CRA, ISED, and the CBSA, also contribute to Canada's federal AML/ATF supervisory framework, either through the regulation of PCMLTFA reporting entities, or other vulnerable sectors, professions, or products, such as NPOs, corporations, and import/export companies.

Provincial and territorial regulators, such as securities regulators, as well as several self-regulatory organizations, including those governing the legal profession, contribute to the oversight framework for Canada's vulnerable businesses and professions.

Private Sector Engagement

The private sector has a frontline role in preventing and detecting money laundering and terrorist financing. There are over 38,000 reporting entities subject to supervision by FINTRAC. Many of these businesses and professions take extra steps to combat money laundering and its predicate crimes including by collaborating with government to assist in the identification of potential threats, uncovering broader financial connections, and providing intelligence to advance national investigations either through public-private partnerships, or through various public-private working groups.

Feedback from the private sector and other stakeholders helps ensure that Canada's AML/ATF framework remains effective. The government seeks feedback from the private sector in various ways, including through the ACMLTF and its working groups, as well as through public consultation processes. The CRA's Advisory Committee on the Charitable Sector also assesses the National Risk Assessment methodologies, taking into account the sector's diversity and efforts to mitigate terrorist financing risks, and reports its findings to the Minister of National Revenue.

Most of these businesses and professions coordinate their AML/ATF efforts through industry associations. In addition to serving as a central point of contact for engaging government, these associations can play a key role in creating industry codes of conduct or risk assessments to assist their members in complying with PCMLTFA requirements.

Although the legal sector is not subject to PCMLTFA requirements, it has also been proactive in its engagement with government on matters related to financial crime. The Federation of Law Societies of Canada (FLSC) has co-chaired a joint working group with Finance Canada since 2019. The FLSC also publishes AML/ATF-related guidance and risk assessments on its public website.[150]

Discussion of the Results of the Vulnerabilities Assessment

Financial Entities

The IMF has assessed Canada to have one of the largest and most developed financial systems in the world. Financial entities in Canada include both federally regulated financial institutions, including banks, trust and loan companies, insurance companies, and credit unions, and smaller financial entity sectors, including factoring companies and financing and leasing companies. This section also provides an assessment of the money laundering and terrorist financing vulnerability posed by open-loop prepaid cards, which are generally issued by financial entities.

ML/TF Vulnerabilities of D-SIBs (Very High) and Other Domestic Banks (High): Canada's financial system is highly concentrated, with 36 Canadian-incorporated domestic banks, including the 'Big Six' D-SIBs as of April 2025. The D-SIBs have a significant presence in the Canadian financial sector in terms of transaction volume, asset holdings, and scope of operations both domestically and internationally. These

[150] Federation of Law Societies of Canada (Accessed 2025) Fighting Money Laundering and Terrorist Financing

financial conglomerates account for the majority of Canada's financial sector, holding approximately 93 per cent of total banking assets,[151] and are extensively involved in various business lines, including banking, trust and loan activities, insurance, and securities dealing. The D-SIBs are assessed as having a very high level of inherent vulnerability, while other domestic banks face a high level. This difference is due to the D-SIBs' broader geographic reach, greater exposure to high-risk jurisdictions, and more substantial number of cross-border clients.

Domestic banks are full-service institutions that offer a large number of vulnerable products and services, including taking deposits, issuing loans and credit cards, investments and corporate banking. Banks deal with a very high volume, velocity and frequency of transactions, elevating their vulnerability profile. Small and medium banks may use the D-SIBs as intermediaries for cheque clearing and wire-transfer services. The sector is also highly integrated with other sectors, including real estate, financing, and securities.

The sector is highly accessible, with branches and ATM services available across the country depending on the institution. All of these institutions also offer some form of online banking services, while some domestic banks in Canada are entirely online with no physical locations. Domestic banks have global exposure through major correspondent banking relationships and maintain exclusive access to the SWIFT network used for wire transfers. A proportion of operations involve high-risk jurisdictions.

The sector services a wide variety of retail and consumer clients with varying occupations and business types. This very large client base includes high-risk clients, including high net-worth individuals, domestic and foreign PEPs (e.g., heads of state or heads of government; members of the executive council of government or member of a legislature; deputy ministers or equivalent rank), non-residents, and those occupying positions in professions or sectors vulnerable to money laundering and terrorist financing. Banks can offer both transactional and ongoing services to their clientele, though the majority of business relationships are ongoing with accountholders that have been onboarded as clients, facilitating ongoing client due diligence and ongoing monitoring efforts.

Banking services are provided through both face-to-face and non-face-to-face delivery channels that vary in terms of complexity and degree of anonymity afforded to customers. Banks are also vulnerable to money laundering and terrorist financing risk when they are used by third parties and intermediaries, such as legal professionals and accountants, to undertake banking transactions on behalf of their clients.

ML/TF Vulnerabilities of Foreign Bank Subsidiaries (High) and Foreign Bank Branches (High): As of April 2025, there are 15 Canadian-incorporated foreign bank subsidiaries and 29 authorized Canadian branches of foreign banks operating in Canada. Of these 29 foreign bank branches, 27 provide full services, while 2 specialize in lending services only.

Foreign bank subsidiaries are full-service banks regulated under the *Bank Act* that are owned by eligible foreign institutions. The vulnerability of the products and services offered by foreign bank subsidiaries is similar to those offered by domestic banks. Foreign bank subsidiaries are closely integrated with their parent companies, as well as with other banks and sectors within their home jurisdictions. Foreign bank subsidiaries in Canada may rely on third-party outsourcing arrangements more frequently than domestic banks. While some services are provided in-house, foreign bank subsidiaries often outsource others either to domestic bank affiliates or to their affiliates in their home country. Examples of commonly outsourced services include asset management, financial planning, mutual fund investments, estate planning, tax advice, trust services, and other advisory services.

Foreign bank branches are Canadian offices of internationally headquartered banks that have been given

[151] Bank of Canada (2025) The International Exposure of the Canadian Banking System

permission to conduct business in Canada. Foreign bank branches are not incorporated under the *Bank Act* and operate under certain restrictions as they are not considered a separate legal entity in Canada. These branches offer a more limited number of vulnerable products and services than retail banking operations provided by domestic banks and foreign bank subsidiaries.

Foreign bank subsidiaries and branches in Canada offer vulnerable products and services to a broad range of clients. The business relationship involves a combination of transactional and ongoing engagements with clients. A large proportion of clients can be classified as high-risk, such as non-residents who are not present in Canada or are from high-risk jurisdictions, high-net-worth individuals, and domestic and foreign PEPs. Foreign bank subsidiaries often target specific diaspora communities in Canada as well as foreign individuals, which may make them more exposed to foreign PEPs and clients with connections to high-risk jurisdictions.

Some foreign bank subsidiaries or branches offer services exclusively in a non-face-to-face environment. The variation in delivery channels can obscure client identification.

ML/TF Vulnerabilities of Trust and Loan Companies (High): The Canadian trust and loan company sector holds a significant amount of assets under management. As of April 2025, there are 41 trust companies and 12 loan companies in Canada regulated under the federal *Trust and Loan Companies Act*.[152] The sector is well integrated, especially with banks, due to legislative changes and acquisitions that led trust and loan companies to become mostly owned and controlled by banks and other financial institutions. Trust and loan companies that are owned by banks conduct a comparable volume, velocity, and frequency of transactions as large banks. Independent trust and loan companies, or those not controlled by other financial institutions, tend to conduct fewer transactions.

Trust and loan companies provide vulnerable products and services, including deposit-taking, lending, and other traditional banking activities. Federally regulated trust companies can act as trustees for trusts, pension plans, and agency contracts, allowing them to administer estates — an activity that banks are not permitted to undertake. Most trust and loan companies are subsidiaries of D-SIBs and are used by the parent bank for specialized services relating to deposits, wealth management, and investment services. Business transactions are primarily conducted in face-to-face settings, including through a network of brokers and agents.

This sector serves millions of customers, many of whom can be considered high-risk clients, such as non-residents, PEPs, and high-net-worth individuals. The client profile is primarily oriented toward the domestic market but may include individuals located in high-risk jurisdictions that conduct business through a third party. Third parties are often involved in the creation and management of trust accounts, as well as in complex loans and real estate transactions. Trust and loan companies receive considerable exposure to the international market, mostly through their relationship with D-SIBs. The sector maintains inherent vulnerabilities to money laundering and terrorist financing from its complex delivery channels and a moderate level of anonymity, driven by the use of outsourcing services and agents.

ML/TF Vulnerabilities of Life Insurance Companies (Medium): Canada's life insurance sector is composed of domestic and foreign life insurance companies operating in Canada, as well as independent brokers and agents, and generates a large volume of policy-related transactions. As of April 2025, there are 34 Canadian life insurance companies and 22 foreign life insurance companies under OSFI supervision.[153]

Life insurance companies offer a range of products and services, such as insurance, wealth management

[152] OSFI (Accessed 2025) Who we regulate
[153] Ibid.

(investment), and estate planning, and are well integrated with other sectors, including banking. The sector displays a complex operating structure with multiple business lines. While the sector's main products and services are low risk, industry experts have raised concerns that the sector is vulnerable to being co-opted for the integration stage of money laundering where illicit funds are placed into the financial system.

Underwriting practices within the life insurance sector provide greater assurance about a client's profile and financial background. However, in certain cases, it may still be challenging to discern the ultimate source of premium payments. Most policy-related transactions are conducted domestically by policy-owners, but there could be an opportunity for money launderers to funnel illicit funds into certain insurance products to conceal their origins depending on the product's features.

The availability of loans on whole and universal life insurance products may also lead to increased vulnerability, as the cash value can be withdrawn and repaid throughout the lifetime of the certificate as well as single-premium payment. Nevertheless, most loan activities are considered low risk, as they primarily support policy premiums and large expenditures. Instances of excessive loan activity suggestive of money laundering or terrorist financing behavior are rare.

Life insurance companies have ongoing, direct, and primarily face-to-face relationships with their clients, a small percentage of whom are PEPs and other high-risk clients. Within the sector, five Canadian insurers operate foreign branches or subsidiaries outside of Canada.

Life insurance companies rely predominantly on independent brokers and agents to sell their products. Most brokers and agents are representatives of life insurance companies and have little direct integration with other business sectors. Accessibility to services is generally confined to the geographic reach of regional Canadian markets. While some online services exist, they primarily serve to direct clients to local brokers. Given the nature of the products sold by life insurance brokers and agents, it is uncommon for them to involve third parties or utilize anonymous delivery channels. Cross-border clients are rare and are typically managed through life insurance companies. Life insurance brokers and agents are thus assessed to pose a low inherent vulnerability to money laundering and terrorist financing.

The life insurance sector is also supported by intermediary entities, also known as managing general agents, which primarily provide 'back office' support to life insurance companies and life insurance brokers or agents. Managing general agents are not known to interact directly with clients and are therefore less exposed to money laundering and terrorist financing risk than the other types of entities in this sector. Due to this low inherent vulnerability, managing general agents are not subject to the PCMLTFA.

ML/TF Vulnerabilities of Credit Unions and Caisses Populaires (High): The Canadian credit union and caisses populaires sector is significant in terms of assets under management and presence across the country. As of December 2024, there were 185 credit unions operating in Canada (excluding the Desjardins Group), collectively managing $313 billion in assets. Desjardins Group, North America's largest cooperative financial group, on its own operated 204 Caisses Populaires in Ontario and Québec, and managed $381 billion in assets in the same period.[154]

Although the sector's overall size and transaction volume is smaller than that of the banking sector, its business operations are still complex. Credit unions and caisses populaires offer a variety of retail products and services, including chequing accounts, wire transfers, lines of credit, and mortgage lending, that are accessible to a broad range of clients. The sector's primary money laundering and terrorist financing

[154] Canadian Credit Union Association (2024) National Sector Results – Third Quarter 2024

vulnerabilities are associated with international transactions, large or rapid fund movements, risks associated with third-party involvement, and cash transactions.

Credit unions and caisses populaires provide banking services across Canada and can conduct domestic and international wire transfers on behalf of clients that may involve high-risk jurisdictions. Credit unions and caisses populaires serving more rural communities can be exposed to elevated levels of crime and corruption due to geographic isolation and specific challenges associated with these regions. Rural Canada experiences 33 per cent higher crime severity than urban areas, both in volume and seriousness,[155] making it vulnerable to exploitation by organized crime involved in drug trafficking and money laundering.

Some credit unions and caisses populaires provide services to transient workers, enabling them to send remittances to their home countries. Some of these countries may be jurisdictions identified by the FATF as having a high-risk of money laundering and terrorist financing. Nonetheless, when compared to banks, the sector is more domestically oriented, mitigating some of the risks that may be posed by greater geographic exposures. Credit unions and caisses populaires, as a sector, tend to prefer face-to-face interaction in branches, bringing a sense of community and reducing anonymity in their business relationships. However, with more financial institutions offering online services to their clients, larger credit unions and caisses populaires are adopting mobile applications comparable to those offered by banks.

ML/TF Vulnerabilities of Factoring Companies (Medium): Factoring is an exclusively business-to-business financial activity. Factoring companies supply liquidity to a client upfront in exchange for the cash value of a certain amount of the client's accounts receivable (i.e., invoices) to be collected by the factor later, plus commission and fees. This specialized sector consists of approximately 65 companies across Canada. While factoring is the sole line of business for most factoring companies in Canada, over half of the total factoring volume in Canada is attributed to federally regulated financial institutions.

The factoring sector is integrated with the banking and legal sectors which assist in facilitating transactions and contract formation. The sector is limited in its ability to directly transfer funds internationally. Most factoring transactions are completed via cheque and electronic funds transfers in large amounts, with limited availability for cash use. Clientele are predominantly large sophisticated corporate entities, although small and medium-sized businesses are increasingly using factoring services. The business-to-business nature of this sector can be exploited by bad actors utilizing complex ownership structures to obscure their ultimate beneficial owner.

As in other sectors, the vulnerabilities specific to the factoring sector can be exacerbated in cases where the company may be criminally controlled leading to collusion between the factoring company and the business from which invoices are purchased.

ML/TF Vulnerabilities of Financing & Leasing Companies (Medium): The financing and leasing sector in Canada is diverse, consisting of more than 220 domestic and international lessors and small independent businesses. Leasing is a process whereby the leasing company allows another party to use an asset, such as equipment or vehicle, for a specified period in exchange for regular payment. A leasing company may be a financial institution or a privately held company that provides leases to individuals and businesses. Approximately 85 per cent of leasing services are conducted by federally regulated financial institutions. The sector provides a range of leasing and financing services to individuals and businesses that can be complex and involve multiple parties across Canada and internationally. The sector is integrated with the banking, automotive, and agricultural sectors, among others.

Leasing arrangements can be offered either directly or indirectly. Under a direct leasing arrangement, a

[155] Statistics Canada (2023) Police-reported crime in rural and urban areas in the Canadian provinces, 2021

vendor or lessor offers leasing as a financing option and has an internal department that oversees the agreement. Under an indirect leasing arrangement, a financial intermediary or leasing company purchases an asset from a vendor and allows the lessee to use the asset during the leasing term and after full payment. The lessee deals directly with the financial intermediary or leasing company. Financing companies can offer a wider range of services than leasing companies and can also operate directly or indirectly with the client. Both direct and indirect financing and leasing arrangements pose known money laundering risks.

Financing and leasing companies allow a variety of payment methods such as pre-authorized debit, cash, electronic funds transfers, money orders, and cheques. Leasing and financing payments can be made with illicit proceeds creating a vulnerability at the integration stage of money laundering.

The sector's activities are both domestic and international, with the level of geographic exposure depending on the specific business model of an individual financing or leasing company. Most asset-based financing and leasing arrangements are domestically focused, while other financing and leasing arrangement types, such as trade and export financing, have more international exposure.

Leasing and financing companies generally have an ongoing business relationship with clients and vendors, reflecting their interest in ensuring that payments are made, and the underlying asset is maintained. This feature is also reflective of the incidence of fraud experienced throughout the sector, which necessitates more in-depth client due diligence and ongoing monitoring than may be observed in other sectors, particularly driven from a loss-prevention perspective.

Criminals are also known to prefer leasing and financing arrangements because they do not incur a loss if the leased asset is seized by law enforcement. There have also been demonstrated cases where OCGs have arranged for the financing of vehicles for street level drug traffickers, partly as a reward and partly to facilitate the drug trade.[156] The financing and leasing of higher value and luxury consumer products, such as motor vehicles, boats, artwork, and other high value items, pose the greatest risk for money laundering amongst the range of services provided by the sector. Financing and leasing arrangements for lower value products, such as most other consumer products (i.e., rent to own furniture, electronics, etc.), are assessed to pose a low risk of money laundering.

Payment Product Spotlight: Open-loop prepaid payment products

Open-loop prepaid payment products are generally issued by federally regulated financial institutions and can be either a physical card or virtual product that can be used almost anywhere that credit or debit cards are accepted. In contrast, closed-loop prepaid payment products are either a physical or virtual prepaid payment product that can only be used to make purchases from a single retail company, affiliated companies (such as those located in a single shopping centre), or other designated locations (e.g., public transit). Closed-loop prepaid payment products are also often referred to as merchant gift cards.

The rate of open-loop prepaid payment product usage by Canadians remains steady but still represents a small fraction of the economy's overall transactions. Notably, the product experienced a substantial drop in ownership between 2017 and 2021 and has remained at lower levels since then. In 2023, open-loop ownership was at 9 per cent, slightly higher than their lowest points in 2021.[157]

Open-loop and closed-loop prepaid payment products present different levels of inherent money

[156] Peter German (2019) Cullen Commission - Dirty Money Report Part 2
[157] Bank of Canada (2024). 2023 Methods-of-Payment Survey Report: The Resilience of Cash

laundering and terrorist financing vulnerability, with open-loop products assessed as being highly vulnerable and closed-loop products as having a lower level of vulnerability. Open-loop prepaid products can be loaded with cash and used as a payment method, be used to withdraw cash, or be transferred person-to-person either in Canada or abroad.

The business relationship with clients is transactional and can involve non-face-to-face transactions. Given the nature of the product, clients can be high-risk, including those in vulnerable occupations and businesses. Some open-loop products can be purchased and loaded relatively anonymously while others are reloadable with higher loading limits and require proof of identification. While prepaid payment products are relatively portable across borders, the environment for issuing them in Canada has evolved and there is reduced anonymity which reduces the risk they pose.

Regulatory, Supervisory & Enforcement Response

Financial entities, including banks, credit unions, caisses populaires, trust and loan companies, and life insurance companies, brokers and agents, have long been subject to AML/ATF regulatory controls under the PCMLTFA and supervision by FINTRAC. Financial entities issuing open-loop prepaid payment products are also subject to extensive record keeping and customer due diligence requirements for these products similar to when they open a bank account.

Factoring companies and financing and leasing companies became subject to the PCMLTFA and FINTRAC supervision as of April 1, 2025. Extending the PCMLTFA to cover businesses that exclusively offer factoring and financing and leasing services closed a regulatory loophole and leveled the regulatory playing field in Canada. Federally regulated financial institutions offering a large volume of the services in these sectors had already been subject to Canada's AML/ATF legislative framework.

The broad geographic reach and international connectivity of Canadian financial entities requires collaboration of supervisory activity across borders. FINTRAC prioritizes effective collaboration and cooperation with foreign regulators through its supervisory strategy. FINTRAC has memoranda of understanding (MOUs) with foreign AML/ATF supervisors and regulators, including several in the US. The Compliance MOU between FINTRAC and FinCEN, the US AML/ATF supervisor and financial intelligence unit, has been in place for mutually beneficial information sharing since 2011. FINTRAC also formalized its cross-border cooperation with US banking supervisors in September 2024, when it signed a multilateral Statement of Cooperation with the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation. This agreement allows for the sharing of mutually advantageous information related to money laundering and terrorist financing, and other illicit financial activities, to facilitate the carrying out of their respective duties on the supervision of cross-border financial institutions.

Domestically, financial entities are subject to extensive oversight and control through various federal statutes in addition to the PCMLTFA, including the *Bank Act, Trust and Loan Companies Act*, *Insurance Companies Act, Co-operative Credit Associations Act*, *Financial Consumer Agency of Canada Act*, *Canada Deposit Insurance Corporation Act*, and the *Personal Information Protection and Electronic Documents Act*. All financial entities operating in Canada are also required to identify property subject to sanction under the *Special Economic Measures Act*, *United Nations Act*, and *Justice for Victims of Corrupt Foreign Officials Act* (Sergei Magnitsky Law). This extensive regulatory framework complements the federal AML/ATF Regime or otherwise deters illegal activities across the sector.

Financial entities in Canada are overseen by several federal regulators. OSFI is Canada's prudential supervisor mandated to contribute to the public confidence in the Canadian financial system by

regulating all Canadian banks, federally incorporated trust and loan companies, insurance companies, fraternal benefit companies, and private pension plans. OSFI supports the AML/ATF Regime through its prudential oversight of money laundering and terrorist financing risks that could affect the financial soundness of the entities they regulate. OSFI issued the Regulatory Compliance Management (RCM) Guideline, requiring banks to establish RCM frameworks to ensure compliance with regulatory requirements. These frameworks are intended to enable federally regulated financial institutions, like banks, to apply a risk-based approach for identifying, assessing, communicating, managing, and mitigating regulatory compliance risk.

The Financial Consumer Agency of Canada (FCAC) administers sections of the *Bank Act* and the *Trust and Loan Companies Act* that have been designated as consumer provisions, ensuring compliance with consumer protection measures. The Bank of Canada promotes the economic and financial welfare of Canada by fostering a stable and efficient financial system. Under the authority of Canada's *Payment Clearing and Settlement Act*, the Bank of Canada conducts regulatory oversight for designated financial market infrastructures (FMIs) and acts as the resolution authority for domestic designated FMIs. The Office of the Privacy Commissioner of Canada enforces compliance with privacy legislation.

Credit unions in Canada are either provincially or federally regulated. The provinces have their own legislation that establishes the legal framework for the operation and oversight of credit unions.

Financial entities are engaged in various government collaborative fora at the federal level, including the ACMLTF led by Finance Canada, which provides both the government and private industry with a venue to share information on emerging money laundering and terrorist financing risks, trends, and mitigation measures. They are also well represented by various industry associations, including the Canadian Bankers Association, Canadian Credit Union Association, the Small Bank Forum, and the Canadian Life and Health Insurance Association. Industry associations provide their members with information, research, and operational support, while also collaborating with governments, regulatory bodies, and law enforcement agencies to raise awareness and combat financial crime.

Financial entities play a key role in deterring criminals and terrorists from operating in the legitimate economy. Canadian banks, in particular, are FINTRAC's largest reporters by volume making them critical sources of the information FINTRAC needs to generate the financial intelligence used by law enforcement to target, disrupt, and dismantle organized crime. Canada's largest banks have assumed leadership roles in public-private partnerships where they work with FINTRAC and other Canadian AML/ATF Regime partners to follow the money to identify potential subjects, uncover broader financial connections, and produce intelligence to support national project-level investigations. These initiatives are resulting in tangible results. In 2023, FINTRAC provided more than 450 disclosures of actionable financial intelligence to law enforcement in relation to its seven public-private partnerships.[158]

FINTRAC has prioritized ensuring the strong compliance of financial entities in the course of their risk-based supervisory activities. Examinations of financial entities undertaken in the 2023-2024 financial year resulted in the largest administrative penalties imposed in FINTRAC's history on several large Canadian banks for serious compliance violations.

[158] FINTRAC (2024) FINTRAC Annual Report 2023-2024

Enforcement Action Spotlight: Bank Accounts

Canadian law enforcement has taken action in cases where criminals have exploited deposit taking financial entities to commit financial crime. Notably, the RCMP and local law enforcement have prioritized restraining criminal's bank accounts involved in laundering the proceeds of crime.

In Project OExplorer, the RCMP, working alongside the London Police Service and CBSA, arrested two male suspects in June 2023 on human trafficking, money laundering, and possession of the proceeds of crime charges while restraining their business's bank account and seizing a number of electronic devices and vehicles as property related to these offences. Investigators also rescued 31 victims who were being criminally exploited by the accused.[159]

In 2022, RCMP's Project Monterey resulted in eight individuals in the Yukon being charged with money laundering and proceeds of crime offences tied to drug trafficking. Approximately $150,000 was seized from one of the suspects' bank accounts with the help of FINTRAC information. In addition, multiple firearms, approximately 528 grams of cocaine, 168 grams of fentanyl, 388 Hydromorphone pills, and 1043 Benzodiazepine pills were seized having a combined street value of over $175,000.[160]

Enforcement Action Spotlight: Financing & Leasing Companies

Law enforcement investigations have identified cases of Canadian financing and leasing companies being fraudulently exploited and used to launder the proceeds of crime. In 2020, a Canadian law enforcement investigation identified a financing company being used to commit fraud and international money laundering. In this case guilty parties used multiple straw buyers and associates to fraudulently finance vehicles and export them internationally for resale.[161]

Securities Sector

ML/TF Vulnerabilities of the Securities Sector (High): Canada's securities sector remains significant in terms of transaction value and volume, as well as assets under management. The sector maintains a complex structure that is well integrated with the banking, legal, and crypto assets sectors. The sector is composed of integrated banking, institutional, and retail level firms. According to the Canadian Securities Administrators (CSA), of the ten largest securities dealers, 94 per cent of the revenue and nearly 90 per cent of assets under management are attributable to dealers owned by Canada's D-SIBs.

The securities sector offers a range of products and services that can be vulnerable to abuse for money laundering and terrorist financing, including tradable financial assets, investment certificates, and mutual funds. While some securities dealers accept cash payments, most transactions are conducted in the form of wire transfers from bank accounts, which are subject to the stringent AML/ATF controls in banks.

[159] RCMP (2023) Police and border services rescue victims of human trafficking ring
[160] RCMP (2022) Yukon RCMP Crime Reduction Unit arrest: speaking notes from media availability on June 8, 2022
[161] RCMP (2020) Alberta RCMP charge three in an international luxury vehicle export fraud

Securities dealers[162] service a wide range of clients, including both domestic and foreign individuals and entities. Most clients maintain an account and ongoing business relationship with the securities dealer. A small portion may be considered high-risk clients, including non-residents of Canada, high-net-worth clients, PEPs, and those engaged in occupations exposed to heightened vulnerabilities to money laundering and terrorist financing. Clients may be trusts or corporations, which may have complex ownership structures for the purpose of obscuring the beneficial owners. The securities sector operates beyond domestic borders and can engage in business within high-risk jurisdictions.

In addition to brick-and-mortar locations supporting face-to-face interaction, securities dealers are also available via online brokerages for tradable financial and crypto assets subject to securities regulations. Traditionally, client onboarding within the securities industry has required face-to-face identity verification. However, the digitalization of the financial sector as a whole has led to a rise in the use of remote identification, allowing for certain know-your-client activities to happen online through the use of recognized software tools. Technology has also enabled order-execution-only firms and automated digital advisory programs (robo-advice) to service clients via mobile or online applications for a lower fee and with little to no human interaction. Online broker firms rely on non-face-to-face identification methods, as do traditional dealers for some clients, but in all cases registered dealers are required to verify the identity of each client.

Regulatory, Supervisory & Enforcement Response

Securities dealers are subject to AML/ATF regulatory controls under the PCMLTFA and supervision by FINTRAC. All categories of registered securities dealers are held to the same client identity verification and due diligence requirements, and regulatory oversight.

The sector is also subject to a robust regulatory framework at the provincial and territorial level, informed by legislation enacted in each jurisdiction and enforced by provincial and territorial securities regulators, and a national self-regulatory organization. These regulatory frameworks add an additional level of scrutiny to the sector, providing protection to investors, enhancing investor confidence, controlling risks, and fostering fair, efficient, and competitive capital markets. Firms or individuals advising on or managing investments, selling securities, and/or trading derivatives in Canada must be registered with the relevant provincial or territorial regulator or their delegate, the Canadian Investment Regulatory Organization.

All securities regulators in Canada share information with each other about securities-related threats for enforcement purposes. Securities regulators in BC, Alberta, Ontario, and Québec, along with other securities regulators around the world, are signatories to memoranda with the International Organization of Securities Commissions, the body that facilitates cross-border collaboration for the purpose of regulatory enforcement regarding securities markets. Canadian securities regulators share compliance and registration-related information with FINTRAC, including through MOUs. FINTRAC is also required to disclose information to provincial securities regulators in cases where it has reached reasonable grounds to suspect that the information would be relevant to investigating or prosecuting an offence under the relevant provincial securities legislation.

[162] For the purposes of the PCMLTFA, a "securities dealer" means a person or entity authorized under provincial legislation to engage in the business of dealing in securities or any other financial instruments or to provide portfolio management or investment advising services. In the securities sector, the terminology varies to denote the category of registration, such as investment dealer and portfolio manager. A registered individual is not a securities dealer, but rather, is authorized to act on behalf of a securities dealer. Investment fund managers are also required to be registered under provincial legislation but rely upon securities dealers to discharge their client identification requirements.

All securities regulators in Canada are members of the CSA, the umbrella organization of provincial and territorial securities regulators dedicated to improving, coordinating, and harmonizing regulation of the Canadian capital markets. CSA working groups focus on disrupting emerging investment fraud, raising public awareness of high-risk threat actors, and exploring new cooperation opportunities with federal agencies to enhance the detection, prosecution, and deterrence of white-collar crime and securities laws violations.

Enforcement Action Spotlight: Securities Sector

Law enforcement, FINTRAC, and securities regulators collaborate on criminal and quasi-criminal investigations. Criminal enforcement action has been taken against individuals operating in the securities sector.

In 2023, the Alberta Securities Commission and the Alberta RCMP Integrated Market Enforcement Team acknowledged FINTRAC's contribution to an investigation of a fraudulent investment scheme that led to a court sentence against an Alberta resident on one count of fraud over $5,000 and one count of laundering the proceeds of crime. The individual was found to have defrauded investors of over $500,000 and sentenced to 4.5 years imprisonment and ordered to pay over $200,000 in restitution to seven investors.[163]

Money Services Businesses

ML/TF Vulnerabilities of the Money Services Businesses Sector (Medium to Very High): The Canadian MSB sector is large and diverse, representing nearly 3,000 businesses as of April 2025 that offer services in various market segments. This includes multi-service retail MSBs, single-service retail MSBs, wholesale or corporate operators, and IVTS. Other MSB market sub-segments, such as cheque cashing businesses, armoured car services, virtual currency dealers, payment service providers, and crowdfunding platforms are addressed in other sections of this chapter.

Although the MSB sector is broadly vulnerable, the degree of vulnerability is not uniform because of variations in size and business models. Two types of MSBs are most vulnerable. The first, retail multi-service MSBs, have the most dominant presence in Canada. Retail multi-service MSBs offer a range of transactional products and services (i.e., wire transfers, currency exchange, and monetary instruments) that are vulnerable to money laundering and terrorist financing. These products and services are widely accessible, and the client profile includes high-risk actors, scuh as PEPs, clientele in vulnerable businesses or occupations, as well as those whose activities are conducted in high-risk jurisdictions.

The second type of highly vulnerable MSB are those that use alternative remittance services, including IVTS, such as *hawalas*, *hundi*, and *fei'chen*. IVTS is characterized by the transfer of value (i.e. remittances) between parties in foreign jurisdictions, without necessarily moving money across borders. Settlement can occur over time through cash, trade, or other means. IVTS MSBs often have geographic and/or cultural ties to correspondent bankers and their clients. IVTS usually serve overseas diasporas and may provide greater access to jurisdictions that are underserved, inaccessible or difficult to access via formal banking channels, provide faster transmission of funds, and/or lower costs to transmit funds. Given the links with the international informal banking sector, these businesses can be somewhat complex.

IVTS activity typically runs parallel to, and independent of, the formal banking system; however, IVTS will

[163] FINTRAC (2024) FINTRAC Annual Report 2023-2024; Alberta Securities Commission (2023) News Release: David Del Bianco Sentenced to 4.5 years in jail for fraud and money laundering

often utilize the formal financial system to absorb funds and settle transactions. Although IVTS can be used for legitimate purposes, such as the provision of remittances to families, they can also be misused by criminal and terrorist groups for money laundering and terrorist financing.[164] IVTS business models can be highly opaque and difficult to track as the settlement of transactions is done through brokers or personal contacts whose ledgers may not be available for scrutiny in Canada.

ML/TF Vulnerabilities of Cheque Cashing Businesses (Medium): Cheque cashing businesses typically employ a simple operating model that offers clients the immediate, hold free, ability to cash a cheque for a fee. There are approximately 600 cheque cashing businesses operating in Canada. While there are some stand-alone cheque cashing businesses, most businesses in the sector provide cheque cashing alongside other cash-related services, such as pay-day loans and tax-rebate discounting. The sector is not highly integrated with other sectors.

Relationships between cheque cashing businesses and their clients can be highly transactional and with no ongoing business relationship. Cashing a cheque typically involves face-to-face interaction and requires clients to provide basic information to facilitate the service. Cheque cashing businesses are generally accessible across Canada, particularly in urban areas where there is a higher demand for such services.

Cheque cashing businesses do not typically service clients in high-risk occupations. Clients using these businesses tend to be under-banked and members of vulnerable populations (i.e., new Canadians, temporary foreign workers, lower income Canadians, and those with poor credit). These clients may pose a slightly higher risk profile if they do not have access to identification documentation issued in Canada.

Cheque cashing can be used to support the layering phase of money laundering, particularly when combined with financial activities undertaken with other business types. Once funds are placed, such as in a bank or a casino, a cheque can be drawn and cashed at a cheque cashing business. This is done to add further distance between the illicit proceeds and their criminal source. There are also various aspects of the cheque cashing business model that makes it vulnerable to fraud. This includes the provision of immediate access to funds (rendering it difficult to reverse a fraudulent transaction after the fact), potential difficulty to detect fraudulent or stolen cheques, vulnerability to identity fraud, and the complexity associated with implementing high-quality client verification processes.

ML/TF Vulnerabilities of Crowdfunding Platforms (High): Crowdfunding is an innovative fundraising solution, used by people from all over the world to raise funds to carry out projects, investments, or other ventures. Usually, these campaigns are operated in conjunction with a dedicated online crowdfunding platform or by initiating informal appeals through social media. Unlike traditional fundraising methods (e.g., loans from financial institutions), crowdfunding platforms allow individuals or groups to appeal for funds directly from members of the public connected online who may be geographically dispersed. As of April 1, 2025, there are over 120 crowdfunding platforms registered to operate in Canada as either MSBs or foreign MSBs under the PCMLTFA.

As a predominately online service, crowdfunding services can quickly allow users to raise funds from large numbers of donors and often across borders. Crowdfunding platforms have extensive geographic reach, including to jurisdictions of concern due to money laundering and/or terrorist financing activity, and there is potential for transactions to involve a high degree of anonymity. Crowdfunding services can be integrated with the financial sector as banks may offer these services directly or hold funds raised via crowdfunding. This sector is also closely integrated with payment service providers to enable the completion of payments involved in a crowdfunding project.

[164] FinCEN (2003) Informal Value Transfer Systems; CTV News (2019) Ancient underground money network flourishes despite more bank regulation

The FATF's 2023 report *Crowdfunding for Terrorism Financing* notes four main ways in which crowdfunding platforms can be abused for terrorism financing purposes.[165] This includes the abuse of humanitarian, charitable or non-profit causes; use of specialized crowdfunding platforms or websites that cater to individuals who have been banned from mainstream platforms; use of social media and messaging apps to amplify and generate momentum for causes; and interaction with cryptocurrency funding options that can enhance anonymity. The FATF identifies donation-based crowdfunding as most likely to be exploited for terrorist financing or violent extremism purposes.

ML/TF Vulnerabilities of Payment Service Providers (High): The term "payment service provider" refers to a diverse group of persons or entities that perform various payment functions as a service or business activity. Payment functions include the provision and maintenance of a payment account; holding of funds; payment initiation; payment authorization and transmission; and clearing and settlement. As of April 1, 2025, there are approximately 1,000 payment service providers registered to operate in Canada as either an MSB or foreign MSB under the PCMLTFA.

Payment service providers can help merchants accept payments from customers by connecting them to payment networks for purposes of authorizing, clearing, and settling transactions. They can also provide the technology, hardware, and services that enable a merchant to accept a variety of payment methods, including credit cards, debit cards, digital e-wallets, and bank-to-bank payments. Payment service providers also include businesses that provide invoice payment services when they act as an intermediary between a payer and a payee to make payments with respect to invoices, such as those pertaining to utilities, payroll and commission, mortgage and rent, and tuition.

Money laundering typologies associated with payment service providers include blending funds, smurfing, invoice fraud, and the use of offshore accounts to hide beneficial owners. The misuse of payment service providers is similar to other layering methods and can include the use of front companies, which use legitimate businesses to cover for criminal activity, and pass through companies, which provide criminal actors access to a legitimate company's payment processing accounts to process credit card payments. Payment service providers are also known to be vulnerable to the use of funnel accounts, which accept credit card charges from multiple companies that do not own their own merchant payment account. Under this typology, the funnel company enters the payments as legitimate transactions to the card payment processing system.

Payment service providers can be used to make payments and transfer funds domestically as well as internationally, and as such have the potential to reach high-risk jurisdictions.

ML/TF Vulnerabilities of White Label ATMs (Medium): White label automated teller machines (WLATMs) are ATM cash machines that are not owned by banks or credit unions and connect to payment networks through intermediary companies known as "acquirers." Of the approximately 70,000 ATMs in Canada, roughly 50,000 are WLATMs. These machines are often located in high-traffic locations, such as bars, convenience stores, and restaurants. With the exception of those operated in the province of Québec, there are no restrictions on who may own or operate a WLATM. The sector's business model is relatively complex, including payment network connectors, ATM sellers, WLATM owners/operators, and end users, and is integrated with the financial sector, payment network providers, and armoured car services.

[165] FATF (2023) Crowdfunding for Terrorism Financing

While WLATMs can only be used for cash withdrawals, the critical vulnerability posed by the sector is their capacity to be owned, operated, or controlled by criminals, who can load the WLATMs with large amounts of illicit proceeds. As WLATM users withdraw criminal proceeds from the WLATM, the WLATM owner receives "clean" money from financial institutions as transactions settle electronically. In addition, given that WLATMs are located in less monitored locations, criminals may be inclined to use them to withdraw funds using stolen payment cards.

***ML/TF Vulnerabilities of Armoured Car Companies (High)*:** Armoured car companies are primarily used by financial institutions and businesses to securely transport cash, monetary instruments, and valuable goods. As of April 2025, there are approximately 20 armoured car companies active in Canada, with the largest players having global reach. The sector is highly integrated with other sectors that are vulnerable to money laundering and terrorist financing, including financial institutions, dealers in precious metals and stones (DPMS), MSBs, and cash intensive businesses, and the geographic footprint of some armoured car operators is vast.

The armoured car sector's scale of operations and the cash-intensive nature of the businesses they serve can allow them to play a role in obscuring the origin of funds. For instance, the cash logistics and cash management services offered by armoured car companies involve the collection of funds, which can then be pooled into a central account, possibly obscuring the origin of funds. Armoured car companies can also be used as a secure storage solution for cash and other valuables outside the formal banking sector. This can make reconciling and determining the source of funds managed by these businesses challenging. These features also make armoured car companies particularly attractive for OCGs and criminals that control, or wish to use, cash intensive businesses as a means of laundering cash.

While the movement of money between financial institutions presents lower concern, an important part of the client profile for armoured car companies includes a combination of transactional and third-party business relationships. Companies in this sector transport the funds of cash-intensive businesses; load and replenish WLATMs; transport currency and monetary instruments on behalf of DPMS and MSBs; and otherwise carry out transactions with a range of originators and destinations, such as financial institution accounts or private businesses.

Regulatory, Supervisory & Enforcement Response

MSBs are subject to AML/ATF regulatory controls under the PCMLTFA and supervision by FINTRAC. The scope of coverage of MSB activities under the PCMLTFA has expanded in recent years. This includes the addition of virtual currency dealers and foreign MSBs to the Regime in 2020, crowdfunding platforms and payment service providers in 2022, the armoured car sector in 2024, and cheque cashing businesses in April 2025. WLATM acquirers will also be regulated as MSBs as of October 1, 2025.

All MSBs must register with FINTRAC. Approximately 3,000 MSBs were registered as of April 1, 2025. Individuals convicted of certain offences under, among other statutes, the PCMLTFA, the *Controlled Drugs and Substances Act,* or the *Criminal Code* are ineligible for registration. The government has introduced various additional measures to prevent the criminal abuse of MSBs in recent years. A new criminal offence for the operation of an unregistered MSB came into force in 2024. Domestic MSBs and their agents will also be subject to criminal record check requirements as of October 2025.

Certain MSBs in Canada are also subject to the *Retail Payment Activities Act* (RPAA), which sets out a federal supervisory framework for payment service providers enforced by the Bank of Canada. The RPAA applies to any business in Canada that performs one or more of the five payment functions identified in the Act as a

service that is not incidental to any non-payment service or business activity. [166] The RPAA regime launched in November 2024 when PSPs were required to submit their applications for registration to the Bank of Canada. The regime will be fully implemented when substantive requirements concerning fund safeguarding and operational risk management come into force in September 2025.

The MSB sector is covered by provincial legislation in Québec and BC, though the breadth of coverage of money services differs between jurisdictions. [167] Responsibility for the administration of the *Money Services Business Act* was transferred to Revenu Québec from the Autorité des marchés financiers in 2021.[168] The Government of BC announced in March 2023 that MSBs active in the province would be subject to oversight by the BC Financial Services Authority. The regulatory framework for this work is outlined in the *Money Services Business Act*, which received Royal Assent in 2023.[169] Regulations are under development to implement the new legislation.

Core MSB services (i.e. foreign exchange dealing, remitting or transmitting funds, issuing negotiable instruments) have been regulated under the PCMLTFA since 2008. These MSB subsectors are subject to a "mature" AML/ATF regulatory framework, and industry level participants are expected to have a strong understanding of their regulatory obligations. However, this same expectation may not be applicable to "newer" MSB sub-sectors, including virtual currency dealers, crowdfunding platforms, payment service providers, the armoured car sector, and cheque cashing businesses.

Members of the MSB sector have varying levels of compliance with the PCMLTFA when assessed by FINTRAC. Top compliance deficiencies include gaps in compliance program policies and procedures, failure to update or provide accurate registration information and, amongst smaller MSBs, non-reporting. When MSBs' reporting is assessed, deficiencies are often cited for quality and timing.

Information on rates of AML/ATF compliance by the crowdfunding and armoured car industries as MSB sub-sectors is limited as the regulations have only newly come into effect. FINTRAC's current supervisory activities associated with these newly regulated sectors are focused on awareness building and fostering strong compliance.

The MSB sector participates in various engagement fora and is represented by the Canadian Money Services Businesses Association at the ACMLTF, led by Finance Canada. This forum provides both the government and private industry with a venue to share information on emerging money laundering and terrorist financing risks, trends, and mitigation measures. Regular engagement between FINTRAC and the MSB sector has fostered a mutual understanding of emerging risks and compliance expectations. Through webinars, conferences, and educational materials, engagement efforts from both FINTRAC and industry has bolstered the sector's approach to risk management, providing businesses with the knowledge and tools necessary to strengthen their compliance capabilities and reinforcing the importance of an effective compliance regime.

---

[166] As per the RPAA, payment function means (a) the provision or maintenance of an account that, in relation to an electronic funds transfer, is held on behalf of one or more end users; (b) the holding of funds on behalf of an end user until they are withdrawn by the end user or transferred to another individual or entity; (c) the initiation of an electronic funds transfer at the request of an end user; (d) the authorization of an electronic funds transfer or the transmission, reception or facilitation of an instruction in relation to an electronic funds transfer; or (e) the provision of clearing or settlement services.

[167] The *Money Services Business Act* in Quebec covers the following "money services:" currency exchange; funds transfer; issuance and redemption of traveller's cheques, money orders or bank drafts; cheque cashing; and the operation of automated teller machines including the leasing of a commercial space intended as a location for an automated teller machine if the lessor is responsible for keeping the machine supplied with cash.

[168] Autorité des marchés financiers (2022) Enforcement Report FY 2021-2022; Revenu Québec (2024) Laws and Regulations administered by Revenu Québec

[169] Government of British Columbia (2023), News Release: Safe money services protect people from money laundering

Enforcement Action Spotlight: Money Services Businesses

Law enforcement has taken various actions to address the money laundering and terrorist financing risks posed by the MSB sector. In 2023 Canadian law enforcement acknowledged FINTRAC's contribution to an investigation that led to charges under the PCMLTFA against two individuals for operating an unregistered MSB. The two individuals made illegal transactions totalling more than $20 million using a scheme to collect and move funds clandestinely from Canada internationally.[170]

Moreover, the MSB sector was identified as a priority financial crime subgroup in the RCMP's Counter Illicit Finance Alliance of BC's (CIFA-BC) 2021-22 Strategic Plan. The MSB financial crime subgroup addresses non-bank entities that offer services to the public including foreign exchange dealing, money transfers, issuing/redeeming money orders, traveler's cheques (or other similar negotiable instruments), and dealings in crypto assets.[171]

Crypto Assets

ML/TF Vulnerabilities of Crypto Assets (Very High): The crypto asset sector is significant, facilitating a large volume of transactions and maintaining a global market capitalization of US$3.26 trillion as of December 31, 2024.[172] A broad range of different types of crypto assets exist, many of which employ complex business models involving a range of participants, including crypto asset exchanges, coin-swap exchanges, DeFi exchanges, and wallet providers.

Businesses that provide virtual currency exchange or transfer services are regulated as virtual currency dealers, a subsector of MSB, under the PCMLTFA. Approximately 1,300 virtual currency dealers are currently registered with FINTRAC. This sector continues to evolve rapidly in terms of services and business/delivery models and is integrated with the Canadian and international financial sectors.

Some crypto asset service providers have a transactional relationship with their clients who can be afforded a relatively high degree of anonymity, with transactions largely being conducted in non-face-to-face settings. Crypto assets have global reach and accessibility, enabling rapid cross-border transfers and exposure to high-risk domestic and foreign clients, as well as high-risk jurisdictions.

The sector provides several vulnerable products and services, including crypto assets, DeFi platforms, initial coin offerings, peer-to-peer transfers, and mixers and tumblers – online services that increase the anonymity and privacy of crypto asset users. Convertible crypto assets continue to be the most vulnerable, largely because they are typically pseudonymous in nature, as well as being highly accessible and transferable.

Crypto assets are purchased and sold through online exchanges, cryptocurrency ATMs or through peer-to-peer platforms. In its 2024 sectoral advisory, *The role of virtual currency automated teller machines in laundering the proceeds of crime*, FINTRAC assessed that cryptocurrency ATMs are becoming a key tool in the placement stage of money laundering, as they have the potential to convert cash into cryptocurrency, or vice versa. The ease, accessibility and pseudo-anonymity of cryptocurrency ATMs are factors that make them susceptible to misuse by criminals.

[170] FINTRAC (2024) FINTRAC Annual Report 2023-2024
[171] Counter-Illicit Finance Alliance (CIFA-BC) (2021): CIFA-BC Annual Report 2021/22
[172] CoinMarketCap (2024) Today's Cryptocurrency Prices by Market Cap - December 31, 2024

The understanding and use of cryptocurrencies as a tool for terrorist and violent extremist groups to raise and move funds has increased over the past five years. Terrorists and criminals have been observed to use cryptocurrencies to obtain proceeds of crime (e.g., by requiring payments related to fraud scams or ransomware attacks to be made in cryptocurrencies) or to distance proceeds from their criminal source.

While Bitcoin has always featured prominently in suspicious transaction reporting, Tether (USDT) is now outpacing Bitcoin as the cryptocurrency of choice, specifically for Daesh and its affiliates. On balance, however, evidence continues to suggest that cryptocurrencies have not replaced terrorist groups' preference to use traditional financial products and services like MSBs, IVTS, and a reliance on cash couriers. This preference is likely in part due to the price volatility of many cryptocurrencies, the limited ability to purchase goods and services with cryptocurrencies, and a lack of infrastructure necessary to exchange cryptocurrencies for fiat currency in some of the jurisdictions where terrorist groups operate.[173]

Regulatory, Supervisory & Enforcement Response

Businesses that offer virtual currency exchange and/or transfer services to Canadians are subject to AML/ATF regulatory controls under the PCMLTFA including requirements to register as an MSB with FINTRAC. This applies to businesses operating inside and outside Canada, so long as they provide services to Canadians. As of April 2025, there are approximately 1,300 virtual currency MSBs registered with FINTRAC.

Additionally, all businesses and professions regulated under the PCMLTFA must submit a large virtual currency transaction report to FINTRAC when they receive virtual currency in an amount equivalent to $10,000 or more in the course of a single transaction, or multiple transactions within a 24-hour period conducted by the same person or entity.

FINTRAC has a strong understanding of cryptocurrencies and assets and actively monitors the money laundering and terrorist financing risks posed by this sector to understand the rapidly evolving landscape. In 2021, FINTRAC published guidance on money laundering and terrorist financing indicators related to virtual currency transactions to help educate reporting entities.[174] Additionally, FINTRAC has published strategic intelligence to help businesses, financial institutions and the public understand and recognize the characteristics of unlawful activity involving cryptocurrency ATMs and the types of individuals and entities that may be involved.[175]

FINTRAC has taken enforcement action against an unregistered foreign virtual currency dealer that it found contravening foreign MSB regulatory obligations under the PCMLTFA. In May 2024 FINTRAC imposed its largest administrative monetary penalty to an MSB to date ($6 million) on a virtual currency dealer for failure to register with FINTRAC as a foreign MSB and for failure to submit large virtual currency transaction reports. The virtual currency dealer has appealed the decision to the Federal Court.[176] The latter violation was determined by FINTRAC using blockchain analytics, highlighting the increasing technological sophistication that FINTRAC employs to supervise virtual currency dealers.

Some crypto asset trading platforms, registered as dealers, are also subject to provincial securities statutes if they facilitate the trading of crypto assets that are securities or derivatives. Such businesses are required to comply with the securities laws of each province or territory in which they offer services and are subject to supervision by the relevant provincial or territorial securities regulator. While many crypto asset trading

[173] US Department of the Treasury (2024) 2024 National Terrorist Financing Risk Assessment
[174] FINTRAC (2021) Money Laundering and Terrorist Financing indicators—Virtual currency transactions
[175] FINTRAC (2024) The role of virtual currency automated teller machines in laundering the proceeds of crime
[176] FINTRAC (2024) FINTRAC imposes an administrative monetary penalty on Binance Holdings Limited

platforms are still registered as restricted dealers, they are expected to transition to become investment dealers and members of the Canadian Investment Regulatory Organization, a self-regulatory organization carrying out regulatory responsibilities under recognition orders from the provincial securities commissions.

Enforcement Action Spotlight: Crypto Assets

Law enforcement has taken various actions to address the money laundering and terrorist financing risks posed by crypto assets, including prioritizing the investigation of crypto asset related crimes and assets forfeiture of crypto assets. For example, between January 1 and July 31, 2024, Saskatchewan RCMP had investigated 116 files involving cryptocurrency fraud, and in total, victims had reported more than $3.4 million in cryptocurrency fraud losses.[177]

In June 2023, RCMP's D Division completed a take-down in relation to Project Decrypt, a drug trafficking and money laundering investigation. The investigation was initiated based on a FINTRAC Voluntary Information Record from a virtual currency dealer and resulted in charges on five individuals and asset seizures over $3 million which included cryptocurrency restraints.[178]

Corporations and Other Legal Persons and Arrangements

This section assesses the money laundering and terrorist financing vulnerabilities posed by legal persons and arrangements, including corporations, partnerships, and express trusts, as well as the company service sector which plays arole in providing incorporation and management services.

ML/TF Vulnerabilities of Corporations (Very High): The Canadian corporate sector is large and complex. According to Corporations Canada there are approximately 4 million Canadian corporations active across the country. Of these, around 15 per cent of Canadian corporations are federally incorporated, with the remainder incorporated provincially or territorially. Although the vast majority of corporations contribute positively to society, certain features of companies can make them vulnerable to misuse for criminal activities, such as money laundering and tax evasion.

In Canada, corporations can be formed quickly, cheaply, and remotely, with or without the assistance of professional intermediaries. Although they are required to have a registered office in a Canadian province or territory, Canadian corporations can be established from anywhere in the world and undertake business globally, including with persons and entities operating in jurisdictions posing high money laundering and terrorist financing risks and/or with a reputation for financial secrecy.

There are limited restrictions on non-resident Canadians owning shares in Canadian corporations or managing Canadian corporations as directors, subject to certain exceptions, such as Canadian residency requirements applicable to directors of federal corporations, Canadian ownership and control requirements to engage in activities in particular business sectors in Canada, and any foreign investment restrictions administered through the provisions of the *Investment Canada Act*.

[177] RCMP (2024) Saskatchewan RCMP report $3.4 million in cryptocurrency fraud loss since start of year
[178] RCMP (2023) Money laundering through cryptocurrency uncovered in RCMP's Project Decrypt

Both in Canada and abroad, corporations are highly susceptible to financial crime as they can be structured to mask beneficial ownership, and be used to move, conceal, or convert illicit proceeds. Their money laundering and terrorist financing vulnerability varies by corporate structure.

Private corporations are the most common type of legal person in Canada. Their shares are generally held by a single or a limited number of non-public investors (e.g., insiders, family, close friends, and business associates) and subject to transfer restrictions. Private corporations are required to file annual returns with incorporation authorities and are subject to certain financial disclosure requirements and other controls under Canadian corporate laws. Nonetheless, they are not subject to the same level of regulatory scrutiny as public corporations. Private corporations are thus assessed to pose the highest money laundering and terrorist financing risks of all corporate structures in Canada.

Quick Definitions

Shell corporations do not have significant operations, assets, or physical presence. Though they can be used for legitimate purposes, they can be subject to abuse by financial criminals as they can be used to conceal beneficial ownership, especially where there is foreign ownership spread across jurisdictions.

Shelf corporations have no activity, including inactive shareholders, directors and secretaries, and can be left dormant for a period of time and later sold to others and used as vehicles to channel funds, carry on business, or enter into certain transactions. Though shelf corporations can be used for legitimate purposes, they can be subject to abuse by financial criminals seeking to create the impression that the corporation is reputable and has an established corporate history.

In order to do business in Canada, foreign corporations incorporated abroad are required to register an office or a branch in a Canadian province or territory, and are subject to Canadian tax and employment laws, among others. However, unless they are listed and traded on a designated stock exchange, within the meaning of the federal *Income Tax Act*, and subject to regulatory disclosure requirements, foreign corporations carrying out activities in Canada can pose unique vulnerabilities because of the opacity and complexity of cross-border structures. If they are incorporated in a jurisdiction with weak regulatory oversight or permissive corporate secrecy laws, this can obscure beneficial ownership information. Foreign corporations also provide foreign actors with access to Canada's financial system and can engage in frequent and high-value international transactions. These factors make them very highly vulnerable to financial crime.

Whether formed in Canada or in a foreign jurisdiction, shell and shelf corporations are forms of private corporations that can pose very high money laundering risks. Both shell and shelf corporations can be used to conceal beneficial owners, the nature of illicit transactions, and make investigations more challenging, making them common tools for money laundering and other financial crimes. Money laundering and terrorist financing vulnerabilities are heightened if they are formed in tax havens or secrecy jurisdictions.

By contrast, public corporations display a lower vulnerability to money laundering and terrorist financing, as they are subject to stringent legal constraints under provincial and territorial securities laws and stock exchange rules, designed to ensure transparency, accountability, and the protection of investors and the public.

The money laundering and terrorist financing vulnerabilities of cooperatives and boards of trade are low based on their ownership structure, governance and purposes. The money laundering vulnerabilities of other types of not-for-profit-corporations[179] vary depending on whether they are organized and operated exclusively other than for profit, or if they may generate profit subject to distribution restrictions and engage in certain limited commercial activities in support of their purposes. However, certain not-for-profit corporations may be particularly vulnerable to terrorist financing, as discussed in the "Non-Profit Sector" section of this chapter.

ML/TF Vulnerabilities of Partnerships (Medium): With approximately 40,000 active partnerships, partnerships are much less prevalent than corporations in Canada. This is primarily because partners can be exposed to the liabilities of a partnership, depending on its type. Partnerships are generally formed by the conclusion of a partnership agreement among the partners. Partnerships are flexible and easy to integrate with multiple sectors of the economy, including the financial and legal sectors.

In Canada, in both common law and civil law jurisdictions, partnerships generally do not constitute distinct legal persons. There are three main types of partnerships in the country: general partnerships (where the partners agree to share in any profits or losses of the partnership, and are generally jointly and severally liable for its debts); limited partnerships (where the general partners are generally jointly and severally liable for its debts, and the liability of limited or special partners is limited to their contributions to the capital or common stock of the partnership); and limited liability partnerships (where partners are generally not liable for the debts, liabilities or obligations of the partnership). According to the CRA, limited partnerships are the most common type of partnership in Canada. In order to carry on business in Canada, partnerships must generally register with the relevant provincial or territorial registrar.

The money laundering and terrorist financing vulnerabilities of partnerships vary depending on their characteristics. General partnerships may be less attractive to financial criminals by virtue of the joint and several liability of the partners. That said, the vulnerability of any type of partnership is heightened if it is structured to conceal its beneficial owners, especially where one or more of the partners are legal persons or other legal arrangements, which criminals can exploit to obscure their identities and their proceeds of crime. More complex partnership arrangements may involve the use of professional intermediaries for advisory services, opening the possibility of such professionals being used, unwittingly or wittingly, to help create a secretive ownership structure for illicit purposes. There is potential exposure to high-risk jurisdictions, as Canadian partnerships can operate overseas and the parties to the partnership may be foreign. Foreign partnerships from countries with reputations for financial secrecy that register to operate in Canada can pose an elevated risk.

However, public partnerships as well as limited partnerships, whose general partner is a securities dealer which are subject to specific AML/ATF obligations under the PCMLTFA or a subsidiary of a public corporation, present low money laundering and terrorist financing vulnerabilities, as the partnership, general partner or parent corporation (as the case may be) are subject to regulatory oversight.

Additionally, the money laundering and terrorist financing vulnerabilities of limited liability partnerships formed in Canada, which are generally permitted for certain categories of regulated professionals are relatively lower, though these may vary by industry (e.g., given the considerations discussed in the "Legal Sector" section, below, law firms operating as limited liability partnerships are exposed to higher money laundering risks than limited liability partnerships comprised of other regulated professionals, by virtue of the types of activities that legal professionals are involved in).

[179] In this context, the term "not-for-profit corporation" refers to federal, provincial and territorial not-for-profit corporations, regardless of their tax status.

There is also less empirical evidence that partnerships are used for money laundering and terrorist financing relative to corporations.

***ML/TF Vulnerability of Express Trusts (Very High)*:** A trust is a legal arrangement where a person – the settlor or the testator – transfers property to a trustee to be held in trust for the benefit of one or more beneficiaries. The term "express trust" designates a trust where the settlor or testator intentionally created the trust (e.g., by contract or by will), as opposed to trusts arising by operation of law or, in certain cases, by judgment. The express trust is a widely used legal arrangement in Canada for a variety of purposes. There were over 1.5 million trusts registered with the CRA in 2022.

Quick Definitions

Settlor refers to a person who created a trust during their lifetime (i.e., an *inter vivos trust*).

Testator refers to the person who created a trust by will (testament).

Express trusts are frequently employed in tax, estate planning, and investment, and are therefore highly integrated with the financial services sector. They are predominantly established through, or with the assistance of, trust companies, lawyers, and accountants.

The critical vulnerability of the express trust is that it separates control of the assets held in the trust from the beneficial ownership. The level of complexity of the arrangement, which may include legal persons or other legal arrangements as trustees and/or beneficiaries, can make it difficult to identify parties to the arrangement and their ownership or control interests in the trust assets. Trusts can also be structured so that the assets held in trust are located outside Canada, which can make it difficult for authorities to seize or freeze the trust's assets depending on the laws of the jurisdiction where the assets are located. The complexity of various trust arrangements impacts their vulnerability to exploitation for money laundering and terrorist financing. Express trusts have global reach, potentially exposing these trusts to high-risk jurisdictions. Canadians can constitute trusts under Canadian law in Canada or abroad, using domestic or foreign-based trustees, and non-residents can do the same in Canada.

Both Canadian trusts and foreign trusts with a Canadian beneficiary, settlor, trustee, or property, may be vulnerable to money laundering and terrorist financing, varying based on their type, objects, structure and other characteristics. Below is an overview of the money laundering and terrorist financing risks of various types of trusts in Canada.

Discretionary trusts are trusts under which the trustee has the power to decide how to distribute the trust income, capital or both to a class of beneficiaries. Discretionary trusts are at a high risk of misuse for money laundering and terrorist financing, relative to trusts where each beneficiary's interest is fixed. Asset protection trusts, which utilize a mechanism to protect trust assets from creditors, are very highly vulnerable. These vulnerabilities are heightened in the case of offshore asset protection trusts, constituted in jurisdictions that have enacted legislation allowing for secrecy, short statutory limitation periods, and/or 'flee' or 'flight' provisions to permit a change of trustee, the governing laws of the trust, or the removal or relocation of its assets to a new jurisdiction.

By contrast, public trusts have a low vulnerability to money laundering and terrorist financing as they are subject to securities regulations and/or stock exchange rules. In Canada, transactions relating to public trusts are also typically carried out by intermediaries such as securities dealers, which are independently subject to specific AML/ATF obligations under the PCMLTFA.

The inherent money laundering and terrorist financing vulnerabilities of Québec civil law *fiducies* established by contract or by will are similar to those of common law express trusts. However, they are subject to more formalities and restrictions than common law express trusts, which may make them less flexible as potential ML/TF vehicles.

ML/TF Vulnerabilities of Company Services Providers (Medium): Company service providers (CSPs), other than professionals such as lawyers and accountants, constitute a relatively small sector in Canada, with many entities providing fee-based online services. CSPs in Canada offer incorporation and management services for companies incorporated both inside and outside of Canada. Clients of company service providers, whether foreign or domestic, can easily access these intermediary services online from anywhere in the world. Given the online nature and global access of these services, the geographic reach of CSPs is substantial and may involve high-risk jurisdictions.

Transactions between CSPs and their clients typically involve small monetary amounts, as these transactions primarily consist of service fees and government fees related to incorporating or filing documents. The majority of CSPs in Canada offer legitimate services; however, the ability of these businesses to create corporate structures can be leveraged for illicit purposes. Services provided by CSPs, especially those that specialize in shell company formation and nominee arrangements, can be used, unwittingly or wittingly, to conceal assets and beneficial ownership. Criminals can exploit CSPs as nominee directors or shareholders and to set up complex corporate structures that obscure the beneficial owners, facilitating money laundering and terrorist financing.

CSPs can be used to modify organizational structures to obscure true beneficial ownership, thereby facilitating the evasion of ministerial directives issued by the Minister of Finance Canada. This manipulation involves adjusting the percentage of shares held by an individual or entity subject to specific sanctions regulations and reallocating them to a new "owner," who may be a non-sanctioned family member or nominee, to bypass ownership thresholds. Financial institutions may encounter difficulties in verifying client identification, monitoring transactions, and detecting and reporting suspicious transactions if CSPs employ complex techniques to assist clients in concealing true beneficial ownership.

Most interactions between CSPs and clients are limited to specific events like incorporation, annual filings, or agent services. While some of these engagements go beyond the initial point of incorporation, their intermittent nature can reduce the likelihood of continuous client monitoring.

The clientele includes a diverse range of individuals and businesses, some of which may have offshore operations in high-risk industries or jurisdictions. Foreign or domestic PEPs may use CSPs to establish complex corporate structures to obscure the origins of illicit funds.

Regulatory, Supervisory & Enforcement Response

Corporations

In Canada, corporate law is a shared responsibility with the provinces and territories. At the federal level, for-profit corporations are incorporated under, and governed by, the *Canada Business Corporations Act*, which contains provisions relating to corporate governance and shareholder rights and prohibits the issuance of bearer shares. Similar statutes covering for-profit corporations exist at the provincial and territorial levels. Under both federal and provincial and territorial statutes governing for-profit corporations, directors and officers generally have a duty of care and a fiduciary duty to act honestly, in good faith and in the best interests of the corporation. When acting with a view to the best interests of a corporation, the directors and officers of the corporation may consider the interests of other stakeholders. Compliance with these statutes is monitored by Corporations Canada, or the provincial/territorial equivalent.

In 2017, federal, provincial and territorial Finance ministers agreed in principle to pursue legislative amendments to their corporate statutes to require corporations to hold accurate and up-to-date information on beneficial owners, and to eliminate the use of bearer shares. In 2019, further amendments

were made to the *Canada Business Corporations Act* to allow investigative bodies to make a request to these corporations to provide information from their registers where authorities believe it would be relevant to an investigation. Since 2019, most provinces and territories have since amended their legislation to allow the same.

In 2024, Corporations Canada launched a publicly available registry of beneficial owners (referred to in the *Canada Business Corporations Act* as "individuals with significant control" or "ISC") of federal corporations. Corporations Canada oversees the federal ISC registry and has authority to inspect a corporation's records. Corporations that contravene their obligations in respect of the ISC registry may be subject to fines or dissolved. FINTRAC, the CRA, the RCMP and other police forces, and provincial and territorial corporate law administrators may have access to non-public ISC information.

Similar measures are being implemented at the provincial level. In 2023, Québec launched its public beneficial ownership registry, overseen by the Registraire des entreprises du Québec. The registry covers businesses carrying on commercial activities in that province, including corporations, partnerships, *fiducies* or trusts operating a commercial enterprise, sole proprietorships and certain cooperatives. In 2023, BC passed legislation to create a public beneficial ownership registry. In the *2024 Ontario Economic Outlook and Fiscal Review*, Ontario announced that it is also exploring options for a beneficial ownership registry. In the 2025 *Ontario Budget: A Plan to Protect Ontario*, Ontario announced its intention to launch public consultations on the establishment of a beneficial ownership registry, and other potential measures to fight money laundering and the financing of organized crime.

Reporting entities under the PCMLTFA that provide financial services to corporations, trusts and partnerships are required to conduct due diligence to ensure they know their customer and beneficial owners and report transactions, as required. As part of this due diligence, reporting entities will be required, starting in October 2025, to flag any discrepancies between the information on the federal beneficial ownership registry and the information they receive as part of their "know your client" obligations.

Partnerships

In Canada, partnerships are established and regulated at the provincial and territorial level. Some provinces and territories have distinct governing legislation for general and limited partnerships. Most provincial and territorial partnership statutes require certain partners' names and addresses, and, in the case of limited partnerships, some of those statutes require information concerning the contributions of the limited or special partners be included in the registration and/or be available for inspection at the registered office of the partnership.

Other information may be required in respect of extra-provincial limited partnerships or limited liability partnerships. For instance, in certain provinces, the registrar may only register an extra-provincial limited partnership if the registrar has received a copy of the partnership agreement verified by a notary public or equivalent. Domestic and foreign partnerships are also subject to beneficial owner disclosure requirements in certain provinces, namely Québec. In certain provinces and territories, limited liability partnerships comprised of regulated professionals, such as lawyers and accountants, are subject to oversight by the professional body regulating and supervising the profession. These bodies may make rules or issue guidance and best practices in respect of AML/ATF for their members.

Trusts

The trustee of all trusts constituted in Canada, whether common law trusts or civil law *fiducies,* are subject to a duty of care and a fiduciary duty of honesty, good faith and loyalty. Under the *Proceeds of Crime*

(Money Laundering) and Terrorist Financing Regulations (PCMLTFR), when reporting entities provide services to a trust, they are required to conduct various customer due diligence activities. A trust company is required to keep information on the beneficiaries of an *inter vivos* trust for which it is trustee, including information on the nature of their principal business or their occupation.

Trust companies, whether federally or provincially regulated, are subject to the PCMLTFA and supervised by FINTRAC. Federally licensed trust companies are subject to prudential supervision by OSFI and by the FCAC for consumer protection. They are subject to the sanctions provisions under the federal *Trust and Loan Companies Act*. Provincially licensed trust companies must be licensed by a provincial authority and are subject to the authority's supervision.

The Government of Canada introduced new trust reporting requirements for tax years ending after December 30, 2023. Under these enhanced reporting requirements, all trusts, unless certain conditions are met, are required to report beneficial ownership information to the CRA as part of an annual trust income tax and information return. Information must be provided for all trustees, settlors and beneficiaries of the trust, as well as on each person who has the ability (through the trust terms or a related agreement) to exert control or override trustee decisions over the appointment of income or capital of the trust, such as a protector. Failure to comply with the new trust reporting rules may result in penalties.

The Government of Québec introduced enhanced trust reporting rules harmonized with the federal ones. Since March 31, 2023, trusts operating a commercial enterprise, such as business trusts, investments trusts or real estate investment trusts, are also required to declare information in respect of their ultimate beneficiaries to the Québec Enterprise Registrar.

Company Service Providers

Given the role of CSPs in corporate formation, many of the regulatory measures that address the vulnerabilities posed by corporations, partnerships, and trusts similarly mitigate vulnerabilities posed by CSPs. The recent creation of beneficial ownership registries for federal corporations and corporations and other legal entities in Québec, along with new legislation in BC to create a beneficial ownership registry, will help mitigate the risks associated with CSPs and the businesses they provide services to. The Government of Canada recognizes the specific vulnerabilities posed by the sector and has announced in the 2024 Fall Economic Statement its intention to expand the application of the AML/ATF framework to include CSPs.

Legal Sector

The legal sector in Canada is large, complex, and composed of a variety of professionals including lawyers, notaries, and paralegals. This assessment pertains particularly to lawyers and Québec notaries as these professionals can provide services related to financial transactions, real estate, and the formation of corporations or other legal arrangements that render them vulnerable to misuse for money laundering and terrorist financing. Paralegals and notaries in most of Canada are not authorized to perform these services and are therefore not assessed to be vulnerable. Notaries in BC do display some vulnerabilities, but due to their unique nature, are assessed separately.

ML/TF Vulnerabilities of Lawyers and Québec Notaries (High): There are approximately 136,000 lawyers and 4,200 Québec notaries active in Canada. [180] The services offered by these professionals can be sophisticated and complex and may be accessed across the country by both

[180] Federation of Law Societies of Canada (Accessed 2024) About Us.

Canadians and foreign clients.

Lawyers and Québec notaries possess knowledge and skills that can be useful to criminal actors seeking to launder proceeds of crime. They can provide a variety of services that relate to financial activities, including operating trust accounts, creating legal entities or arrangements, facilitating real estate transactions, and acting as shareholders or directors. Lawyers can also accept cash to perform financial transactions on behalf of a client. The services that legal professionals provide give them a unique window into their clients' business structure, arrangements, and practices.[181]

Three types of activities that legal professionals may engage in are assessed as particularly vulnerable to exploitation for money laundering and terrorist financing purposes. These consist of the use of trust accounts, real estate transactions, and the creation, operation, and management of corporations, trusts, and other legal persons or arrangements.

A trust account is an account held by a lawyer or law firm that holds funds remitted by one or more clients to be used towards transactions directly related to legal services. The use of trust accounts may obscure the deposit taking institution's understanding of the intended nature, use, and ownership of these funds due the involvement of the legal professional managing the account. As a result, trust accounts are vulnerable to misuse or abuse, particularly by bad actors seeking to place proceeds of crime into the formal financial system and/or to layer these funds by retaining the services of legal professionals.

In most provinces and territories in Canada, lawyers are relied on to undertake the transfer of real estate,[182] which can be used as a method to launder proceeds of crime. Through the use of legal professionals, funds can appear to be legitimized as they move through a law firm's trust account as well as when they are exchanged for ownership of property.

Criminals may seek legal services to create corporations, trusts or other legal persons or arrangements, or engage in complex, cross-border transactions or structures, in order to retain control over proceeds of crime while hindering the ability of law enforcement to trace the origin and ownership of property. These vulnerabilities can be heightened in cases where lawyers may act as directors, officers, trustees, or as shareholders of a company or trustees of a trust on behalf of a client.

While many of the clients of legal professionals are low-risk, the client profile can also include a combination of corporations, PEPs, clients in vulnerable businesses and professions, and clients whose activities are carried out in jurisdictions identified as high-risk by the FATF and other locations of concern.

Communications between a lawyer and client are protected by solicitor-client privilege in common law systems and professional secrecy under Québec civil law. Criminals have been observed by law enforcement to abuse solicitor-client privilege and professional secrecy by retaining the services of legal counsel in an effort to hide their activities and other information from competent authorities, such as law enforcement, and financial institutions who process financial transactions from trust accounts. The abuse of privilege and professional secrecy protections to mask criminal activity is of particular concern to law enforcement as it poses barriers to investigation, including additional levels of legal complexity and time constraints.

[181] FINTRAC (2024) Special Bulletin on the use of the legal profession in money laundering and sanctions evasion.
[182] In Québec, the transfer of immovable property is the exclusive domain of Québec notaries (to the exclusion of lawyers).

ML/TF Vulnerabilities of British Columbia Notaries (Medium): The BC notary sector as regulated under the PCMLTFA consists of approximately 300 reporting entities. The sector provides a restricted range of legal services primarily for residents of the province. This includes the provision of certain vulnerable services, including real estate transactions, creating trust accounts, and executing financial transactions. Though these services constitute a significant portion of the sector's business operations, the sector's overall vulnerability profile is assessed as lower than that of lawyers and Québec notaries, given the sector's comparatively simple structure, smaller relative size, low geographic reach, and the lack of professional secrecy protections conferred to the sector.

BC notaries have some ongoing business relationships as well as some one-time transactional business. Services are oriented towards individuals as opposed to corporate clients. The sector's client profile also includes the presence of high-risk clients, including foreign and domestic PEPs, as well as clients with high-risk occupations.

In comparison to other legal professionals in Canada, such as lawyers and Québec notaries, BC notaries do not confer a high level of anonymity to their clientele, particularly because the services they offer to clients are not protected by solicitor client privilege. Moreover, most interactions occur with the client physically present. However, non-face-to-face interactions are possible, as are engagements with third parties, particularly with the emergence of virtual notary services.

Regulatory, Supervisory & Enforcement Response

BC notary publics and BC notary corporations (collectively referred to as BC notaries) are subject to AML/ATF requirements as set out in the PCMLTFA when engaging in prescribed services[183] on behalf of a person or entity and are subject to supervision by FINTRAC. BC notaries are generally found of have strong compliance results when subject to FINTRAC compliance assessments.

BC notaries are also governed by the *Notaries Act* of BC and subject to the discipline of their professional society. The Society of Notaries Public of BC is responsible for establishing standards of education and professional conduct, inquiring into matters of conduct by members, conducting discipline proceedings, and ensuring that the sector is regulated in the public interest.

Conversely, Canadian lawyers and Québec notaries are not subject to the PCMLTFA and its regulations. In 2015, the Supreme Court of Canada rendered a decision in *Canada (Attorney General) v. Federation of Law Societies of Canada*, stating that certain provisions of the PCMLTFA, as they then applied to the legal profession, breached certain sections of the *Canadian Charter of Rights and Freedoms*. The Supreme Court acknowledged the important public purpose of Canada's AML/ATF Regime and affirmed that Parliament could impose obligations on the legal profession that are within constitutional boundaries.

Under the Canadian Constitution, the provinces have legislative jurisdiction to license and regulate various professions including the legal profession. Provincial and territorial statutes created law societies to self-regulate the legal profession in the public interest. These statutes set out the authorities of the professional bodies that govern the legal profession, including rules of practice and standards of conduct and competence, oversee the licensing of lawyers, and investigate and discipline members for professional misconduct.

These standards are relevant to AML/ATF activities, as legal professionals are prohibited from engaging in

[183] These services include receiving or paying funds or virtual currency (other than those received or paid as professional fees, disbursements, expenses or bail); purchasing or selling securities, real property or immovables, or business assets or entities; or transferring funds, virtual currency or security by any means.

activity that would constitute professional misconduct and have a duty not to assist or facilitate conduct by a client that the lawyer knows or ought to know is dishonest, fraudulent, unlawful, or illegal.

Every lawyer in Canada and notary in Québec is required by law to be a member of one of Canada's provincial and territorial law societies. Canada's law societies review and investigate complaints received against their members and proactively detect professional misconduct through their audit programs. Their statutes empower them to investigate their members for violations of law society rules or standards, which can lead to disciplinary hearings and may result in reprimands, fines, practice conditions or restrictions, suspensions from practice, or disbarment. In certain provinces and territories, law societies may refer instances of possible criminal activity to law enforcement for investigation, in certain circumstances.

The FLSC, the national association representing all provincial and territorial law societies, has developed Model Rules and provides guidance and assistance to the law societies to combat money laundering and terrorist financing.[184] This includes the Model Rules on Cash Transactions, Client Identification and Verification, and Trust Accounting, which have been implemented by all law societies in Canada. Notably, the Model Trust Accounting Rule prohibits the use of legal professionals' trust accounts for any purpose other than one directly related to the provision of legal services and the Model Cash Transactions Rule prohibits a lawyer from accepting or receiving cash that totals more than $7,500 in respect of any one client matter, subject to certain exceptions.[185]

In addition to these rules, in each Canadian province and territory, the legal profession is bound by a code of professional conduct, which, among other things, requires reporting to a law society where a legal professional is believed to be engaging in serious misconduct or criminal activity, unless doing so would be unlawful or would involve a breach of solicitor-client privilege or confidentiality.[186] In all provinces and territories, lawyers and Québec notaries are also required to report to their respective law society if they have been charged, convicted or found guilty of offences under the *Criminal Code* or other offences that are inconsistent with the high standards of conduct expected of law society members.

Since June 2019, the FLSC has worked with the Government of Canada through a joint working group to explore issues related to money laundering and terrorist financing in the legal profession and to strengthen information sharing between law societies and the government. This working group, which includes representation from Finance Canada and Justice Canada, with regular participation from FINTRAC and the RCMP, also provides a venue through which information on money laundering and terrorist financing risks, trends, and mitigation measures are shared. The RCMP has leveraged this forum in order to formalize information-sharing mechanisms with law societies through MOUs.

[184] Federation of Law Societies of Canada (Accessed 2024) Fighting money laundering and terrorist financing
[185] Federation of Law Societies of Canada (2018), Model Trust Accounting Rule; and Model Rules on Cash Transactions
[186] Federation of Law Societies of Canada (2024), Model Code of Professional Conduct; The duty to report has been incorporated in all provincial and territorial codes of professional conduct.

Enforcement Action Spotlight: Legal Sector

In 2023, the Law Society of British Columbia disbarred a Vancouver lawyer who was accused of facilitating money laundering, having moved more than $30 million from clients he knew were being investigated by law enforcement for securities fraud. The lawyer received nearly $900,000 in fees from those clients even though they provided no substantive legal services. The lawyer was also found to have used twenty burner phones over eighteen months to cover their tracks when moving the clients' funds.[187]

Accounting Sector

ML/TF Vulnerabilities of Accounting Sector[188] (Medium): Approximately 1,000 accountants and accounting firms in Canada undertake activities vulnerable to money laundering and terrorist financing abuse and have obligations under the PCMLTFA. The professionals that make up this sector have specialized knowledge and expertise that may be vulnerable to being exploited unwittingly or wittingly for illicit purposes. This expertise predominantly encompasses financial and tax advice and can include providing help and counsel around company and trust formation.

The profession offers vulnerable services to a range of individuals and businesses and can act as third parties in transactions. The profession is well integrated with other complex and vulnerable sectors of the economy, such as the banking, securities, and real estate sectors. This feature, coupled with the sector's unique expertise relating to taxation, fiscal policies, and finance, enables members of the profession to act as facilitators or 'gatekeepers' to other areas of the financial system, which can present heightened vulnerability to being abused for illicit purposes.

The client profile of accountants includes high net worth clients, PEPs, and cash intensive businesses. Accountants can engage in activities associated with high-risk jurisdictions, particularly those that are employed by large accounting firms that have international operations or linkages. Members of the profession tend to have ongoing, direct relationships with their clients, with interactions predominantly occurring in face-to-face settings, minimizing anonymity.

Regulatory, Supervisory & Enforcement Response

Accountants and accounting firms are subject to AML/ATF regulatory controls under the PCMLTFA and supervision by FINTRAC. Accountants that are Chartered Professional Accountants (CPAs) and accounting firms must comply with PCMLTFA requirements when engaging in prescribed activities on behalf of a person or entity. Prescribed activities include receiving or paying funds or virtual currency; purchasing or selling securities, real property or immovables, or business assets or entities; transferring funds, virtual

[187] Law Society of British Columbia (2022) Decision of the Hearing Panel on Disciplinary Action

[188] Accounting firms and accounting services provided by regulated accountants and non-regulated individuals as well as their knowledge and skills were considered for the assessment. For the purposes of the PCMLTFA and its regulations, "Accountants" means a chartered accountant, a certified general accountant or a certified management accountant. An accounting firm means an entity that is in the business of providing accounting services to public that has at least one accountant who is a partner, an employee or an administrator.

currency or security by any means; or giving instructions in connection with any of these activities.

These activities do not include those that are carried out in the course of an audit, a review or a compilation engagement within the meaning of the CPA Canada Handbook prepared and published by the Chartered Professional Accountants of Canada. Accountants that are not CPAs are not subject to the PCMLTFA nor to professional standards.

Accountants have strong compliance results when subject to FINTRAC compliance assessments. The accounting sector is active in various government engagement fora at the federal level, including the ACMLTF led by Finance Canada, which provides both the government and private industry with a venue to share information on emerging money laundering and terrorist financing risks, trends, and mitigation measures.

The profession is also governed by the Acts, by-laws and regulations of their respective province or territory, which place several obligations on accountants, such as adhering to professional codes of conduct, continuing professional development requirements, submitting to practice inspections, and maintaining designation and licensing standards.

Enforcement Action Spotlight: Accounting Sector

In 2019, through Project Hobart, the OPP identified that a chartered professional accountant assisted with laundering the proceeds of crime for an OCG operating an illegal online sportsbook. The accountant used a nominee's bank account to conduct financial transactions on behalf of his client. Additionally, this member of the OCG used a lawyer's trust account to conduct financial transactions valued in the millions of dollars. Approximately $40 million in assets were restrained or seized as proceeds of crime from six individuals who were charged with various crimes.[189]

Enforcement Action Spotlight: Accounting Sector Tax Evasion

In 2019, the CRA announced that an individual in Kingston, Ontario, was sentenced in the Ontario Court of Justice in Ottawa to an eighteen-month conditional jail sentence for which the first six months are served under house arrest, 240 hours of community service, a $34,432 fine, and a three-year term of probation. The individual, an accountant, was sentenced for assisting his client in a tax protester scheme and pleaded guilty on the same day to one count of assisting his client in obtaining Goods and Services Tax Credit and Canada Child Tax Benefit payments to which his client was not entitled. For the years 2008 to 2012, the individual assisted his client with reporting income from his dentistry practice totaling $2,045,572, but then wrongfully deducting the entire amount as a business expense, under "private contracts". The client was also sentenced for tax evasion and money laundering. [190]

Real Estate Sector

ML/TF Vulnerabilities of Real Estate Sales Representatives, Brokers & Developers (High): Real estate brokers, sales representatives, and developers are involved in the development of land, the construction

[189] OPP (2020) Annual Report
[190] CRA (2019) Kingston accountant sentenced for assisting client in tax protester scheme

of new buildings, and their subsequent sale and re-sale. Real estate transactions are integrated with a range of other sectors, and the purchase and sale of real estate involves a variety of facilitators, including legal professionals, mortgage providers, mortgage and title insurers, and appraisers. Each of these sectors and professions have their own expertise and access to information at different stages of a real estate transaction.

Most real estate transactions are completed in face-to-face settings and are not complex. However, in some markets, transactions are becoming more complex due to the use of digital identification and signatures, as well as the use of third parties and complex corporate ownership structures to complete transactions. Complex real estate transactions can include the use of shell companies for property purchased as investments, as well as the use of assignment clauses in the Contracts to Purchase and Sell. These clauses allow another buyer (the "assignee") to assume the buyer's rights and obligations before the original buyer takes possession of the property.

Real estate brokers, sales representatives, and developers can be exposed to high-risk clients, including PEPs, foreign investors (including from high-risk jurisdictions or jurisdictions of concern), and individuals in vulnerable occupations and businesses. This feature renders the sector particularly vulnerable to the laundering of proceeds generated from foreign corruption.

ML/TF Vulnerabilities of Mortgage Brokers (Medium): Mortgage brokers are professional intermediaries that provide a range of mortgage financing options to their clients (applicants) and handle applications with a chosen lender. Mortgage financing is the sector's main business line, which entails maintaining relationships with a variety of lenders, including banks, credit unions, and private lenders. Mortgage brokers also offer other financing products based on home equity, such as home equity lines of credit, home equity loans, and reverse mortgages. The sector is not complex, and in most cases, brokers do not handle the funds directly from borrowers.

Mortgage brokers usually conduct client due diligence activities, gather information on the creditworthiness of applicants, and work with mortgage lenders to obtain lending rates. The necessary requirement to validate a client's creditworthiness for mortgage providers can help with customer due diligence, but the scope of a credit assessment can be narrow and may not extend to other due diligence activities relevant to AML/ATF controls, such as PEP determination.

Although mortgage brokers pose a medium level of vulnerability to ML/TF, they have a sightline of the financing of real estate transactions that can be leveraged for AML/ATF purposes (e.g., detection of suspicious borrowers).

ML/TF Vulnerabilities of Mortgage Lenders (High): While deposit-taking financial entities, such as banks and credit unions, hold a significant share of outstanding mortgages, other types of lenders have grown rapidly over the last decade and now hold more than $100 billion in mortgage assets.[191] These entities include mortgage finance companies,[192] mortgage investment corporations (MICs), syndicated mortgages, or other private lenders such as private corporations, individuals, and mutual-fund trusts.

These lenders generally offer one type of vulnerable product, namely mortgages (residential and commercial) and other loan products based on home equity. Some of these lenders (e.g., MICs and syndicated mortgages) also provide direct investment opportunities to individuals or businesses who wish

[191] Bank of Canada (2024) Non-bank financial intermediation: Canada's submission to the 2023 global monitoring report

[192] Some MFCs have to comply with OSFI Guideline B-20 which include AML requirements when they underwrite and administer mortgages packaged and sold to regulated financial institutions or securitized through government-sponsored programs.

to invest funds to finance the loans.

The mortgage lending sector can be complex in terms of financing arrangements and its business operations. Ownership structures of some types of private lenders or of entities providing them with capital can also be highly complex and opaque. The sector is integrated with a number of other sectors, including the real estate sector, legal sector, financial sector, and private or institutional investors.

The sector is exposed to high-risk clients, including PEPs, foreign investors (including from high-risk jurisdictions or jurisdictions of concern), and individuals in vulnerable occupations and businesses. Some private lenders promote their services to individuals more likely to work in vulnerable businesses, such as those that are cash intensive. Additionally, certain segments of the sector, such as private MICs, syndicated mortgages, and other private lenders are more likely to deal with corporate entities as borrowing clients and high-net-worth individuals as providers of capital than traditional mortgage lenders. Although transactions can be conducted in a face-to-face setting, non-face-to-face transactions have increasingly become the norm across the sector.

Regulatory, Supervisory & Enforcement Response

Real estate brokers, sales representatives, and developers are subject to AML/ATF regulatory controls under the PCMLTFA and supervision by FINTRAC. As of October 11, 2024, mortgage administrators, brokers, and lenders have similarly been subject to AML/ATF regulatory controls under the PCMLTFA and supervision by FINTRAC.

The government continues to advance actions to mitigate the vulnerabilities posed by the sector. Notably, *Fall Economic Statement, 2023* announced the government's intention to extend PCMLTFA requirements to title insurers and by requiring real estate representatives to identify unrepresented parties and third parties in real estate transactions. These requirements will come into force on October 1, 2025.

These sectors are also subject to provincial and territorial regulations in several jurisdictions.[193] Several provinces and territories operate registration or licensing schemes for real estate sales representatives, sale estate brokers, and mortgage brokers. Licensing schemes, in particular, often require a criminal record check component to provide controls against criminal infiltration across the sector.

For instance, in Québec, mortgage brokers are subject to the *Real Estate Brokerage Act*[194] and the regulations of the *Organisme d'autoréglementation du courtage immobilier du Québec*. As of May 1, 2020, mortgage brokerage is covered by the Act respecting the distribution of financial products and services[195] and subject to regulation by the Autorité des marchés financiers.

New Brunswick oversees its real estate sector through a co-regulatory model.[196] The New Brunswick Real Estate Association Office of the Registrar shares regulatory duties with the Financial and Consumer Services Commission, the province's crown corporation that regulates and enforces provincial legislation

[193] The following provincial and territorial regulatory bodies govern real estate activities: BC Financial Services Authority (BCFSA); Real Estate Council of Alberta (RECA); Saskatchewan Real Estate Commission (SREC); Manitoba Securities Commission; Real Estate Council of Ontario (RECO); Organisme d'autoréglementation du courtage immobilier du Québec (OACIQ); New Brunswick Real Estate Association (NBREA) and Financial and Consumer Services Commission of New Brunswick; Nova Scotia Real Estate Commission; Government of Prince Edward Island; Newfoundland and Labrador Government Modernization and Service Delivery; Government of the Yukon; Northwest Territories Municipal and Community Affairs.

[194] LégisQuébec (2024) C-73.2 - Real Estate Brokerage Act

[195] LégisQuébec (2024) d-9.2 - Act respecting the distribution of financial products and services

[196] New Brunswick Real Estate Association (Accessed 2025) About the Office of the Registrar

for real estate, mortgage brokers, and various other consumer-focused industries.[197]

Any real estate agent operating in Prince Edward Island must be licensed through the Registrar of Real Estate in accordance with the *Real Estate Trading Act*.

BC established a Land Owner Transparency Registry, which includes information about individuals who are deemed to have an indirect interest in land (e.g., through corporations, trusts and partnerships) in a searchable, public database.

The real estate and mortgage sectors are engaged in various government engagement fora at the federal level, including the ACMLTF led by Finance Canada. FINTRAC frequently engages the industry directly to provide information regarding sectoral obligations and has published guidance and special bulletins on sector-specific risks to support compliance program and reporting requirements.[198]

Challenges persist in achieving a consistent understanding of money laundering indicators across the real estate sector. Reporting levels of suspicious transactions to FINTRAC in the sector remain low. Common deficiencies in the sector's AML/ATF programs often relate to compliance requirements, ongoing monitoring, enhanced due diligence, record keeping, and client due diligence obligations. Rates of AML/ATF compliance by the mortgage sector is limited as the regulations have only newly come into effect. FINTRAC's current supervisory activities associated with this newly regulated sector are focused on awareness building and fostering strong compliance.

FINTRAC has conducted extensive outreach to the real estate sector to bolster compliance. This includes holding several meetings in the 2023/24 financial year with large real estate brokerages to enhance the effectiveness of STRs and promote best practices. FINTRAC has also worked directly with the Canadian Real Estate Association (CREA), the industry association that represents real estate brokers, agents and salespeople across Canada, on communicating updates to FINTRAC's materials available to CREA members. This includes client information forms, receipt of funds records, and CREA's risk assessment template, all updated to reflect FINTRAC's latest advice and guidance. The updated materials enhance brokers' ability to collect risk-related information, enabling them to more effectively identify reportable transactions.

[197] Financial and Consumer Services Commission of New Brunswick (Accessed 2025) About the Commission
[198] FINTRAC (2024) Operational alert: Laundering the proceeds of tax evasion in real estate; FINTRAC (2016) Operational brief: Indicators of ML in financial transactions related to real estate

Enforcement Action Spotlight: Real Estate Sector

In 2022, an RCMP Integrated Money Laundering Investigative Team uncovered a series of suspected complex mortgage frauds. The scheme defrauded millions from multiple financial institutions over a five-year period.[199]

In 2024, the CRA announced that an individual in Richmond, BC, was sentenced[200] to a conditional sentence order of two years less a day and was fined a total of $2,153,394 for failing to report $7,485,246 in taxable income on his individual income tax returns for the years 2011, 2012, and 2014. The individual failed to report income from the assignment fees earned from flipping 14 properties between January 1, 2011, to December 31, 2014, thereby evading $2,153,394 in federal Income taxes. Since then, a new home flipping tax and assignment registry has come into effect, to discourage speculative buyers and increase the transparency of sales transactions, thereby reducing the tax evasion and laundering risks associated with real estate transactions.

Gambling Sector

ML/TF Vulnerabilities of Brick-and-Mortar & Online Casinos (High): The gambling sector in Canada consists primarily of brick-and-mortar and online casinos. As of April 2025, 19 provincially regulated casinos are licensed to operate in Canada. Among them, 10 are brick-and-mortar casinos that also offer online gaming, while eight do not. Each of these casinos have multiple operators and various locations. The other provincially regulated casino, iGaming Ontario, strictly offers online gaming through the registration and contracting of private operators and maintains a list of regulated operators and gaming sites: Regulated iGaming Market | iGaming Ontario.

While casinos provide a limited number of vulnerable products and services, they conduct a large amount of business across Canada, most of which is highly transactional and cash intensive. Very important person (VIP) floors of casinos can represent a particular vulnerability, as the clientele typically have significant funds and may include higher-risk individuals. Casino clientele include PEPs, non-residents and clientele in vulnerable businesses and professions. Some casinos offer clients the ability to transfer funds electronically, including internationally. Clients can conduct gaming activity in brick-and-mortar casinos relatively anonymously, although casinos are monitored, and regulators require face-to-face interaction with casino staff for some activities. Casinos' business relationships with clientele have increasingly become account-based due to the sector's increased awareness and understanding of money laundering and terrorist financing risks posed by anonymous clients.

Online casinos have both transactional and ongoing client relationships including clients in vulnerable occupations and businesses. All transactions are conducted online through non-face-to-face interactions and can involve intermediaries. Non-face-to-face users must register to use the site and must provide a method of payment (e.g., credit or debit card). Although this reduces the anonymity of the accountholder, it remains difficult to determine who is in control of the account. The level of complexity varies among information management systems hosted by each online casino, notably the use of technology to identify a user's IP location and authenticate identification documents to verify client identity. Fraud, and the

[199] RCMP (2022) RCMP Federal Policing Integrated Money Laundering Investigative Team charge man in $2.1 million mortgage fraud scheme

[200] CRA (2024) Over $2 million in fines and a conditional sentence for a Richmond man convicted of tax evasion in the real estate industry

subsequent laundering of the proceeds from these offences, poses the greatest risk for the regulated online gaming sector.

The prevalence of online gambling has increased in recent years, with the International Center for Gaming Regulation projecting the global industry to grow to US$100 billion by 2026. Industry growth accelerated during the COVID-19 pandemic, with the closure of brick-and-mortar casinos forcing many gamblers online. In Canada, industry growth has coincided with new regulatory changes, such as the legalization of single event sports betting that came into force in August 2021, and the subsequent entrance of new gambling operators.[201] Notably, in April 2022 when iGaming Ontario became operational, Ontario's online gambling marketplace was opened to private operators, including international gambling corporations.

The rapid expansion of online gaming has created new and novel betting products. Peer-to-peer sports betting, in which players can wager directly against one another, rather than versus a sportsbook, carries collusion risks that can facilitate money laundering and terrorist financing. Equally, in traditional online casino games like poker, money launderers may engage in "chip dumping" to circumvent restrictions on peer-to-peer transactions by purposely losing to another player early on in a game in order to transfer funds to that player's account.

Spotlight: Unlicensed and Illegal Gambling

Illegal unlicensed and offshore gambling pose regulatory challenges for all governments. Despite the availability of regulated online gambling in Canada, some Canadians continue to use unlicensed gaming websites that operate in contravention of the *Criminal Code*. Advertisements on national broadcasts by betting operators licensed in certain jurisdictions only, may create confusion amongst players regarding which products and services they can legally use. Attempts to access provincially unlicensed applications sometimes redirect users to international sites operated by the same companies, exposing them to unregulated play, in contravention of the *Criminal Code*.

Transactions with unlicensed offshore sites — especially those in jurisdictions with financial secrecy or weak AML/ATF regimes — pose heightened money laundering and terrorist financing risks. Even without Canadian-based accounts, funds can be sent to domestic financial institutions. Individuals involved in criminal activity have also been observed gambling on behalf of others at both licensed and unlicensed gambling sites, by receiving email money transfers from unrelated third parties, which reference terms relating to gambling.

Other gaming activities in Canada, including horse racing and pari-mutuel betting and ship-based casinos, are assessed to have a lower vulnerability to money laundering and terrorist financing relative to casinos.

Racetracks are provincially licensed and operate in most Canadian provinces, either independently or alongside brick-and-mortar casinos. Pari-mutuel betting on horse-racing is licensed and regulated by the Canadian Pari-Mutuel Agency, which is mandated to maintain the integrity of pari-mutuel betting in Canada but does not have an AML/ATF-related mandate. The size of the sector is small and in decline.[202] Betting on horse races can be done through cash (in-person), betting account (in-person or online), or other means, and the nature of business relationships is largely short-term and transactional.

[201] FINTRAC (2024) Special Bulletin on laundering the proceeds of crime through online gambling sites
[202] Covers (203) Documents Show Sports Betting-Related Uncertainty for Canada's Horse Racing Sector

Gambling on international cruise ships is restricted to international waters. There are no known cruise operators that conduct gaming within Canada's territorial limits. Moreover, unlike some other jurisdictions, casino junkets that facilitate high-value gambling for foreign clients do not pose a notable money laundering and terrorist financing risk in Canada.

Regulatory, Supervisory & Enforcement Response

All brick-and-mortar and provincially regulated online casinos in Canada are subject to comprehensive AML/ATF regulatory controls under the PCMLTFA and supervision by FINTRAC. These casinos are also required to be licensed and regulated under provincial Acts.

FINTRAC regularly engages each group/provincial casino and shares information on sector risks. The casinos are represented by a rotating chair of the provincial regulators at the ACMLTF and Public Private Partnerships have been established with the sector, such as Project Athena and Project Dolus (online gambling).

FINTRAC supervision examination findings indicate that the majority of brick-and-mortar casinos have implemented an ongoing training program and that employees understand their obligations under the PCMLTFA including ensuring they understand the source of funds and report suspicious activity to FINTRAC. However, deficiencies have been found in relation to Know-Your-Client requirements and the quality and timeliness of client profiles. PCMLTFA compliance has strengthened as a result of the Cullen Commission's focus on the sector. BC has strengthened the authority of its gambling regulator and introduced preventive measures to strengthen client due diligence, monitor transactions, and curtail high-risk activity.[203]

FINTRAC supervision of online casinos is nascent, with early findings indicating that the quality of client identification profiles, in particular client occupation, can be improved. This information is needed for assessing risks and identifying suspicious gaming activity.

Pari-mutuel betting and racetracks are not subject to PCMLTFA obligations. However, racetracks impose limits on cash betting at terminals ($1,000), record keeping for high-value bets, and account registration requirements for online betting on horse races, which mitigate money laundering and terrorist financing vulnerabilities.

[203] Government of BC (2025) Quick glance - Government actions taken to address Cullen Commission Recommendations

Public-Private Collaboration: Counter-Illicit Finance Alliance British Columbia Combatting Money Laundering in BC and across Canada

The Counter Illicit Finance Alliance of BC (CIFA-BC) is an RCMP financial information-sharing partnership composed of 36 public and private organizations. Its mission is to lawfully exchange information to protect the economic integrity of BC through the prevention, detection, and disruption of illicit financial activity. CIFA-BC grew out of Project Athena, a public-private partnership launched by the RCMP in 2019 to better combat money laundering through casinos and underground banks.

FINTRAC's 2019 Operational Alert on laundering the proceeds of crime through a casino-related underground banking scheme and 2023 Updated indicators: Laundering the proceeds of crime through underground banking schemes, assist businesses in identifying suspicious transactions that may be related to professional money launderers and money laundering organizations.

FINTRAC provided 42 disclosures of actionable financial intelligence on 88 subjects in 2023–24, in support of the money laundering investigations of Canada's police and law enforcement agencies related to CIFA-BC.

Dealers in Precious Metals & Stones

ML/TF Vulnerabilities of Dealers in Precious Metals and Stones (High): Canada has a large number of dealers in precious metals and stones (DPMS) that are located across the country, ranging from very small, one-person operations to large multinational corporations. The sector operates across a broad-spectrum of market activities, including extracting/mining, manufacturing, refining, wholesaler/retailer, bullion markets, and pawnbrokers. The variation in business models, products, and delivery channels results in differing levels of transaction complexity and inherent money laundering vulnerability within the sector. Wholesale and investment business models, such as bullion markets, are typically the most complex and vulnerable aspects of the sector.

Quick Definitions

Precious metals include gold, silver, palladium, and platinum. They can be coins, bars, ingots, granules or in other similar forms.

Precious stones include diamonds, sapphires, emeralds, tanzanite, rubies, and alexandrite.

Jewellery means objects made of precious metals, precious stones or pearls that are intended for personal adornment.

DPMS are easily accessible to domestic clients through brick-and-mortar retailers in commercial districts, as well as through retail websites and online marketplaces for personal purchases. In some cases, Canadian DPMS are accessible to international clients, particularly through online personal sales or wholesale import/export business models. Many DPMS conduct a large volume of business in high-value goods, some of which are commodities that are particularly vulnerable to money laundering and terrorist financing. The highest vulnerability is ascribed to precious metals, such as gold and silver bullion, in forms that derive most of their value from the underlying metal, such as bars or ingots and diamonds, which are more commodified than other precious stones. The vulnerabilities for these products stem from their high value, potential high liquidity, limited traceability, and ease of transport. These products are also negotiable worldwide and can be exchanged for cash, goods or services, or used as an alternative form of currency.

High value finished jewellery also presents some vulnerabilities, including being purchased as luxury goods as part of a criminal lifestyle. However, their level of vulnerability is generally lower than that of commodified metals and stones. This is because the resale of finished jewellery results in a loss of value, making it an unattractive option for storing and transferring value. At the low end of the vulnerability spectrum are low value finished jewellery sold at retail, which are typically purchased for personal use and are not effective mechanisms for value transfer.

DPMS have largely transactional relationships with their clients and there are opportunities for clients to conduct cash transactions with a high degree of anonymity. The client profile continues to be assessed to include high-risk clients, notably those in vulnerable businesses or professions. This is a highly accessible sector, both domestically and internationally, where there are high-risk clients who can purchase high-value goods for cash relatively anonymously. Additional jurisdictional risk is posed to DPMS businesses that import raw or unrefined precious metals and stones for sale, such as refiners, manufacturers, and wholesalers.

Regulatory, Supervisory & Enforcement Response

DPMS are subject to AML/ATF regulatory controls under the PCMLTFA and supervision by FINTRAC. For the purpose of the PCMLTFA, a DPMS is a person or entity that buys or sells precious metals, precious stones or jewellery in the course of its business activities. Regulatory obligations are triggered once the DPMS engages in the purchase or sale of precious metals, precious stones, or jewellery in the amount of $10,000 or more.

The DPMS sector participates in various federal engagement fora, including the ACMLTF, where information is shared on money laundering and terrorist financing risks, trends and mitigation measures. FINTRAC has also publicized guidance and special bulletins on sector-specific risks to support risk mitigation and reporting and has taken various enforcement actions against entities operating in the sector in recent years.[204]

Enforcement Action Spotlight: DPMS Sector

In 2022, through Project Prospecteur, the Service de police de la Ville de Montréal dismantled an organized network involved in the production of cannabis and the laundering of proceeds of crime through a scheme involving the processing and trading of gold. The gold trading scheme alone was estimated to generate over $31 million, which was reinvested in further fraudulent schemes. The investigation also helped uncover a network linked to the production and sale of illegal cannabis. As a result of Project Prospecteur, charges were laid against 28 people for fraud, money laundering, and cannabis production/distribution, and there were significant proceeds of crime seizures, including gold (estimated value of $225,000), watches and jewellery (estimated value of $1,866,459), and cash ($865,465).[205]

[204] FINTRAC (2019) Operational brief: Risks and indicators for dealers in precious metals and stones
[205] Service de police de la Ville de Montréal (Accessed 2025) Projet Prospecteur : le SPVM met au jour une fraude de plus de 31 M$

Import/Export Companies

***ML/TF Vulnerabilities of Import/Export Companies (High)*:** There are approximately 215,000[206] import and export companies of various sizes active in Canada, ranging in terms of complexity and scale of operations. Import and export companies facilitate trade in goods and services across geographical borders. There are several business models, including acting as an intermediary between two entities or directly purchasing goods for sale from overseas. Import and export companies differ from customs brokerages in that customs brokerages are usually certified by a border agency or other government body, such as the CBSA in Canada, and facilitate the shipment and delivery process rather than simply handling the customs process.

Import and export companies navigate various layers of complexity in facilitating international transactions, taking into consideration international trade rules for the given product type, free trade agreements, licensing and customs regulations, modes of transport, in-transit insurance, and the risk of default by the counterparty.

Import and export companies can be created and maintained with relative ease by both residents and non-residents of Canada. Unlike the regulatory framework governing the registration of other border-related entities, such as customs brokers, carriers, and freight forwarders, the import and export company registration process is relatively simple and can be easily exploited. As with other sectors, the vulnerabilities posed by this sector are heightened in cases where criminally complicit actors can gain control of the company to facilitate trade fraud and/or TBML.

The role of these businesses as a driver of international trade creates opportunities to abuse global trade chains and financial institutions through TBML and to conceal these activities by obfuscating the true parties to trade transactions, as well as the source of funds. Their potential involvement as intermediaries in the trade chain creates layers of complexity and anonymity that can be exploited to obfuscate the identity of the true underlying importer and/or exporter. For example, import and export companies can conceal the true parties to a TBML scheme through opaque beneficial ownership. They can also layer the payments for goods through unrelated third parties, often based in other countries with no apparent connection to the transaction.

Goods can also be shipped through convoluted routings, including through the more than 7,000 special economic zones currently in operation,[207] to conceal both the origin and destination of goods, as well as the counterparties to the trade. The absence of strict regulations and transparency of the special economic zones that is beneficial for legitimate businesses, also makes them highly attractive for illicit actors who take advantage of this relaxed oversight to launder the proceeds of crime and finance terrorism. Countries with high rates of TBML are frequently located in trading hubs along international trade routes with a high concentration of import and export companies (e.g., China, Hong Kong, United Arab Emirates).

***ML/TF Vulnerabilities of Customs Brokerages and Freight Forwarders (Medium)*:** There are 3,172 freight forwarders and 356 customs brokers that operate in Canada. Freight forwarders do not move goods directly; they provide expertise in navigating the logistical component and contracting with carriers to ship goods across the border using various modes of transport (e.g., marine shipping, rail, air). Customs brokers are licensed service providers who obtain, prepare and submit commercial goods import and export information and documentation to customs services, such as the CBSA, in order to expedite the customs clearance process.

[206] This number reflects the number of import/export companies active (meaning they imported or exported goods within the last two years) from 2019 to 2023 per available data from Statistics Canada.
[207] Industry Analytics Platform (2024) New Trends in Special Economic Zones: Opportunities for Developing Countries

The scope of services and activities offered by freight forwarders is far more extensive than what custom brokers offer as the former will facilitate movement of goods on both sides of the border.

Overall, both entities can act as facilitators of TBML, as they can use their knowledge of trade logistics to control and direct TBML schemes, while disguising their role from law enforcement by acting as a facilitator, rather than the driver of the trade transactions under suspicion.

Regulatory, Supervisory & Enforcement Response

The CBSA is responsible for providing integrated border services that support national security and public safety priorities and facilitate the free flow of persons and goods. This includes responsibility for the administration of Part 2 of the PCMLTFA, which requires reporting on the cross-border movement of currency or monetary instruments valued at $10,000 or more and any associated seizures. The movement of bulk cash is one of the primary ways that proceeds of crime are laundered.

The CBSA's role in mitigating Canada's money laundering and terrorist financing vulnerabilities was expanded in April 2025 when PCMLTFA Part 2.1 (Reporting of Goods) and associated regulations came into force. PCMLTFA Part 2.1 compels importers and exporters (or their representatives) to attest to the truthfulness, accuracy, and completeness of their customs documents for AML/ATF purposes. As a result, the CBSA's mandate for AML/ATF compliance has grown beyond currency and monetary instrument reporting to include the cross-border trade in goods. The CBSA's new authorities include the ability to seize and forfeit goods, or apply equivalent monetary penalties, when it believes that these shipments are being used as a pretext to transmit illicit financial flows. The CBSA, within the Border Financial Crime Centre division, will launch a new cadre of PCMLTFA Regulatory Compliance Investigators, alongside a data-analytics oriented Trade Transparency Unit to support its new compliance mandate.

Enforcement Action Spotlight: Import/Export Companies

In 2023, the RCMP with assistance from CBSA, the Ottawa Police Service and Colombian authorities dismantled an Ottawa-based OCG responsible for the importation of large shipments of cocaine into Canada. It was identified that a Canadian business was using sea containers to smuggle drugs from Colombia to Canada. This operation prevented 52 kilograms of cocaine, with a street value between $1.4-1.7 million dollars, along with firearms from entering Canada. Four individuals who were looking to profit from selling illegal drugs were charged with *Criminal Code* and *Controlled Drugs and Substances Act* violations.[208]

In 2020, following an 11-month investigation, the RCMP identified an OCG involved in trafficking high volumes of illegal drugs into Canada and linked to illegal import and export activity. In total, 14 people were arrested on one hundred charges combined. Hundreds of kilograms of illegal drugs, $369,000 in cash, and ten firearms were seized. Five properties and five vehicles were also restrained.[209]

[208] RCMP (2023): Ottawa RCMP, CBSA and Ottawa Police foil attempt to smuggle large shipment of cocaine
[209] RCMP (2021) RCMP disrupts drug trafficking ring, seizes significant quantity of drugs and firearms

Non-Profit Sector

TF Vulnerabilities of Non-Profit Organizations (Medium): NPOs play a vital role in the delivery of essential services, humanitarian aid, and life-saving support for those in need, which often includes those in marginalized or excluded communities.[210] The NPO sector is diverse, and the risks of vulnerability to terrorist abuse vary from entity to entity.

Canada's non-profit sector contains an estimated 246,000 organizations. However, the portion of the Canadian non-profit sector that raise and disburse funds, and therefore could be vulnerable to terrorist financing, are fewer in number. These organizations represent the majority of Canada's 85,518 registered charities and only a small subset of the roughly 160,000 estimated tax-exempt non-profits.

Organizations operating in Canada's NPO sector display relatively simple corporate structures with low cross-border transactions. The sector's client profile is primarily composed of the beneficiaries of the sector's services, which pose low terrorist financing risks. The client profile either does not include, or has very limited, high-risk clients, and clients or beneficiaries of NPO activities would have limited ability to direct how the organization's resources are used. Further, most of the sector engages in domestic activities, and would be subject to oversight requiring record keeping and public transparency, which limits the sector's ability to engage in anonymous transactions through non-traditional channels.

The NPO sector plays a key role in Canadian society. However, certain features and services of the NPO sector that are instrumental in providing societal good, can also be exploited by bad actors for illegitimate purposes. Specifically, organizations that undertake the following activities are most vulnerable to abuse:

Quick Definitions

In Canada, the term "non-profit organization" (NPO) includes, for income tax purposes, tax-exempt non-profits and registered charities.

Tax exempt non-profit refers to a club, society or association that is not a charity that operates exclusively for social welfare, civic improvement, pleasure or recreation, or for any other purpose except profit.

Registered Charity refers to an organization that is constituted and operated exclusively for charitable purposes, that devotes its resources to its own charitable activities or by making qualifying disbursements, and that operates for a public benefit.

1. Organizations undertaking activities in high-risk jurisdictions, such as those where terrorist groups are known to operate, funds for terrorist groups are consistently generated, or that have been defined by the FATF to have strategic deficiencies in their frameworks for combatting money laundering and terrorist financing. Organizations whose activities can support the operational needs of threat actors are particularly vulnerable to functional abuse, such as the abuse of programming and the diversion of funds.
2. Organizations undertaking activities domestically that, irrespective of the actual nature of their activities, are vulnerable to abuse due to their ability to reach certain communities or groups of communities that threat actors target for sympathy and support, notably communities with linkages to conflict regions where terrorist groups operate.

[210] Human Security Collective (2023) The Future of FATF Recommendation 8: A Foresight Piece

Typologies associated with NPO abuse includes diversion (or 'skimming off') of funds raised for legitimate humanitarian purposes that are re-directed towards terrorist activities (with or without the NPO's or donors' knowledge); NPO-funded programs that can be exploited to create an environment which provides support for terrorist recruitment efforts (whether knowingly or unknowingly); false representation, whereby organizations or individuals exploit charitable causes to falsely raise money for these activities but instead use those funds to support terrorism; and the use of legitimate NPOs as a revenue stream through taxation imposed by a terrorist entity active in the region in which the exploited NPO operates.

Spotlight: Unintended Consequences in the NPO Sector

Though common characteristics of NPOs may render them more exposed to terrorist financing risk, they should be treated with care. Using broad characteristics to generalize conclusions on risk across diverse NPO subgroups may not be reflective of actual risk. These characteristics should provide a starting point for developing more nuanced risk profiles on NPO subgroups.

While some NPO activities can pose potential risks for terrorist financing abuse, overly restrictive policies in the name of protecting Canada's financial systems from terrorist financing abuse can have unintended consequences. Some NPOs have reported challenges in accessing financial services to support their activities. Financial exclusion, or de-risking, is where financial institutions terminate or restrict business relationships with clients or categories of clients to avoid, rather than analyze or manage, their risk.

De-risking can have significant negative effects. These include impeding the delivery of genuine humanitarian assistance and pushing clients to use high-risk, unsupervised IVTS, or resort to cash couriers - all of which can create visibility gaps for these funds and leave them more vulnerable to terrorist abuse. Financial institutions are responsible for managing their risk exposure and risk tolerances and may determine some clients pose unacceptable risks. However, assessing risk on a case-by-case basis can help strike a balance between enabling clients to use regulated financial systems, while also ensuring effective mitigation measures are in place to protect against terrorist financing.

Regulatory, Supervisory & Enforcement Response

In Canada, NPOs, including registered charities and tax-exempt non-profits, are subject to general administrative oversight, particularly regarding incorporation or tax status which help to mitigate the risk of terrorist financing abuse faced by vulnerable NPOs.

The small subset of the sector exposed to terrorist financing risks is also subject to targeted administrative oversight and enforcement by the CRA's Review and Analysis Division, which maintains a specific focus on the terrorism abuse faced by registered charities.

Both registered charities and tax-exempt non-profits working in high-risk jurisdictions may also be subject to additional ATF measures by Global Affairs Canada where, for example, they apply to receive government funding to support humanitarian aid or international development work. Further, under Canada's new Authorization regime,[211] registered charities and tax-exempt non-profits that receive

[211] Public Safety Canada (2024) Authorization regime and humanitarian exception for activities in terrorist group controlled areas - Section 83.03 Criminal Code

authorizations to shield from criminal liability certain activities that would result in an unavoidable benefit to a terrorist group may be required to adhere to reporting requirements or other terms and conditions imposed by Public Safety Canada.

Risks faced by other tax-exempt non-profits are addressed leveraging the range of activities undertaken across national security and other partners that support ATF efforts more broadly. This includes administrative approaches, such as federal and provincial regulation of not-for-profit incorporations, the CRA's general monitoring and compliance efforts for tax regulation, as well as law enforcement's criminal investigations and intelligence gathering activities.

Together, these oversight mechanisms help Canada apply focused and proportionate mitigating measures to organizations in the sectors most vulnerable to terrorist financing abuse, in line with the risk-based approach.

The Government engages with the NPO sector on the risks of abuse through the CRA's Advisory Committee on the Charitable Sector and on an ad hoc basis through the above-mentioned government departments. In addition, in 2024 the Government launched new interdepartmental dialogues with the NPO sector to deepen awareness, enhance communication, and help address money laundering, terrorist financing, and sanctions evasion risks. The CRA maintains webpages to educate the NPO sector (and public) on the risks of terrorist abuse. These webpages may be useful to better understand how terrorists abuse NPOs, to identify risks that relate to NPOs, and to understand measures that NPOs can take to reduce the risks they may face. See *Educating charities about the risks of terrorist abuse*.

Annex A: Methodology

2025 Assessment Framework and Scope

The 2025 Report was coordinated by the Department of Finance Canada, with the support of a dedicated working group consisting of intelligence, supervisory and law enforcement experts, co-chaired by FINTRAC.

The 2025 Report's findings were informed and validated through consultations with both government and external stakeholders, including federal government departments and agencies operating outside of Canada's AML/ATF Regime, provincial and territorial governments, the private sector, and non-profit organizations.

The core assessment model to identify and understand inherent money laundering and terrorist financing risks and their relative impact in Canada was developed in 2015 and applied in the 2015 and 2023 Reports. The basis of the risk assessment model is that risk is a function of three components: threats, inherent vulnerabilities, and consequences. Risk is viewed as a function of the likelihood of threats exploiting inherent vulnerabilities to launder illicit proceeds or fund terrorists and the consequences should this occur.

The 2025 assessment builds on this core assessment model by introducing various methodological enhancements, including a residual risk lens, to align with international best practices and provide a more nuanced understanding of risk in the Canadian context.

Quick Definitions

Threat: a person or group who has the intention, or may be used as a facilitator, to launder the proceeds of crime or fund terrorism.

Inherent Vulnerability: the properties in a sector, product, service, distribution channel, customer base, institution, system, structure or jurisdiction that threat actors can exploit to launder the proceeds of crime or to fund terrorism.

Residual Risk Lens: the analysis of the mitigating measures employed by federal, provincial and territorial governments, supervisory bodies, law enforcement, and the private sector to mitigate the inherent money laundering and terrorist financing vulnerabilities exhibited by a business sector, profession, or financial product.

Likelihood: the likelihood of money laundering and terrorist financing threats exploiting inherent vulnerabilities.

Consequence: the harm caused by money laundering and terrorism financing, including facilitating criminal and terrorist activity, on a society, economy, and government.

Assessing Canada's Money Laundering and Terrorist Financing Threats and Vulnerabilities

Canada's National Risk Assessment model assesses money laundering and terrorist financing threats separately. Although there is some overlap, these criminal activities are fundamentally different. In contrast, the assessment of vulnerabilities is not differentiated as money laundering and terrorist financing threats tend to seek to exploit the same set of vulnerable features of business sectors and professions, including the products and services they offer, to launder the proceeds of crime or fund terrorism.

The assessment of both threats and vulnerabilities includes a rigorous and systematic analysis of qualitative and quantitative data from various sources, including observations of law enforcement, tax and border authorities, financial and criminal intelligence, public and private sector data, and insights drawn from international collaborations on money laundering risks, methods, and trends through networks such as the FATF, G-7, G-20, the J5, the Egmont Group of Financial Intelligence Units, and the World Customs Organization.

Threat and vulnerability information is analyzed by subject matter experts with diverse perspectives from across Canada's AML/ATF Regime, including professionals in policy, strategic and tactical intelligence, law enforcement, national security, asset recovery, and prosecution. These experts work together to identify emerging patterns, developments, and typologies and inform assessments on the relevance, nature, and extent of money laundering and terrorist financing threats and vulnerabilities in the Canadian context.

Given the clandestine nature of criminal activity, quantitative data is difficult to source for some threat and vulnerability assessments. To account for these limitations, subject matter experts also assign confidence levels to the findings of each assessment.

Key Changes to 2025 Report

The 2025 Report maintains the basic tenants of the 2015 assessment model with the following methodological enhancements to the threat and vulnerability rating criteria to produce a more comprehensive and nuanced understanding of risk:

Money laundering threat assessment:

- Compared to the 2015 and 2023 risk assessment, the 2025 Report assigns risk ratings to a more consolidated set of distinct money laundering threat categories and improves the clarity of the assessment by distinguishing between threats and threat actors or enablers. This change provides a more accurate and comprehensive picture of Canada's money laundering threat environment.
- The 2025 threat assessment model was recalibrated to reduce overlap between rating criteria for money laundering threat assessment and assign greater weight on criterion of estimated proceeds of crime generated. This improvement allows for a broader distribution of threat ratings, ranging from high to low, provides a more accurate and realistic representation of the threat landscape, and enables more effective prioritization for policy, law enforcement, and private sector stakeholders.

Terrorist financing threat assessment:

- The 2025 terrorist financing threat assessment focuses on a smaller number of terrorist financing actors with a direct nexus to Canada, highlighting those that are most active in raising and moving funds through Canada and the Canadian financial system.
- The terrorist financing analysis is structured around categories of ideologically, politically or religiously motivated threats, as opposed to individual threat actors, as in previous assessments. This approach enables a more robust understanding of differences and similarities in terrorist financing methods across threat actors.

Money laundering and terrorist financing vulnerabilities assessment:

- The 2025 rating of vulnerabilities remains based on the inherent properties of a sector, profession, or financial product that threat actors may exploit to launder the proceeds of crime or to fund terrorism. This approach underscores the need for ongoing risk mitigation efforts.
- The 2025 Report applies an additional residual risk lens to highlight policy, supervisory, and law enforcement measures by federal, provincial, and territorial governments, as well as private sector actions, to mitigate vulnerabilities. This aims to better support priority setting and identify residual gaps that may require greater attention or further mitigating measures.

Annex B: Statement on GBA+ and Financial Inclusion

Financial crimes profoundly impact the lives and livelihoods of Canadians, and often particularly impact the most vulnerable in our society and abroad. Economically motivated crimes, such as fraud and theft, disproportionately victimize women, young people, Indigenous communities, racialized individuals, seniors, and newcomers. The government recognizes that measures to combat money laundering and terrorist financing may have varied impacts on different groups of Canadians and business sectors.

In developing the 2025 National Risk Assessment, careful consideration was given to these differences to avoid unintended consequences, particularly with regards to vulnerable Canadians and communities, the charity and non-profit sector, and financial inclusion. This includes the introduction of methodological changes, such as applying a residual risk lens for a more nuanced understanding or risk across the Canadian economy and targeting sectoral assessments on areas of greater risk to ensure that lower risk activities are not unduly impacted. Contributors to the Report also benefited from training on implicit biases and utilized information from a broad range of sources and stakeholders to ensure that the assessment remained balanced and well informed. Additional details on these efforts are outlined below.

Application of a residual risk lens

The 2025 Report applies a residual risk lens to highlight the policy, supervisory, and law enforcement measures implemented by federal, provincial and territorial governments, and private sector actions to mitigate vulnerabilities. This additional element aims to better guide policymakers, law enforcement agencies, supervisory bodies, and reporting entities to optimize their risk-based approach by taking into account existing mitigation measures and focus on areas of greatest residual money laundering and terrorist financing risk. Applying a residual risk lens improves the understanding of the assessed sector's vulnerability to money laundering and terrorist financing.

A nuanced understanding of residual risk within a particular sector can help prevent overly broad risk-mitigation practices that disproportionately affect certain groups or communities in Canada. For financial institutions, de-risking refers to the practice of terminating or restricting business relationships with certain clients, or categories of clients, to avoid risk rather than manage it. This approach can disrupt businesses, non-profit organizations, and humanitarian assistance groups, push financial transactions underground, and reduce transparency, ultimately increasing money laundering and terrorist financing risks.

Targeted assessments on high-risk areas

A refined understanding of risk allows governments, supervisory bodies, law enforcement, and the private sector to focus mitigation efforts on activities and organizations that pose higher risks within an economic sector. By targeting these areas, resources can be allocated appropriately and proportionately, avoiding a one-size-fits-all approach for all entities. From this angle, the approach is expected to minimize unintended consequences and prevents adverse impacts on individuals and communities that rely on the legitimate operations of entities in the sector being assessed.

Canada’s commitment to an effective, risk-based approach to combating money laundering and terrorist financing aligns with international best practices. For instance, a more precise assessment of risks within Canada’s charity and NPO sector enables the implementation of more focused, proportionate, and risk-based measures without unduly disrupting or discouraging legitimate NPO activities.

Training for the working group developing the national risk assessment

The 2025 National Risk Assessment was coordinated by Finance Canada in close collaboration with experts from the 13 federal departments and agencies included in Canada's AML/ATF Regime. A dedicated, interdepartmental Working Group co-Chaired by Finance Canada and FINTRAC conducted the threat and vulnerability assessments for the 2025 Report. Working Group members completed both mandatory and elective training sessions on equity, diversity, and inclusion provided by their respective departments and agencies, as well as by the Canada School of Public Service. They also completed training on identifying and mitigating implicit biases that could adversely affect their work.

Sources of the information and statistics

Threat and vulnerability information used in money laundering and terrorist financing risk assessments is sourced from a variety of verified and reputable channels, both internal and external to the Government of Canada. The 2025 Report incorporates statistics and qualitative assessments gathered from Canada's AML/ATF Regime partners, provincial and territorial authorities, the private sector, international partners, and academic institutions. Finance Canada, the principal Regime partner responsible for Canada's money laundering and terrorist financing risk assessment process, continues to work with its intelligence and security partners to reaffirm that the Report's assessments are derived from best objective information available to the Government of Canada by drawing from a variety of sources.

The wide array of information used to develop the report was analyzed by a range subject matter experts specializing in policy, strategic and tactical intelligence, law enforcement, national security, asset recovery, and prosecution.

Stakeholder consultations

Finance Canada conducted extensive consultations in developing the 2025 Report, including with federal organizations, provincial and territorial governments, industry associations, businesses, academics, and representatives from the non-profit sector. The 2025 National Risk Assessment takes into account and incorporates feedback and recommendations gathered through various public consultation forums, as well as guidance on international best practices.

Finance Canada remains committed to hearing from diverse stakeholders in order to continually improve the methodology and process for assessing and understanding Canada's money laundering and terrorist financing risks, and the effectiveness of Canada's National Risk Assessment to support the implementation of well targeted, proportionate and effective risk mitigation policies, measures, and enforcement actions.

Annex C: Supplement Products from Canada's AML/ATF Regime Partners

Bank of Canada: Information on the prevalence of counterfeiting in Canada and its impact on victims and society
https://www.bankofcanada.ca/wp-content/uploads/2021/04/prevalence-victim-impact.pdf

Canadian Anti-Fraud Centre: 2022 Annual Report
https://antifraudcentre-centreantifraude.ca/annual-reports-2022-rapports-annuels-eng.htm

Canadian Anti-Fraud Centre: Extortion
https://antifraudcentre-centreantifraude.ca/scams-fraudes/extortion-extorsion-eng.htm

Canadian Anti-Fraud Centre Bulletin: New technology
https://antifraudcentre-centreantifraude.ca/features-vedette/2024/03/bulletin-4-eng.htm

Canadian Anti-Fraud Centre Bulletin: Solicitation methods
https://antifraudcentre-centreantifraude.ca/features-vedette/2024/02/bulletin-2-eng.htm

Canadian Centre for Cyber Security: National Cyber Threat Assessment 2025-2026
https://www.cyber.gc.ca/sites/default/files/national-cyber-threat-assessment-2025-2026-e.pdf

Criminal Intelligence Service Canada: National Criminal Intelligence Estimate on The Canadian Criminal Marketplace: Money Laundering and Fraud, 2020
https://publications.gc.ca/collections/collection_2021/scrc-cisc/PS64-162-2020-eng.pdf

Criminal Intelligence Service Canada: Public Report on Organized Crime 2023
https://publications.gc.ca/collections/collection_2024/scrc-cisc/PS61-39-2023-eng.pdf

Commission of Inquiry into Money Laundering in British Columbia Final Report
https://cullencommission.ca/files/reports/CullenCommission-FinalReport-Full.pdf

Edmonton Police Service: Mass Market (mass-marketing fraud)
https://www.edmontonpolice.ca/CrimePrevention/PersonalFamilySafety/Frauds/MassMarket

Financial Consumer Agency of Canada: Credit card fraud
https://www.canada.ca/en/financial-consumer-agency/services/credit-fraud.html

Financial Consumer Agency of Canada: Debit card fraud
https://www.canada.ca/en/financial-consumer-agency/services/debit-fraud.html

FINTRAC Annual Report 2022-23 Safe Canadians, Secure Economy
https://fintrac-canafe.canada.ca/publications/ar/2023/ar2023-eng.pdf

FINTRAC Annual Report 2023-24 Safe Canadians, Secure Economy
https://fintrac-canafe.canada.ca/publications/ar/2024/ar2024-eng.pdf

FINTRAC guidance related to the Ministerial Directive on Financial Transactions Associated with Russia issued on February 24, 2024
https://fintrac-canafe.canada.ca/obligations/dir-rus-eng

FINTRAC guidance related to the Ministerial Directive on the Democratic People's Republic of Korea issued on December 9, 2017
https://fintrac-canafe.canada.ca/obligations/dir-dprk-eng

FINTRAC guidance related to the Ministerial Directive on Financial Transactions Associated with the Islamic Republic of Iran issued on July 25, 2020 (Updated on February 24, 2024)
https://fintrac-canafe.canada.ca/obligations/dir-iri-eng

FINTRAC Operational alert: Laundering of the proceeds of romance fraud
https://fintrac-canafe.canada.ca/intel/operation/rf-eng

FINTRAC Operational Alert: Terrorist Activity Financing
https://fintrac-canafe.canada.ca/intel/operation/taf-eng.pdf

FINTRAC Operational Alert: Updated indicators: Laundering the proceeds of crime through underground banking schemes
https://fintrac-canafe.canada.ca/intel/operation/ml-rec-eng.pdf

FINTRAC Special Bulletin on financial activity associated with suspected sanctions evasion
https://fintrac-canafe.canada.ca/intel/bulletins/sanctions-eng

FINTRAC: Special Bulletin on the use of the legal profession in money laundering and sanctions evasion
https://fintrac-canafe.canada.ca/intel/bulletins/legal-juridique-eng.pdf

FINTRAC: Special Bulletin on laundering the proceeds of crime through online gambling sites
https://fintrac-canafe.canada.ca/intel/bulletins/gambling-jeu-eng.pdf

FINTRAC: The role of virtual currency automated teller machines in laundering the proceeds of crime
https://fintrac-canafe.canada.ca/intel/advisories-avis/atm-ga-eng

FINTRAC: Underground Banking through Unregistered Money Services Businesses
https://fintrac-canafe.canada.ca/intel/advisories-avis/bank-eng

FINTRAC: Updated Indicators: Laundering of proceeds from human trafficking for sexual exploitation
https://fintrac-canafe.canada.ca/intel/operation/oai-hts-2021-eng

Fisheries and Oceans Canada: Illegal, Unreported and Unregulated (IUU) Fishing
https://www.dfo-mpo.gc.ca/international/isu-iuu-eng.htm

Global Affairs Canada: Canada's Fight against Foreign Bribery - twenty-fourth Annual Report to Parliament
https://www.international.gc.ca/transparency-transparence/bribery-corruption/2022-2023.aspx?lang=eng

National Coalition Against Contraband Tobacco: Submission to the House of Commons Standing Committee on Public Safety and National Security – Study on Gun Control, Illegal Arms Trafficking and the Increase in Gun Crimes Committed by Members of Street Gangs
https://static1.squarespace.com/static/58e3aecb5016e199be776da1/t/62212ca8259d0159d7eb77f2/1646341288966/NCACT+SECU+Study+Submission.pdf

Public Safety Canada: Listed Terrorist Entities
https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/lstd-ntts/index-en.aspx

Royal Canadian Mounted Police: Fraud Prevention Month 2024: Fighting fraud in the digital era
https://rcmp.ca/en/news/2024/02/fraud-prevention-month-2024-fighting-fraud-digital-era

Royal Canadian Mounted Police: Statistics pertaining to counterfeit Canadian currency
https://www.rcmp-grc.gc.ca/fsis-ssji/statistics-statistiques-eng.htm

Statistics Canada: Juristat Bulletin Quick Fact: Trafficking in persons in Canada, 2022
https://www150.statcan.gc.ca/n1/pub/85-005-x/2023001/article/00002-eng.htm#r23

Statistics Canada: Incident-based crime statistics, by detailed violations, Canada, provinces, territories, Census Metropolitan Areas and Canadian Forces Military Police
https://www150.statcan.gc.ca/t1/tbl1/en/tv.action?pid=3510017701&pickMembers%5B0%5D=1.1&pickMembers%5B1%5D=2.44&cubeTimeFrame.startYear=2013&cubeTimeFrame.endYear=2023&referencePeriods=20130101%2C20230101

Statistics Canada: Police-reported crime for selected offences, Canada, 2022 and 2023
https://www150.statcan.gc.ca/n1/daily-quotidien/240725/t005b-eng.htm

Annex D: List of Key Acronyms and Abbreviations

Acronyms	Abbreviations
ACMLTF	Advisory Committee on Money Laundering and Terrorist Financing
AGC	Attorney General of Canada
AI	Artificial Intelligence
AML	Anti-Money Laundering
AML/ATF	Anti-Money Laundering and Anti-Terrorist Financing
ATF	Anti-Terrorist Financing
ATM	Automated Teller Machine
BC	British Columbia
CAD	Canadian Dollar
CAFC	Canadian Anti-Fraud Centre
CBSA	Canada Border Services Agency
CIFA-BC	Counter-Illicit Finance Alliance British Columbia
CIROC	Canadian Integrated Response to Organized Crime
CISC	Criminal Intelligence Service Canada
COVID-19	Coronavirus Disease 2019
CPA	Chartered Professional Accountant
CRA	Canada Revenue Agency
CREA	Canadian Real Estate Association
CSA	Canadian Securities Administrators
CSIS	Canadian Security Intelligence Service
CSP	Company Service Provider
CDSS	Canadian Drugs and Substances Strategy
DeFi	Decentralized Finance
DPMS	Dealers in Precious Metals and Stones
DPRK	Democratic People's Republic of Korea
D-SIB	Domestic Systemically Important Bank
FATF	Financial Action Task Force
FCAC	Financial Consumer Agency of Canada
FDI	Foreign Direct Investment
FinCEN	Financial Crimes Enforcement Network
FINTRAC	Financial Transactions and Reports Analysis Centre of Canada
FLSC	Federation of Law Societies of Canada
G7	Group of Seven (Canada, France, Germany, Italy, Japan, the United Kingdom and the US)
GAC	Global Affairs Canada
GBA+	Gender-based Analysis Plus
GDP	Gross Domestic Product
HIO	Heads of International Organization
IMLIP	Integrated Money Laundering Intelligence Partnership
IMF	International Monetary Fund
IMVE	Ideologically Motivated Violent Extremism

IRCC	Immigration, Refugees and Citizenship Canada
ISC	Individuals with Significant Control
ISED	Innovation, Science and Economic Development Canada
IVTS	Informal Value Transfer System
J5	Joint Chiefs of Global Tax Enforcement
MIC	Mortgage Investment Corporation
ML	Money Laundering
MOU	Memorandum of Understanding
MSB	Money Services Business
NPO	Non-Profit Organization
OCG	Organized Crime Group
OPP	Ontario Provincial Police
OSFI	Office of the Superintendent of Financial Institutions
PCMLTFA	Proceeds of Crime (Money Laundering) and Terrorist Financing Act
PEP	Politically Exposed Person
PMVE	Politically Motivated Violent Extremism
PPSC	Public Prosecution Service of Canada
PSPC	Public Services and Procurement Canada
RCM	Regulatory Compliance Management
RCMP	Royal Canadian Mounted Police
RMVE	Religiously Motivated Violent Extremism
RPAA	Retail Payment Activities Act
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TBML	Trade-Based Money Laundering
TF	Terrorist Financing
US	United States
WLATM	White Label Automated Teller Machine