Department of Finance Canada
Ministère des Finances Canada

Updated Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada

March 2023

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 and comprehensive Anti-Money Laundering and Anti-Terrorist Financing (AML/ATF) Regime, which promotes the integrity of the financial system and the safety and security of Canadians. It supports combating transnational organized crime and is a key element of Canada's counter-terrorism strategy.

The Government of Canada first conducted an assessment to identify inherent money laundering and terrorist financing risks in Canada in 2015 when it published the *Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada*[1] (the 2015 Report). Since 2015, the government has been monitoring and assessing new risks on a continual basis and developed internal analysis to ensure that its understanding of these risks remains current and up-to-date. In conjunction with this, various government partners and agencies such as the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), have also published strategic intelligence reports to promote the awareness of new emerging trends in risks by reporting entities and the public. This report consolidates the work conducted before the release of the 2015 report and between 2015 and 2020 to provide a systematic and comprehensive update of all the areas assessed in 2015 using a similar approach and methodology. Furthermore, it also extends Canada's assessment to other new areas not assessed in 2015.

It is important to note that this report provides an overview of the risks of money laundering and terrorist financing before the application of any mitigation measures. Those measures include a range of legislative, regulatory and operational actions that prevent, detect and disrupt money laundering and terrorist financing. Sectors confronted with higher inherent money laundering and terrorist financing risks assessed in this report typically also have strong mitigation measures in place to limit those risks. The report presents overall vulnerabilities and risks, such as for sectors or products as a whole. Risks and risk mitigation practices will vary, and so in practice, should be considered on a case-by-case basis. This report is a tool to support the assessment of money laundering and terrorist financing risks, and the updates since 2015 recognize that the government must be vigilant to avoid systemic and unconscious bias influencing how it is applied.

Canada's AML/ATF Regime provides a coordinated approach to mitigating the inherent risks identified in this assessment and in combating money laundering and terrorist financing more broadly. The AML/ATF Regime is operated by 13 federal Regime partners, which all contributed to the development of the report, coordinated by the Department of Finance Canada (Finance Canada). The inherent risks identified are being addressed through a strong regime that focuses on policy coordination, both domestically and internationally; the prevention and detection of money laundering and terrorist financing in Canada; disruption activities, including investigation and prosecution and the seizure of illicit assets; and the implementation of measures to continually enhance the AML/ATF Regime.

This report provides critical risk information to the public and, in particular, to over 24,000 regulated entities across the country[2] that have reporting obligations under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA), whose understanding of inherent, foundational money laundering and terrorist financing risks is vital in applying the preventive measures and controls required to effectively mitigate these risks. Building off of the 2015 Report, the Government of Canada encourages these entities to use the findings in this report to continue to inform their efforts in assessing and mitigating risks. Having an up-to-date understanding of Canada's risk context and the intrinsic properties that expose sectors and products to inherent money laundering and terrorist financing risks in Canada is important in being able to apply measures to effectively mitigate them.

This updated report also responds to the Financial Action Task Force's (FATF) global AML/ATF standards calling on all members to assess money laundering and terrorist financing risks on an ongoing basis. This report will be considered as part of the next FATF Mutual Evaluation of Canada, which will assess Canada against these global standards.

[1] 2015 Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada.

[2] As of November 2020, received from FINTRAC.

The inherent risk assessment consists of an assessment of the money laundering and terrorist financing threats and inherent money laundering and terrorist financing vulnerabilities in Canada as a whole (e.g., economy, geography, demographics) and the country's key economic sectors and financial products, while taking into account the consequences of money laundering and terrorist financing. The overall inherent money laundering and terrorist financing risks were assessed by matching the threats with the inherently vulnerable sectors and products through the money laundering and terrorist financing methods and techniques that are used by money launderers, terrorist financiers and their facilitators, to exploit these sectors and products. By establishing a relationship between the threats and vulnerabilities, a series of inherent risk scenarios were constructed, allowing one to identify the sectors and products that are exposed to the highest money laundering and terrorist financing risks.

The money laundering threat assessment examined 23 criminal activities in Canada that are most associated with generating proceeds of crime that may be laundered. It also examined the money laundering threat emanating from third-party money laundering, which includes the use of money mules, nominees and professional money launderers. The money laundering threat was rated very high for illicit drug trafficking, certain types of fraud, illegal gambling, corruption, collusion and bribery, and third-party money laundering. Transnational organized crime groups (OCGs) and professional money launderers are the key money laundering threat actors in the Canadian context. Many of these threats are similar to those faced by several other countries.

The terrorist financing threat was assessed for the groups and actors listed by the United Nations and Canada that are of greatest concern to Canada. The assessment indicates that there are networks operating in Canada that are suspected of raising, collecting and transmitting funds to various terrorist groups. However, based in part on the existing strengths of the regime, the terrorist financing threat in Canada is not as pronounced as in other regions of the world, where weaker anti-terrorist financing regimes can be found and where terrorist groups have established a foothold, both in terms of operations but also in financing their activities.

The inherent money laundering and terrorist financing vulnerabilities are presented for 33 economic sectors and financial products. The assessment indicates that there are many sectors and products that are highly vulnerable to money laundering and terrorist financing. Of the assessed areas, domestic banks, corporations (especially, private corporations), certain types of money services businesses and express trusts were rated the most vulnerable, or very high. In addition, 18 sectors and products had a vulnerability rating of high, nine sectors and products had a vulnerability rating of medium and one sector had a vulnerability rating of low. Many of the sectors and products are highly accessible to individuals in Canada and internationally and are associated with a high volume, speed and frequency of transactions. Many conduct a significant amount of transactional business with high-risk clients and are exposed to high-risk jurisdictions that have weak AML/ATF regimes and significant money laundering and terrorist financing threats. There are also opportunities in many sectors to undertake transactions with varying degrees of anonymity and to structure transactions in a complex manner.

By connecting the threats with the inherently vulnerable sectors or products, the assessment revealed that a variety of them are exposed to very high inherent money laundering risks involving threat actors (e.g., OCGs and third-party money launderers) laundering illicit proceeds generated from ten groups of profit-oriented crimes. The assessment also identified four very high inherent terrorist financing risk scenarios that involve six different sectors that have been assessed to be very highly vulnerable to terrorist financing, combined with one high terrorist financing threat group of actors.

This update to Canada's risk assessment highlights the importance of maintaining a shared understanding of inherent money laundering and terrorist financing risks in Canada on an ongoing basis. Criminal threats can evolve over time as criminals continuously look for new methods and techniques to obfuscate the source of illicit funds, for example by leveraging technological innovation. In addition, it is important to retain an awareness that many money laundering and terrorist financing vulnerabilities, threats and methods can remain the same or consistent over time. As such, this report provides a comprehensive overview of the money laundering and terrorist financing threats, vulnerabilities and risks that have persisted since the 2015 report, as well as of new trends identified in the risk landscape's evolution.

Based on additional evidence from this updated assessment, the threat levels for tax evasion, illegal gambling, and wildlife trafficking have increased since the 2015 report, while they decreased for illegal tobacco smuggling and trafficking. This was often a reflection of changes in the average sophistication and capability exhibited by the threat actors involved. For example, concerns around tax evasion have increased following growing trends around the usage of complex offshore corporate structures and accounts and the leveraging of expertise from facilitators such as lawyers, accountants and financial advisors.

Some threat levels remained the same but were marked by new dynamics and trends that push government and private sectors to adapt. New typologies of threats and vulnerabilities have notably emerged from the fentanyl trade, new types of online mass-marketing fraud, capital market fraud and extortion schemes. Growing vulnerabilities in the real estate market partly a result of rapid price increases in some regions of Canada and constant technological developments around virtual assets were other notable trends.

This update to Canada's risk assessment also broadens the scope of the risks assessed in 2015. New issues assessed in this update include, among others, potential money laundering threats generated by illegal fishing activities, as well as inherent vulnerabilities faced by the armoured car sector, partnerships, unregulated mortgage lenders, import/export companies, freight forwarders and custom brokers. Canada also conducted a preliminary terrorist financing threat assessment of ideologically motivated violent extremists.

Finally, the COVID-19 pandemic has helped demonstrate how adaptable the Canadian financial sector is, with more and more consumers adopting digital channels as well as new financial services and products being made available by emerging technologies. The pandemic has also shown that criminal actors are adapting in the current context by leveraging online schemes and COVID-related fraud to generate funds. The shift to digital platforms and financial products may also present new opportunities for criminals and terrorist organizations to move funds. Furthermore, border closures disrupted traditional cash-courier techniques and affected trade-based fraud methodologies, while regional lockdowns of non-essential businesses such as casinos led to reports of increased underground illegal gambling and related money laundering activities.

New experiences from the COVID-19 pandemic reinforce the importance of national authorities and the private sector monitoring and understanding of evolving risks on an ongoing basis. The updated assessment has and will continue to help enhance Canada's AML/ATF Regime, further strengthening the comprehensive approach it already takes to risk mitigation and control domestically, including with the private sector and with international partners. It also complements and completes the various information and documents published by the government since 2015 around new risks and typologies observed in relation to certain sectors or specific issues as they were unfolding.

Forward Looking Plan

The Updated Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada, unless otherwise noted, reflects analysis that was available up to December 2020. Certain targeted updates have been made to the report to communicate early findings for new and emerging risks, such as Ideologically Motivated Violent Extremism.

Emerging risks such as the use of crowdfunding platforms, payment service providers, cryptocurrency as well as the risk of actors trying to evade sanctions, for example, in relation to Russia's unprecedented aggression towards Ukraine will continue to be monitored. Future updates on these risks will be included in subsequent updates to this report.

Introduction

Money laundering and terrorist financing compromise the integrity of the international financial system and are a threat to global safety and security. Money laundering is the process used by criminals to conceal or disguise the origin of criminal proceeds to make them appear as if they originated from legitimate sources. Money laundering frequently benefits the most successful and profitable domestic and international criminals and organized crime groups. Terrorist financing, in contrast, is the collection and provision of funds from legitimate or illegitimate sources for terrorist activity. It supports and sustains the activities of domestic and international terrorists that can result in terrorist attacks in Canada or abroad causing loss of life and destruction.

The Government of Canada is committed to combating money laundering and terrorist financing, while respecting the Constitutional division of powers, the *Charter of Rights and Freedoms* and the privacy rights of Canadians. To do so, the Government of Canada has put in place a robust and comprehensive Anti-Money Laundering and Anti-Terrorist Financing (AML/ATF) Regime. The Regime is operated by 13 federal departments and agencies each responsible for certain elements according to their mandates and expertise, coordinated by Finance Canada. Provincial and municipal law enforcement bodies and provincial financial sector and other regulators are also involved in combating these illicit activities. Within the private sector, there are over 24,000 Canadian financial institutions and non-financial businesses and professions [3] with reporting obligations under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA), known as reporting entities that play a critical frontline role in efforts to prevent and detect money laundering and terrorist financing.

Regime partners' understanding of money laundering and terrorist financing risks plays a key role in the government's ability to effectively combat these illicit activities. That understanding helps to support the policy-making process to effectively address vulnerabilities and other potential gaps in the Regime. It helps to inform operational decisions about priority setting and resource allocation to combat threats and to focus on those that have the greatest economic, social and political consequences. It also plays a central role in how the private sector, especially reporting entities, applies its risk-based approaches and mitigates their risks. Overall, Regime partners' understanding of risks helps them focus on adequately mitigating the risks of greatest concern in Canada.

Given the central role that the understanding of risk plays in the Regime, the Government of Canada has built on existing practices to update the 2015 *Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada* (the 2015 Report).[4] This update consists of building on the foundational risk assessment that was published in 2015. This report presents the results of the updated assessment of inherent money laundering and terrorist financing risks in Canada. These are the fundamental risks in Canada, which the AML/ATF Regime seeks to control and mitigate.

This report specifically examines these risks in relation to key economic sectors and financial products in Canada and it assesses the extent to which key features make Canada vulnerable to being exploited by threat actors to launder funds and to finance terrorism. It is meant to raise awareness about Canada's risk context and the intrinsic properties that expose these sectors and products to money laundering and terrorist financing risks in Canada. The vast majority of businesses, professions and sectors assessed in this report follow Canadian laws and contribute to the social and economic prosperity of the country; only a very small subset of actors are complicit in illicit activities such as money laundering.

[3] As of November 2020, received from FINTRAC.

[4] In addition to the 13 federal Regime partners, the Bank of Canada, Environment and Climate Change Canada, Fisheries and Oceans Canada as well as government stakeholders from the provinces and territories (either directly or indirectly through agencies such as the Criminal Intelligence Service Canada) contributed to the development of the risk assessment update.

Nonetheless, properly understanding these inherent money laundering and terrorist financing risks is critical in being able to identify and apply measures to effectively mitigate them. In this regard, the Government expects that this updated report will be used by financial institutions and other reporting entities to understand how and where they may be most vulnerable and exposed to inherent money laundering and terrorist financing risks. The report presents overall vulnerabilities and risks, such as for sectors or products as a whole. Risks and risk mitigation practices will vary, and so in practice, should be considered on a case-by-case basis. This report is a tool to support that assessment. The report complements other analysis undertaken by Regime partners and will contribute to setting priorities and assessing the effectiveness of measures to address money laundering and terrorist financing risks.

The first chapter describes Canada's AML/ATF Regime and the comprehensive approach taken to mitigate the inherent money laundering and terrorist financing risks that are the subject of this assessment. The second chapter provides a general description of the methodology used to assess the inherent money laundering and terrorist financing risks in Canada, while the subsequent three chapters present the results of the updated assessment of the money laundering and terrorist financing threats and inherent money laundering and terrorist financing vulnerabilities. These components of risk are then combined in the final chapter to provide an assessment of the inherent money laundering and terrorist financing risks in Canada, including setting out a number of inherent risk scenarios and case examples.

Unless otherwise noted, the content of the report reflects what was available up to December 31, 2020, and it excludes some information, intelligence and analysis for reasons of national security.

Chapter 1: Risk Mitigation

Canada has a comprehensive AML/ATF Regime that provides a coordinated approach to mitigating the inherent money laundering and terrorist financing risks identified in this assessment and in combating money laundering and terrorist financing more broadly. This chapter will briefly review the framework that exists in Canada to prevent, detect and disrupt money laundering and terrorist financing. The Regime also complements the work of law enforcement and intelligence agencies engaged in fighting domestic and transnational organized crime as well as terrorism, notably as part of Canada's Counter-Terrorism Strategy.[5]

The AML/ATF Regime is operated by 13 federal Regime partners, nine of which receive incremental funding totalling nearly $70 million annually from the AML/ATF horizontal funding initiative.[6] The nine funded partners are the Canada Border Services Agency (CBSA), Canada Revenue Agency (CRA), the Canadian Security Intelligence Service (CSIS), Finance Canada, Justice Canada, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), the Public Prosecution Service of Canada (PPSC), Public Services and Procurement Canada (PSPC) and the Royal Canadian Mounted Police (RCMP). The remaining four Regime partners are Global Affairs Canada (GAC), Innovation, Science and Economic Development Canada (ISED), the Office of the Superintendent of Financial Institutions (OSFI) and Public Safety Canada. Although not receiving dedicated funding from the AML/ATF horizontal funding initiative, these four partners make important contributions to the Regime.

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

(i) Policy and Coordination

The first pillar consists of the Regime's policy and legislative framework as well as its domestic and international coordination, which is 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*.

[5] Counter-terrorism Strategy (publicsafety.gc.ca), December 2020.

[6] Departmental Results Report 2018–19: Supplementary Information Tables.

The PCMLTFA requires prescribed financial institutions as well as certain non-financial businesses and professions,[7] 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 certain other prescribed transactions. It also creates obligations for the reporting entities to identify money laundering and terrorist financing risks and to put in place measures to mitigate those risks, including through ongoing monitoring of transactions and enhanced customer due diligence measures.

The PCMLTFA also establishes an information sharing regime where, under prescribed conditions respecting individuals' privacy, information submitted by the reporting entities is analyzed by FINTRAC and the results are disseminated to Regime partners. The information disseminated under the PCMLTFA can be intelligence used to support domestic and international partners in the investigation and prosecution of money laundering and terrorist financing related offences, or can be in the form of trends and typologies reports used to educate the public, including reporting entities, on money laundering and terrorist financing issues. In addition to the PCMLTFA, other statutes also contribute a comprehensive AML/ATF Regime. For example, the *Income Tax Act* creates obligations around trusts registration with CRA, while the *Canadian Business Corporations Act* sets out beneficial ownership transparency requirements for federally incorporated companies.

Given the number of Regime participants and the complexity of money laundering and terrorist financing issues, the effective regime-wide coordination of strategic, policy and operational matters is important. All federal partners share responsibility for the outcomes of the Regime, which is governed by various inter-departmental committees with the participation of senior officials from each organization. These committees work together to maintain an efficient regime with a focus on both policy and operations.

There is also frequent collaboration and discussion between the public and private sectors. For example, the Advisory Committee on Money Laundering and Terrorist Financing (ACMLTF) is a public-private discussion forum to support emerging issues and overall AML/ATF policy.[8] Private sector representatives are invited to provide their perspective and advice on Canada's AML/ATF Regime both within a domestic context, including its effectiveness and efficiency, and in support of international work. ACMLTF also provides an opportunity for the Government to provide valuable feedback to the private sector on overall AML/ATF trends and efforts. This committee benefits all participants by fostering more effective communication and results for the Regime writ large.

In addition, given that many serious forms of money laundering and terrorist financing often have international dimensions, Canada's cooperation internationally is also a key component. International cooperation is a core practice of the Regime, and for many partners it is conducted on a routine basis, in particular in supporting investigations and prosecutions of money laundering and terrorist financing. This includes information exchanges between FINTRAC and other financial intelligence units from partner countries[9] and through formal mutual legal assistance led by Justice Canada.

Canada recognizes that protecting the integrity of the international financial system from money laundering and terrorist financing requires playing a strong international role to broadly increase legal, institutional, and operational capacity globally. Canada's international AML/ATF initiatives are advanced through the leadership role that it plays in the FATF, the G7, the G20, the Egmont Group of Financial Intelligence Units and the counter-financing work stream of the Global Coalition against Daesh.[10]

[7] This refers to casinos, real estate brokers/agents and real estate developers, dealers in precious metals and stones, British Columbia notaries and accountants. For some of these entities, obligations are only when carrying out certain activities on behalf of their clients.

[8] Advisory Committee on Money Laundering and Terrorist Financing (ACMLTF) - Canada.ca

[9] Where a memorandum of understanding has been signed between FINTRAC and the foreign financial intelligence unit.

[10] The Global Coalition against Daesh consists of 83 members that are committed to tackling Daesh on all fronts, including tackling Daesh's financing and economic infrastructure.

Canada is a founding member of the FATF and an active participant. The FATF develops international AML/ATF standards, and monitors their effective implementation among the 39 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 with weaker regimes, including through the Anti-Crime Capacity Building Program and the Counter-Terrorism Capacity Building Program, which are led by GAC.

(ii) Prevention and Detection

The second pillar provides strong measures to prevent individuals from placing illicit proceeds or terrorist-related funds into the financial system, while having correspondingly strong measures to detect the placement and movement of such funds. At the centre of this prevention and detection approach are the reporting entities who are core to the financial system and implement the prevention and detection measures under the PCMLTFA, and the regulators, FINTRAC and OSFI principally, that supervise them. FINTRAC is the primary agency conducting AML/ATF assessments of federally regulated financial institutions to promote compliance with the PCMLTFA and its associated regulations, whereas 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.

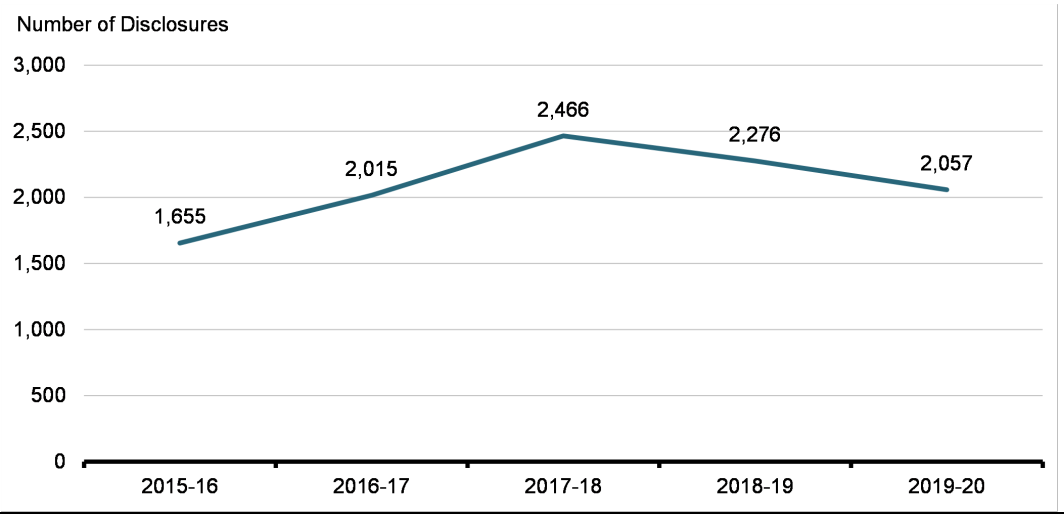
Greater transparency of corporations and trusts also contributes to preventing and detecting money laundering and terrorist financing. This is fostered by requirements on financial institutions, money services businesses (MSBs), life insurance dealers, and securities dealers to identify the beneficial owners of the corporations and trusts with whom they do business.[11] Provincial and federal corporate laws, registries and securities regulations also contribute in preventing and detecting money laundering and terrorist financing in Canada. Recent and ongoing federal, provincial and territorial legislative changes will require that information on the beneficial ownership of corporations is made available to relevant law enforcement agencies and authorities on a timely basis. As part of Budget 2022 the government committed to a publicly accessible beneficial ownership registry of federally incorporated businesses by 2023.

FINTRAC is also Canada's financial intelligence unit; it acts at arm's length and is independent from the police services, law enforcement agencies and other entities to which it is authorized to disclose financial intelligence. The chart below provides the annual number of cases disclosed by FINTRAC to partners from 2015-16 to 2019-20. For example, in 2019-20, FINTRAC made 2,057 disclosures to Regime partners. Of these, 1,582 were associated with money laundering, while 296 dealt with cases of terrorist activity financing and other threats to the security of Canada. 179 disclosures dealt with all three areas.

[11] For the other reporting sectors or professions, these requirements came into force on June 1, 2021.

Chart 1[12]

FINTRAC Case Disclosures from 2015–16 to 2019–20



(iii) Disruption

The final pillar deals with the disruption of money laundering and terrorist financing. Regime partners, such as CSIS, CBSA and the RCMP, supported by FINTRAC's intelligence disclosures and analysis activities, undertake financial investigations in relation to money laundering, terrorist financing, and other profit-oriented crimes. CRA also plays an important role in investigating tax evasion and its associated money laundering and in detecting charities that are at risk and taking actions to prevent them from being abused to finance terrorism. CBSA administers the Cross-Border Currency Reporting program, and transmits information from reports and seizures to FINTRAC.

Ultimately, PPSC prosecutes financial crimes to the fullest extent of the law. The restraint and confiscation of proceeds of crime is also an important law enforcement component of the Regime. PSPC manages all seized and restrained property for criminal cases prosecuted by the Government of Canada.

The Regime also has a robust terrorist listing process to freeze terrorist assets, pursuant to the *Criminal Code* and the *Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism*, which is led by Public Safety Canada and GAC, respectively. Canada has 113 terrorist-related listings under the two processes.

Oversight and Enhancements

Canada's AML/ATF Regime is reviewed on a regular basis by a variety of bodies to ensure that it operates effectively, in keeping with its legislative mandate, while respecting the Constitutional division of powers, the *Charter of Rights and Freedoms* and the privacy rights of Canadians.

The Parliament of Canada is required by statute to undertake a comprehensive review of the PCMLTFA, and indirectly the Regime, every five years. In addition to the parliamentary review, there are other periodic reports on performance,[13] reviews and audits, including a mandatory privacy audit of FINTRAC by the Office of the Privacy Commissioner every two years. Internationally, Canada's Regime is assessed by the FATF against its global AML/ATF standards and is subject to the FATF's follow-up process.

[12] Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). Safe Canadians, Secure Economy. Annual Report 2019-20. Ottawa: FINTRAC, 2020.

[13] See, for example, Finance Canada's Departmental Plan, which explains the AML/ATF Regime's spending plans, priorities, and expected results, available for 2020-21, at Departmental Plan 2020-2021, as well as its Departmental Results Report, available for 2019, at Departmental Results Report 2018–19.

Since the publication of the 2015 Report, the Government has made significant amendments to its legislation and regulations. Notably, in July 2019, the Government finalized regulatory amendments to regulate money services businesses dealing in virtual currency, as well as to include foreign money service businesses (FMSBs) in Canada's AML/ATF Regime, update customer due diligence requirements and beneficial ownership reporting requirements, modernize client identification measures, update the schedules to the regulations, and clarify a number of existing requirements.[14] In June 2020, further regulatory amendments were finalized to apply stronger customer due diligence requirements and beneficial ownership requirements to certain businesses and professions, modify the definition of business relationship for the real estate sector, align customer due diligence measures for casinos with international standards, align virtual currency record-keeping obligations with international standards, and clarify the cross border currency reporting program.[15]

As part of Budget 2019, the Government announced an investment of over $220 million starting in 2019-20 to modernize Canada's AML/ATF Regime by strengthening federal policing operations and its technology infrastructure, increasing operational capacity for FINTRAC, strengthening available data resources, launching a pilot project to enhance information sharing, expertise, and coordination of financial crime investigations and prosecutions, building capacity and expertise related to trade-based money laundering[16] (TBML) and trade fraud, as well as increasing tax compliance and deterring financial crime in the real estate sector.[17] The Government also made amendments to the *Criminal Code* to add an alternative requirement of recklessness to the offence of money laundering.[18]

In 2020, the Government announced additional funding of almost $700 million to combat financial crime. Approximately $70 million of that funding would be allocated directly to strengthening Canada's AML/ATF framework and enhance FINTRAC's effectiveness to identify and meet evolving threats.[19] $606 million will be used to fund new initiatives and extend existing programs to focus on individuals who avoid taxes by hiding income and assets offshore, enhance the audit function targeting higher-risk tax filings, including those of high-net worth individuals, and strengthen the CRA's ability to fight financial crimes such as money laundering and terrorist financing by upgrading tools and increasing international cooperation.[20]

Canada remains committed and engaged, both domestically and internationally, in the fight against money laundering and terrorist financing. The risks are present and evolving. Canada has a strong regime and it remains committed to take appropriate action to mitigate the money laundering and terrorist financing risks identified in this assessment and to continue to assess evolving risks on an ongoing basis.

Implementation

The Government of Canada expects that this report will be used by financial institutions and other reporting entities to contribute to their understanding of how and where they may be most vulnerable and exposed to inherent money laundering and terrorist financing risks. FINTRAC will continue to include relevant information related to inherent risks in their guidance documentation to assist financial institutions and other reporting entities in integrating such information in their own risk assessment methodology and processes so that they can effectively implement controls to mitigate money laundering and terrorist financing risks. The valuable lessons learned from this exercise will also be used to help set priorities for policy development and operational efforts to combat money laundering and terrorist financing.

[14] Regulations Amending Certain Regulations Made Under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, 2019.

[15] Regulations Amending the Regulations Amending Certain Regulations Made Under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, 2019.

[16] Trade-based money laundering is defined by the FATF as the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origins.

[17] Budget 2019.

[18] This criminalizes the activity of moving money on behalf of another person or organization while being aware that there is a risk that this activity could be money laundering and continuing with that activity in spite of the risk.

[19] Economic and Fiscal Snapshot (July 8, 2020). Economic and Fiscal Snapshot (July 8, 2020).

[20] Fall Economic Statement (November 30, 2020). Fall Economic Statement (November 30, 2020).

Chapter 2: Overview of the Methodology to Assess Inherent Money Laundering and Terrorist Financing Risks in Canada

Overview

In 2015, the Government of Canada developed an assessment model to identify and understand inherent money laundering and terrorist financing risks in Canada, and their relative importance, through a rigorous and systematic analysis of qualitative and quantitative data and expert opinion about money laundering and terrorist financing. This update uses the same methodology and continues to provide the basis to think critically and systematically about money laundering and terrorist financing risks, on an ongoing basis, as well as to promote a continued common understanding of these risks and their evolution. This chapter provides an overview of the risk assessment methodology.

Scope of the Methodology

The methodology continues to assess the inherent money laundering and terrorist financing risks, which are the fundamental risks in Canada that are the subject of the broad suite of government and private sector controls and activities to effectively mitigate those risks. Understanding Canada's risk context and the intrinsic properties that expose sectors and products to inherent money laundering and terrorist financing risks in Canada is important to being able to identify and apply measures to effectively mitigate them.

The basis of the risk assessment is that risk is a function of three components: threats, inherent vulnerabilities and consequences. Furthermore, 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.

Key Definitions

Money Laundering and Terrorist Financing Threats: a person or group who has the intention, or may be used as facilitators, to launder proceeds of crime or to fund terrorism.

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

Consequences of Money Laundering and Terrorist Financing: the harm caused by money laundering and terrorism financing, including facilitating criminal and terrorist activity, on a society, economy and government.

Likelihood of Money Laundering and Terrorist Financing: the likelihood of money laundering and terrorist financing threats exploiting inherent vulnerabilities.

The money laundering threat was assessed separately from the terrorist financing threat. Although there is some overlap, the nature of these criminal activities is different, warranting separate assessments. In contrast, the assessment of the money laundering and terrorist financing vulnerabilities did not require such separation since money laundering and terrorist financing threats seek to exploit the same set of vulnerable features and characteristics of products and services offered by sectors to launder proceeds of crime or to fund terrorism.

As a first step, the core components of the money laundering and terrorist financing threats and inherent vulnerabilities were identified and categorized. With these categories, criteria were developed to rate the extent of the money laundering and terrorist financing threats and the inherent money laundering and terrorist financing vulnerabilities. These ratings were then used to assess the likelihood of money laundering and terrorist financing occurring, which involved matching the threats with the inherent vulnerabilities, while considering the consequences of money laundering and terrorist financing, which then resulted in the assessment of inherent money laundering and terrorist financing risks. The important types of economic, social and political consequences of money laundering and terrorist financing are identified in the Annex.

Assessing the ML/TF Threats and Inherent Vulnerabilities

Experts from Canada's AML/ATF Regime, supported by a series of workshops, assessed the money laundering and terrorist financing threats and inherent vulnerabilities of sectors and products using the rating criteria set out in the methodology. In addition, the experts harnessed the Regime's store of information, data and analysis to update and rate each threat and vulnerability. Experts provided ratings of low, medium, high or very high using the defined rating criteria to assess the range of threats and inherent vulnerabilities. The individual ratings were then aggregated to arrive at an overall rating.

The money laundering threat in Canada was assessed for 23 criminal activities that are most associated with generating proceeds of crime in Canada as well as the threat from third-party money laundering. The money laundering threat was rated for each criminal activity against four rating criteria, namely the extent of the threat actors' knowledge, expertise and overall sophistication to conduct money laundering; the extent of the threat actors' network, resources and overall capability to conduct money laundering; the scope and complexity of the money laundering activity; and the magnitude of the proceeds of crime being generated annually from the criminal activity. The money laundering threat rating results are presented in Chapter 3.

The money laundering risks Canada faces are global in nature. Canada-linked professional money launderers and transnational organized crime groups (OCG) launder proceeds of crime using complex global networks that involve multiple jurisdictions at all stages of the money laundering cycle. These jurisdictions vary significantly and change based on many factors including the OCG involved, the predicate offence from which the criminal proceeds are derived, and any intermediary jurisdictions where the trade or financial system can be exploited for the purposes of money laundering.

The Financial Action Task Force (FATF) maintains a current list of global jurisdictions as posing higher risks for money laundering and terrorist financing.[21] For all countries identified as high-risk, the FATF calls on all members and urges all jurisdictions to apply enhanced due diligence, and, in the most serious cases, countries are called upon to apply counter-measures to protect the international financial system from the money laundering, terrorist financing, and proliferation financing risks emanating from the jurisdiction.

[21] "Black and grey" lists (fatf-gafi.org).

The terrorist financing threat in Canada was assessed for terrorist groups as well as for foreign terrorist fighters that, based on financial and other intelligence available, are considered either because they represent the greatest risk of engaging in terrorist financing activities, or due to the emerging terrorist financing risks they pose. Foreign terrorist fighters are defined as those who travel abroad to support and fight alongside terrorist groups. The terrorist financing threat of these groups was assessed against six rating criteria, namely the extent of the threat actors' knowledge, expertise and overall sophistication to conduct terrorist financing; the extent of the threat actors' network, resources and overall capability to perform terrorist financing operations; the scope and global reach of their terrorist financing operations; the estimated value of their fundraising activities annually in Canada; the extent of the diversification of their methods to collect, aggregate, transfer and use funds; and the extent to which the funds may be used against Canadian domestic and international interests. The terrorist financing threat rating results are presented in Chapter 4.

The assessment considered the inherent features of Canada that may be exploited by threat actors for illicit purposes (e.g., geography, economy, demographics). Against this, the inherent money laundering and terrorist financing vulnerabilities were assessed for 33 economic sectors and products. The areas were assessed against five rating criteria, namely the inherent characteristics of the assessed areas (size, complexity, accessibility and integration); the nature and extent of the vulnerable products and services; the business relationship with its clients; geographic reach (extent of activity with high-risk jurisdictions and locations of concern); and the degree of anonymity and complexity afforded by the delivery channels. Canada's inherent features and sector and product vulnerability assessment results are presented in Chapter 5.

Assessing the Inherent ML/TF Risks

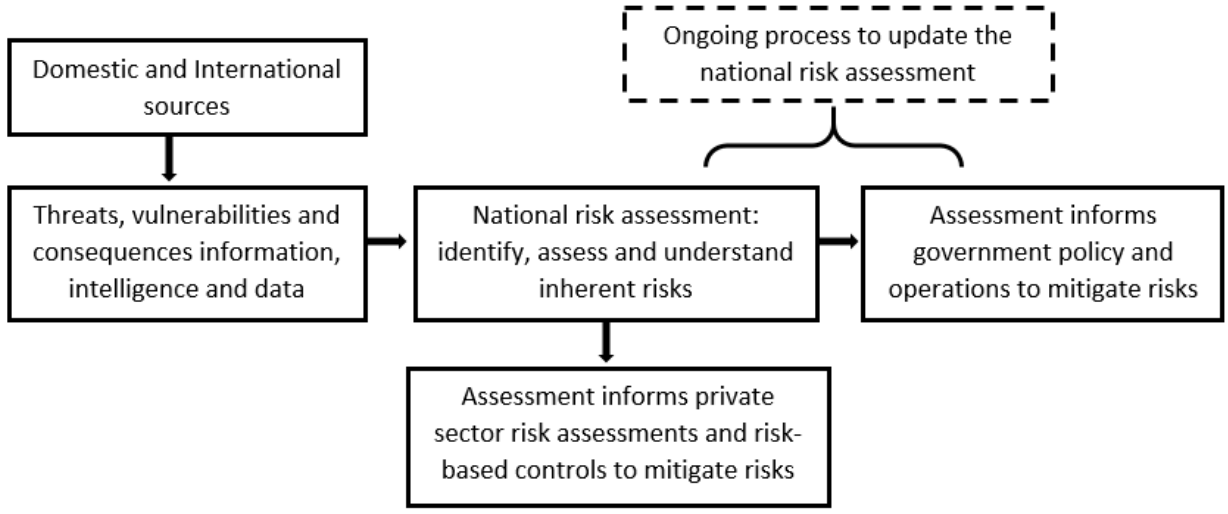
The inherent money laundering and terrorist financing risks were assessed based on the likelihood of money laundering or terrorist financing occurring while considering the consequences of such events. The likelihood of the money laundering or terrorist financing was assessed by matching the money laundering and terrorist financing threats with the inherently vulnerable sectors and products through the money laundering and terrorist financing methods and techniques that are used by threat actors to exploit these sectors and products. Inherent money laundering and terrorist financing risk scenarios were created from these judgements and used to plot the inherent risk results by sector, product or service in a number of illustrative charts. This presentation allows one to compare the different levels of exposure of various sectors and products to inherent money laundering and terrorist financing risks in Canada.[22] The results are presented in Chapter 6.

Risk Assessment and Mitigation Framework

The inherent risk assessment and its methodology should be viewed as one 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 below in Chart 2.

[22] In interpreting the results, one should note that threat actors can abuse multiple sectors and products as part of the same scheme.

Chart 2
Canada's ML/TF Risk Assessment Framework



Chapter 3: Assessment of Money Laundering Threats

Overview

The money laundering threat assessment indicates that there is a broad range of profit-oriented crime conducted by a variety of threat actors in Canada. This criminal activity generates billions of dollars in proceeds of crime annually that might be laundered.

Threat actors who perpetrate profit-oriented crime in Canada range from unsophisticated, criminally-inclined individuals, including petty criminals and street gang members, to criminalized professionals[23] and OCGs.[24] An OCG can be defined as a structured group of three or more persons acting in concert with the aim of committing criminal activities, in order to obtain, directly or indirectly, a financial or other material benefit. In 2020, the Criminal Intelligence Service Canada assessed 506 OCGs and believes that there could be more than 2000 operating in Canada. The majority of Canada-based OCGs are not considered transnational OCGs, even though many have international links and associations. While some of these domestic OCGs represent significant money laundering threats, transnational OCGs with a presence or ties to Canada are generally the most threatening both in terms of generating the most proceeds of crime and in the intensity of efforts to launder the proceeds.[25] The most powerful transnational OCGs in Canada, consist of factions with ties to Italy, Eastern Europe, Latin America and Asia, as well as certain Outlaw Motorcycle Gangs, are involved in multiple lines of profit-oriented crime and have the infrastructure and network to launder large amounts of proceeds of crime on an ongoing basis through multiple sectors using a diverse set of methods to avoid detection and disruption. These OCGs have strong networks and strategic relationships with other criminal organizations both domestically and internationally (e.g., transnational drug cartels).

[23] An individual who holds or purports to hold a professional designation and title in an area dealing with financial matters who uses their professional knowledge and expertise to commit or wittingly facilitate a profit-oriented criminal activity. Criminalized professionals would include lawyers, accountant, notaries, investment and financial advisors, stock brokers and mortgage brokers.

[24] OCGs are present in every region and jurisdiction across Canada, and are particularly active in heavily populated areas such as the B.C. lower mainland, Southern Ontario, and the Greater Montreal Region.

[25] Transnational OCGs operate transnationally for the purpose of obtaining a financial or other material benefit wholly or in part by illegal means, while protecting their activities through a pattern of corruption and/ or violence, or while protecting their illegal activities through a transnational organizational structure and the exploitation of transnational commerce or communication mechanisms.

Transnational OCGs appear to frequently rely on professional money launderers to establish and administer schemes to launder the proceeds emanating from their criminal activities. Large-scale, sophisticated money laundering operations rarely take place in Canada without the employ of professional money launderers. The nexus between transnational OCGs and professional money launderers is a key money laundering threat in Canada. In addition to professional money launderers, unwitting and witting facilitators appear to continue to play a key role in supporting the perpetration of profit-oriented crime and the laundering of criminal proceeds. The corruption of individuals and the infiltration of private and public institutions is also a notable concern as it establishes the conditions to foster money laundering and other criminal activity.

The conduct of larger scale profit-oriented crimes often have a significant international dimension and tend to be supported by transnational distribution networks. These networks exhibit a high level of sophistication and capability in moving illicit goods into (destination), out of (source), or through (transit) Canada, including stolen goods, counterfeit products, illicit drugs, illicit firearms, wildlife and people. Mapped against this sophisticated illicit global supply chain appears to be a correspondingly sophisticated flow of illicit funds and a network to launder these funds. Some threat actors appear to have the sophistication and capability to exploit the global trade and financial systems to clandestinely deal in the transnational trafficking of illicit goods and launder illicit proceeds. This capability includes having criminal associates in legitimate positions of employment in ports of entry, or controlling employees using methods like bribery, blackmail or extortion, in order to have insiders facilitate the movement of illicit goods and proceeds into and out of Canada. These threats also appear to have the ability to exploit the AML/ATF weaknesses of foreign countries or situations of unrest or conflicts occurring in foreign countries to facilitate money laundering and other criminal activities.

Discussion of the Money Laundering Threat Assessment Results

Experts assessed the money laundering threat for 23 profit-oriented crimes and third-party money laundering using the following criteria:

1. Sophistication: the extent to which the threat actors have the knowledge, skills and expertise to launder criminal proceeds and avoid detection by authorities.
2. Capability: the extent to which the threat actors have the resources and network to launder criminal proceeds (e.g., access to facilitators, links to organized crime).
3. Scope: the extent to which threat actors are using financial institutions and other sectors to launder criminal proceeds.
4. Proceeds of Crime: the magnitude of the estimated dollar value of the proceeds of crime being generated annually from the profit-oriented crime.

As presented in Table 1, eight profit-oriented crimes and third-party money laundering were rated as a very high money laundering threat, ten were rated high, five were rated medium, and none were rated low.

Table 1
Overall Money Laundering Threat Rating Results

Very High Threat Rating	
Capital Markets Fraud	Illicit Drug Trafficking
Commercial (Trade) Fraud	Mass Marketing Fraud
Corruption and Bribery	Mortgage Fraud
Illegal Gambling	Third-Party Money Laundering
High Threat Rating	
Currency Counterfeiting	Payment Card Fraud
Counterfeiting and Piracy	Pollution Crime
Human Smuggling	Robbery and Theft
Human Trafficking	Tax Evasion/Tax Fraud
Identity Fraud	Tobacco Smuggling and Trafficking
Medium Threat Rating	
Extortion	Loan Sharking
Firearms Smuggling and Trafficking	Wildlife Crime
Illegal Fishing	

Very High Money Laundering Threat

ML Threat from Capital Markets Fraud: Securities fraud, including investment misrepresentation and other forms of capital markets fraud-related misconduct, such as insider trading and market manipulation, continues to occur in Canada. When this fraud occurs, it frequently involves large dollar amounts and a significant number of investors. While fewer Canadians are being approached with investment fraud (18 per cent in 2017, down from 22 per cent in 2016 and 27 per cent in 2012), just as many Canadians are falling victim to investment fraud with the level of fraud victimization remaining steady at 4 per cent.[26] Although it is challenging to be definitive on the actual amount of reported losses, capital markets fraud is a rich source of proceeds of crime. Most of the large-scale securities frauds in Canada have been perpetrated by criminalized professionals, who have (or purport to have) professional credentials and financial expertise.

Perpetrating capital markets fraud, especially the larger, more elaborate national and international schemes (such as Ponzi schemes), requires significant knowledge and expertise and, often, access to a network of witting or unwitting facilitators to help orchestrate and perpetuate the fraud. Alongside the sophisticated fraudulent schemes, there are sophisticated money laundering schemes designed to integrate and legitimize the fraud-related proceeds into the financial system. Money laundering schemes in this context would involve a range of sectors and methods, including shell or front companies, electronic funds transfers (EFTs), structuring and/or smurfing deposits[27] and nominees. However, an emerging trend that has been observed is the presence of Internet scammers in capital markets fraud, using the Internet and other high technology (as well the public's interest in emerging technology, such as blockchain) to commit capital markets fraud.

[26] 2020 CSA Investor Index, https://mbsecurities.ca/about-msc/pubs/csa_index_2020.pdf

[27] Structuring is a money laundering technique whereby criminal proceeds (i.e., cash or monetary instruments) are deposited at various institutions by individuals in amounts less than what these institutions would normally be required to report to the authorities under AML/ATF legislation. After the cash has been deposited, the funds are then transferred to a central account. Smurfing is a money laundering technique involving the use of smurfs (i.e., multiple individuals) to conduct structuring activity at the same time or within a very short period of time.

ML Threat from Commercial (Trade) Fraud: Commercial trade fraud is unique in that it is a designated offence for money laundering and terrorist financing as well as a money laundering mechanism itself. The transnational OCGs and the terrorist actors and networks that use commercial fraud to launder are very sophisticated and capable, with the knowledge, expertise and international relationships to manipulate multiple trade chains, customs processes and financing mechanisms, often operating under the cover of front or legitimate companies. This is known as trade-based money laundering (TBML).

A high degree of sophistication and capability in terms of conducting the commercial fraud and laundering proceeds of crime continues to be observed. The threat actors in this space appear to use multiple sectors to launder proceeds both in Canada and internationally. Actors are suspected of using domestic and foreign front and shell companies, to commingle illicit funds within legitimate businesses (both cash and non-cash intensive businesses), and to use third-party money launderers, including professional money launderers. It has been observed that criminal organizations will manipulate customs and shipping documents and engage in fraudulent international trading activity with colluding foreign importer/exporters. The trade in misdescribed goods allows illicit finances to flow to the jurisdiction of choice in the form of payment for the goods in question with the importer/exporter paying inflated amounts to move illicit proceeds. Further, it has been observed that TBML schemes reveal a preference for goods which are either subject to spoilage (increasing the incentive by customs authorities to minimize examination of goods), difficult to physically examine, or where average and mean unit prices for goods can be difficult to establish as a result of variable values, making misdescription more difficult to detect. Recent law enforcement reports indicate an increased observance of use of customs fraud techniques for TBML to and from Canada, which may have been exacerbated in the context of the COVID-19 pandemic.

ML Threat from Corruption, Collusion and Bribery: Corruption and bribery in Canada comes in many different forms, ranging from small-scale bribe paying activity to obtain an advantage or benefit to large-scale schemes aimed at illegally obtaining lucrative public contracts. Public contracts can also be obtained illegally through collusive schemes that do not implicate the payment of a bribe. Although these schemes do not generate proceeds in the form of the payment of a bribe, they still generate illicit funds, e.g., through inflated procurement costs incurred. Direct control of legitimate business by OCGs or resorting to threats and intimidation to coerce other entrepreneurs are typically used to conduct these criminal activities.

The money laundering threat from corruption, collusion and bribery is rated very high principally due to the size of the public procurement sector and the opportunities this presents to illegally obtain high-value contracts. In addition to corrupt activities carried out domestically, some Canadian companies have also been implicated in paying of bribes to foreign officials to advance their company's business interests. OCGs with the ability to infiltrate the public procurement process and the legitimate economy have the sophistication and capability to launder large amounts of illicit funds, using a variety of money laundering methods and techniques, including banks, MSBs, high-end goods, investments and front companies. Cases have especially illustrated how networks and layers of shell companies have been used for the payment of bribes and corruption of foreign officials. Lawyers, accountants, professional money launderers and public officials may also be used to facilitate the laundering of corruption-related proceeds.

ML Threat from Illegal Gambling: This threat is being upgraded to Very High to reflect heightened law enforcement awareness of the known extent of the capabilities, scope and proceeds of crime associated with these activities. Illegal gambling in Canada continues to comprise private betting and gaming houses, unregulated video gaming and lottery machines, and unregulated online gambling.[28] Organized crime is the major provider of illegal gambling opportunities in Canada, although there are some smaller operators. The illegal gambling market appears to be small in terms of the numbers of threat actors involved, but it is suspected to be highly profitable for those involved. Traditional bookmaking betting activities use pyramid-style schemes to protect more senior members of the pyramid, with bookmakers accepting only cash to benefit from its anonymity.

[28] Private Member's Bill C-218 decriminalizing single event sports betting and allowing provinces and territories to conduct and manage single event sport betting received royal assent on June 29, 2021 (see: https://www.parl.ca/LegisInfo/en/bill/43-2/C-218).

OCGs also continue to run illegal gambling sites in jurisdictions where online gambling is legal or enforcement is lacking. OCGs operating in this space continue to have the sophistication and capability to launder proceeds of crime through a variety of sectors and methods. The main forms of illegal gambling proceeds are cash and possibly high value goods (in instances where gamblers may have run out of cash). Illegal gambling can further be a laundering technique in itself through the lending of proceeds of crime to gamblers. Law enforcement reports that closures of brick and mortar casinos due to the COVID-19 pandemic have led to an increase in underground illicit gaming and related money laundering activities.

According to the RCMP, illegal gambling is a key source of income for organized crime networks, with Criminal Intelligence Service Canada reporting that these proceeds are used to fund other criminal activity including drug trafficking and money laundering. OCGs may further be collaborating in sharing some overhead costs involved in the creation and upkeep of illegal online gambling websites, hosting onshore or offshore gambling servers as well as providing initial start-up capital.[29]

ML Threat from Illicit Drug Trafficking: Illicit drug trafficking remains the largest criminal market in Canada. Cannabis (post-legalization), cocaine, methamphetamines and heroin each comprise a significant share of this market, with fentanyl and its analogues rising in prominence. Although numerous threat actors engage in drug trafficking, transnational OCGs remain the most threatening and powerful actors, exhibiting very high levels of sophistication, capability and scope in their money laundering activities. They are often connected to other OCGs, and multiple organized networks at both the domestic and international levels to launder drug-related proceeds. OCGs continue to have access to professional money launderers, facilitators (such as money mules and nominees), and often have control over a number of companies (front and/or legitimate) as part of their money launderingoperations. OCGs use a large number of money laundering methods, including the use of multiple sectors, commingling of illicit funds within legitimate businesses, domestic and foreign front and shell companies, bulk cash smuggling, TBML, and prepaid cards. Despite the prevalence of cash transactions for laundering drug proceeds, the use of virtual currencies to procure drugs via the dark web is becoming more common. With border closures due to the COVID-19 pandemic, traditional cash-courier money laundering techniques have been disrupted.[30] It is not yet clear if OCGs will seek permanent alternative methods such as wire transfers or return to traditional techniques once borders reopen.

ML Threat from Mass Marketing Fraud (MMF): MMF remains prevalent in Canada and the scams associated with MMF have been growing in frequency and sophistication over time. Toronto, Montreal, Vancouver, Calgary and Edmonton continue to be considered the main bases of operation for MMF schemes. Common types of scams in Canada include extortion scams, phishing scams, service scams, and cyber scams. The CRA tax scam is an example of extortion scam. Fraudsters pretending to be the CRA have been calling consumers and telling them they owe money from a past tax return. The consumers are told they will incur additional fees, face jail time or be deported if they fail to pay the sum — by wire transfer, pre-paid credit cards, gift cards or bitcoin. The CRA scam alone has resulted in reported losses of more than $17.2 million in Canada between 2014 and 2019. Another rising trend is continuity scams, which involve a "free" trial or product offered online, where the victim must cover the cost of shipping via credit card and is subsequently charged hidden monthly fees. There has been an 859 per cent increase in continuity scams over the past two years. Another emerging trend is fraudsters impersonating banks or credit card providers to obtain financial information or money transfers abroad via MSBs.

[29] Criminal Intelligence Bulletin on Illegal Online Sportsbooks in Canada, March 2019.

[30] United Nations Office on Drugs and Crime - Money Laundering and COVID-19: Profit and Loss, April 2020.

While some Canada-based OCGs are involved, foreign actors, sometimes using Canadian associates for payment forwarding, are major threats in this activity. They use a range of money laundering methods and techniques, including smurfing, structuring, the use of nominees and money mules, shell companies, MSBs, informal banking system and front companies. Although reported losses have averaged at about $74 million annually from 2014 to 2017,[31] the actual losses are viewed as being much higher, in the hundreds of millions of dollars annually, given that MMF is generally under-reported by victims. The COVID-19 pandemic has led to an observed increase in online schemes and pandemic-related fraud, using prepaid cards and virtual currencies.

ML Threat from Mortgage Fraud: Mortgage fraud is suspected to have increased since the first publication of this report in 2015. It continues to occur across Canada, although it is most prevalent in large urban areas in Quebec, Ontario, Alberta and British Columbia, especially the Greater Vancouver and Toronto areas. Some forms of mortgage fraud are undertaken by persons misrepresenting their personal information such as their income in order to qualify for a loan they would not obtain otherwise. This is often referred to as fraud for housing as the borrower try to access property ownership and has no intent to default on the loan. However other types of mortgage fraud schemes are also undertaken by OCGs to facilitate another criminal activity (e.g., illicit drug production and distribution, money laundering) or directly for profit by defrauding a lender.

Rapid escalation of housing prices in certain areas of Canada in recent years have provided new lucrative opportunities for mortgage fraud (e.g., by making overvaluation schemes easier) which may have significantly increased the attractiveness of this type of fraud for OCGs. OCGs conducting mortgage fraud schemes are sophisticated in terms of the fraud and the associated money laundering activity. To orchestrate the fraud, they often seek the assistance of witting or unwitting professionals in the real estate sector, including agents, brokers, appraisers and lawyers. OCGs also frequently use straw buyers as nominees and misrepresent information to obfuscate the real identify of the borrower. As a result, discrepancies that could originally appear to a lender as fraud for housing may in fact involve more egregious criminal activities by OCGs which are in fact using a straw buyer to obfuscate the real party to the transaction. To launder mortgage-fraud related proceeds, professional money launderers can use criminally inclined real estate professionals, including real estate lawyers. OCGs involved in mortgage fraud also appear to launder funds through banks, MSBs, legitimate businesses and trust accounts. Victims of mortgage fraud, which can include Canadian homeowners and lending institutions, can incur significant financial losses.

ML Threat from Third-Party Launderers: Large-scale and sophisticated money laundering operations in Canada, notably those connected to transnational OCGs, frequently involve third-party money launderers, namely professional money launderers, nominees or money mules.[32] Of the three, professional money launderers pose the greatest threat both in terms of the level of funds and sophistication employed in laundering domestically generated proceeds of crime as well as laundering foreign-generated proceeds through Canada (and through its financial institutions). Professional money launderers specialize in laundering proceeds of crime and generally offer their services to criminals for a fee and are usually not associated with the underlying criminal activity. These individuals are in the business of laundering large sums of money and by their very nature have the sophistication and capability to support complex, sustainable and long-term money laundering operations. As a group, they use many different methods and techniques, often involving the use of multiple shell businesses, unregulated MSBs and nominees to conduct multiple layers of transactions to obfuscate the trail and impede the ability to link funds to its criminal origins. Professional money launderers are of principal concern since they are often the masterminds behind large-scale money laundering schemes and are frequently used by the most powerful transnational OCGs in Canada. Nominees and money mules are less of a threat, but are nonetheless important because they may be critical in carrying out or facilitating money laundering schemes, both large and small.

[31] Compiled from the annual statistical reports of the Canadian Anti-Fraud Centre.

[32] *Nominees* are individuals with familial or business ties to the threat actors who may be used periodically by criminals to knowingly assist in money laundering. Nominees are essentially directed by the criminals on how to launder the funds. The methods used tend to be fairly basic and can be used to launder smaller amounts of proceeds of crime. *Money mules* are those who facilitate fraud and money laundering schemes, often unknowingly (e.g., moving money through international electronic funds transfers on behalf of criminals). They are often located in different jurisdictions from where the crimes are committed and they tend to exhibit very low levels of sophistication and capability and are essentially directed to undertake certain actions to launder the funds.

High Money Laundering Threats

ML Threat from Counterfeiting and Piracy: This threat is being downgraded to High to reflect more recent intelligence on the relative known prevalence of these activities in the Canadian environment. A broad prevalence of counterfeit and pirated products in Canada has continued to persist. China is the primary source of counterfeit products imported into Canada, with Toronto, Montreal and Vancouver providing entry points. Foreign and potentially domestic OCGs appear to have established links and have tapped into illicit global distribution channels, allowing them to bring increasingly more counterfeit products into Canada. Available information indicates that involved actors are sophisticated and capable in terms of laundering the proceeds from counterfeit goods. These capabilities would continue to be fundamental to the sustainability of the operations given the large numbers of participants throughout the global supply chain.

ML Threat from Currency Counterfeiting: The large-scale production of Canadian counterfeit currency continues to be primarily undertaken by OCGs based in major cities in Canada, with a target on the new polymer series of bank notes. This is a proceeds-generating crime, but OCGs also launder the proceeds generated from currency counterfeiting. In 2019, the value of passed counterfeit notes was approximately $1.6 million, which has remained relatively consistent between 2015 and 2020. OCGs continue to conduct currency counterfeiting alongside other profit-oriented criminal activities. OCGs that produce and distribute high-quality counterfeit currency are suspected to exhibit a high level of sophistication and capability in terms of the methods used to launder the proceeds arising from currency counterfeiting. OCGs have the network and infrastructure in place to successfully launder, through a number of sectors, predominantly cash proceeds arising not only from currency counterfeiting but also from their other criminal activities.

ML Threat from Human Smuggling: Canada is a target for increasingly sophisticated global human smuggling networks. Human smuggling continues to be carried out primarily by a small number of OCGs that are well-established, having developed the sophistication and capability to smuggle humans for profit across multiple borders, which requires a high degree of organization, planning and international connections. OCGs in this space continue to be very sophisticated and capable in terms of laundering the proceeds of crime arising from human smuggling. A review of recent suspected money laundering cases largely related to human smuggling reinforced that OCGs may use a variety of sectors and methods to launder the proceeds, including front companies, legitimate businesses, banks, MSBs and casinos. Changes in technology, such as the use of cryptocurrencies, cheap labour demand, and the ease of money movement may be facilitating human smuggling services.

ML Threat from Human Trafficking: Canada continues to be a source, transit, and destination country for human trafficking. Police services in Canada have reported 1,708 incidents of human trafficking between 2009 and 2020. Between 2008/2009 and 2017/2018, there were 582 completed cases in adult criminal courts that involved at least one charge of human trafficking. Domestic human trafficking for sexual exploitation is the most common form of human trafficking in Canada.[33] Sex trafficking is largely perpetrated by criminally inclined individuals, who recruit and traffic domestically and, to a lesser extent, OCGs, some of which only recruit and traffic domestically, while others recruit and traffic domestically and internationally. Criminally inclined individuals are not believed to exhibit significant levels of sophistication or capability in terms of laundering their sex trafficking-related proceeds. It is suspected that most of their activity would center on laundering mostly cash proceeds for immediate personal use, leveraging a very limited or non-existent network, and using a limited number of sectors and methods. The OCGs that conduct sex trafficking and generate significant proceeds are suspected to use established money laundering infrastructure to launder the proceeds. Some OCGs, although less sophisticated in terms of money laundering, are nonetheless more capable because they may have access to venues to facilitate money laundering (e.g., strip clubs and massage parlors) as well as victims that can be used as nominees for deposits and wire transfers.

[33] Although less common, there have been cases of labour trafficking, notably in the construction sector and in housekeeping services. There have been no confirmed cases of organ trafficking in Canada.

ML Threat from Identity Theft and Fraud ("Identity Crime"): Identity crime continues to be prevalent in Canada and it is a concern given that stolen identities are often used to support the conduct of other criminal activities. In 2018, police services across Canada reported 19,584 incidents of identity theft and fraud, representing a 37 per cent increase over 2015. These can be conducted by individual criminals, foreign-based OCGs, and Canadian OCGs. The OCGs conducting identity crime are well-established, resilient and have well-developed domestic and international networks. They are also associated with drug trafficking, human smuggling and counterfeiting currency. It is suspected that these OCGs use multiple methods and sectors to launder the funds. Identity crime itself can support money laundering by providing individuals with fake credentials to subvert customer due diligence safeguards. In 2017, Canadians reported over $11 million in losses to identity crime.[34] Identity theft also facilitates the conduct of other criminal activities that generate significant proceeds of crime.

ML Threat from Payment Card Fraud: Between 2014-2019, reported losses from credit card fraud increased significantly while debit card fraud over the same period decreased (largely due to technology advancements). Payment card fraud continues to be a profitable market as reinforced by the fact that in 2013, Canadians reported close to $500 million annually in payment card fraud-related losses which, by 2016, had increased to $700 million annually.[35] "Card not present"[36] fraud comprises the largest value of all categories of credit card fraud in Canada, followed by credit card counterfeiting.[37] As with other frauds, OCGs, are heavily involved, with 24 domestic OCGs reported to be involved with payment card fraud in 2017 and possibly many more predominantly operating abroad. Organized crime involvement in payment card fraud can involve card thefts, fraudulent card applications, fake deposits, skimming or card-not-present fraud. In large part, the OCGs in this space are sophisticated and have specialized technological knowledge in committing payment card fraud. This is further reflected by high levels of sophistication and capability in laundering the proceeds generated. Multiple sectors are suspected to be used to launder payment card-related proceeds, including financial institutions, MSBs and casinos, as well as multiple methods, including structuring bank deposits, smurfing, front companies and the use of nominees and money mules.

ML Threat from Pollution Crime: Pollution crime in Canada continues to come in a variety of forms with some OCGs and companies being involved. Of the forms taken, there is particular concern that OCGs have infiltrated the waste management sector, as owning waste management companies can be an effective vehicle to generate illicit profits, by dumping waste illegally, and to launder proceeds from other criminal activities. OCGs may also be involved in the trafficking of electronic waste and in the importation of counterfeit products that do not meet Canada's environmental standards (e.g., counterfeit engines). Finally, some private and public companies may be using deceptive practices to undermine emissions schemes and may be dumping or using third parties to dump waste illegally. The OCGs continue to show a high degree of sophistication in the nature of their activities and operations, it is observed that there is a great degree of sophistication, capability and scope in terms of being able to launder the proceeds arising from pollution-related crime.

ML Threat from Robbery and Theft: Smaller scale thefts and robberies continue to be most frequently carried out by opportunistic individuals and petty thieves, while larger scale thefts and robberies are more frequently associated with OCGs, which are heavily involved in motor vehicle, heavy equipment, and cargo theft. There is a long-term downward trend of police-reported vehicle theft and robbery, but the rising proportion of uncovered vehicles suggests that vehicles are stolen by OCGs and then trafficked. The most sophisticated and capable actors continue to be the OCGs that have well-established auto theft networks in Canada, which are used to supply foreign markets with stolen Canadian vehicles. The OCGs that have established auto theft networks in Canada are also suspected to be highly sophisticated and capable from a money laundering perspective.

---

[34] Canadian Anti-Fraud Centre.

[35] Canadian Bankers Association. Credit Card Fraud and Interac Debit Card Statistics—Canadian Issued Cards.

[36] https://www.cfib-fcei.ca/en/tools-resources/card-not-present-fraud : Card not present fraud happens when a fraudster used a stolen credit card and the real cardholder later disputes the transaction.

[37] Card-not-present fraud: the unauthorized use of a credit (or debit) card number, the security code printed on the card (if required by the merchant), and the cardholder's address details to purchase products or services in a non-face-to-face setting (e.g., online, telephone). In many cases, the victims maintain possession of their card and are unaware of the unauthorized activity until notified by a merchant or they review their monthly statements.

As with the previous assessment, OCGs appear to use a range of trade-based fraud and related money laundering techniques to disguise the illicit origin of the automobiles as well as a range of methods to move the proceeds back into Canada, including bulk cash smuggling and EFTs. Front companies, shell companies and nominees may be used to obscure the flow of funds back to Canada arising from the illicit sales in other countries. Professional money launderers may be utilized to mastermind money laundering schemes given the large amounts of proceeds generated by these networks and the challenges of laundering proceeds that are generated across multiple jurisdictions.

ML Threat from Tax Evasion: Tax evasion is carried out in many different forms in Canada, with the ultimate objective of underpaying or evading the payment of taxes owing or to unlawfully claim refunds or credits. Although frequently carried out by opportunistic individuals using relatively unsophisticated techniques to misrepresent their tax situation, offshore tax evasion presents an increasingly complex, global and aggressive threat. Some tax preparers – including some accountants, lawyers and financial advisors – provide counsel on how to evade taxes or obtain fraudulent refunds using a variety of different techniques. Tax evasion is also conducted by professional criminals, including OCGs, who may orchestrate tax evasion schemes (e.g., duty or tax refund fraud). Money laundering techniques continue to reflect the sophistication of techniques involved in the tax evasion schemes themselves, while the globalization of financial transactions, increased prevalence of technology and greater access to facilitators increases their capability and sophistication. There is a trend towards using increasingly complex offshore corporate structures and accounts to shift profits to low-tax countries and move funds to accounts that are undeclared to tax authorities.

ML Threat from Tobacco Smuggling and Trafficking: The largest quantity of illicit tobacco found in Canada continues to originate from the manufacturing operations based on Indigenous reserves that straddle Quebec, Ontario, and New York State. In addition, proceeds of crime are generated from counterfeit cigarettes imported from overseas; cigarettes produced legally in Canada, the United States, or abroad, and sold tax-free; and "fine cut" tobacco imported illegally, mostly by Canadian-based manufacturers. Both OCGs and criminally inclined individuals continue to operate in the illicit tobacco trade, with the illicit market remaining profitable. Some of the OCGs involved in the illicit tobacco trade are highly sophisticated and capable in terms of money laundering, as a result of leveraging their expertise from involvement in other criminal activities, such as the narcotics trade. These OCGs use a variety of sectors and methods (e.g., commingling, structuring, smurfing and refining) to launder the large amount of cash proceeds that are generated from illicit tobacco smuggling and trafficking. Criminally inclined individuals likely possess much lower sophistication and capability in terms of money laundering. The threat rating of illicit tobacco smuggling and trafficking has been lowered from the previous report to better reflect the varying levels of money laundering sophistication and capability demonstrated by criminal actors in this space.

Medium Money Laundering Threats

ML Threat from Extortion: Police-reported incidents of extortion grew by 44 per cent between 2017 and 2018,[38] largely driven by a significant increase in cyber-related extortion[39] (e.g., ransomware). Cyber-related extortion is becoming the predominant proceeds-generating form of extortion and has affected Canadian businesses, hospitals and universities, primarily via ransomware attacks. Some OCGs continue to systematically use traditional methods of extortion in conjunction or in furtherance of other crimes. For example, using extortion as a tool to obtain money and property in exchange for the protection of certain businesses (i.e., extortion racketeering); to control the distribution of illicit drugs; to force the payment of illegal gambling debts; or to gain access to ports of entry.

[38] Statistics Canada table 35-10-0177-01.

[39] Data on cyber-extortion from Statistics Canada table 35-10-0001-01.

The criminal actors involved in extortion can range from individuals to OCGs, and as such they display varying levels of sophistication, capability and scope for laundering extortion-related proceeds. Structuring and smurfing, the commingling of illicit funds and casino refining activities may be used to launder proceeds of extortion, particularly proceeds in cash. Criminals engaged in cyber-related extortion often possess technological expertise to commit their crimes and conceal their identity and physical location. Cyber-related incidents of extortion predominantly generate proceeds of crime in the form of virtual currency, and these funds are laundered through the same vector (e.g., layering funds through multiple virtual transactions) to make use of online anonymity.

ML Threat from Firearms Smuggling and Trafficking: The illicit firearms market in Canada continues to be dominated by unsophisticated OCGs (primarily street gangs operating in metropolitan cities). Very few sophisticated OCGs are involved in the trafficking or smuggling of firearms for the purpose of achieving large profits. Instead, these activities are usually tied with other criminality such as illicit drugs. OCGs mainly use firearms to strengthen their position within other criminal markets, such as the illicit drugs market. While the majority of guns recovered in crime in Canada are believed to be domestically sourced, a majority of successfully traced handguns are smuggled into Canada from abroad, mostly from the United States. OCGs may sell illicit firearms to other OCGs and criminally inclined individuals, although it is unclear how important these OCGs are in terms of acting as a general supply hub for illicit firearms in Canada.

There is evidence to suggest that in some parts of the country there is a growing trend of licensed citizens that will purchase firearms and, in turn, sell them illegally given the markup on the firearms sold on the black market. It is, however, not seen as widespread. Overall, these OCGs may use their established money laundering infrastructure to launder the proceeds arising from their firearms trafficking activities, which would generally focus on exploiting a number of different sectors using a variety of methods. Unsophisticated or small traffickers will do this as a one-off activity where transactions are done either with cash, or facilitated through online platforms for cash or virtual currency.

ML Threat from Illegal Fishing: Illegal fishing generally 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. It can also entail or be associated with other illegal activities that are frequently transnational and organized in nature such as document fraud, drug trafficking, and money laundering.[40] Canadian coasts present the greatest vulnerability, but the illegally harvested goods are still known to move nationally. The coasts are prone to small- and medium-scale enterprises, as well as opportunistic and organized individuals who perpetrate fraud through the under-reporting and/or misreporting of legally and illegally caught fish. While the main actors are harvesters, buyers, shippers and processors attempting to bypass catch reporting and regulatory requirements, it is still believed that there is OCG involvement in this activity. There is a notable level of sophistication, scope and scale of these activities. However, OCG capacity is not seen to be as advanced as with other traditional forms of organized crime, such as the narcotics trade. Methods of profiting are: 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.

ML Threat from Loan Sharking: Loan sharks[41] appear to target wealthy gamblers who gamble with large amounts of money, low-income individuals, problem gamblers, illicit drug seekers and cash-strapped entrepreneurs. Loan sharking can be used by OCGs as a method to take over legitimate businesses facing financial difficulties. OCGs can then use them as a front to comingle proceeds of crime with legitimate incomes or to conduct other types of criminal activities.

[40] Crimes in the Fisheries Sector (unodc.org).

[41] For general information on the definition of loan sharking see: https://www.justice.gc.ca/eng/rp-pr/csj-sjc/crime/rr02_3/p34.html.

There have been notable examples suggesting that loan sharking has increased in the real estate financing market. This is partially due to the rapidly increasing house prices in some regions of Canada and resulting challenges for some borrowers to qualify for a loan with traditional lenders. Example situations can include lenders targeting newcomers or tourists who have purchased property in Canada, which they use as leverage to borrow cash for gambling or to pay down other debts. Many of these borrowers would have already reached their borrowing limit with Canadian financial institutions and, even when they possess wealth or financial assets in their countries of origin, may be unable to access or transfer the wealth due jurisdiction-specific obstacles, such as the existence of strict controls on capital that can leave the jurisdiction each year. Some borrowers may use capital gains when the property is sold to cover extremely high interest payments, a risky move that relies on the increasing cost of real estate. Alternatively, if the borrower flees Canada due to an inability to make loan repayments, the private lender can reap the benefits of these capital gains.

Conducting loan sharking activities requires working capital, financial aptitude and a capacity to enforce debt collection. Debt collection can include the remittance of both monies and/or property. As this is a unique skill set, loan sharking activity appears to be undertaken by a small number of the more sophisticated OCGs in Canada as well as by a small number of independent operators. It is also undertaken by some private lenders acting as professional money launderers. Some OCGs and independent operators conducting this criminal activity continue to exhibit a relatively high level of sophistication and capability in terms of being able to launder the proceeds emanating from illicit loans. However, other individual/small group loan shark activities may not be as sophisticated as the loan sharking activities of OCGs. Loan sharks continue to use a variety of money laundering methods to launder their proceeds, including through casinos, financial institutions, real estate and the construction sector.

ML Threat from Wildlife Crime: The threat level of this activity was increased from low to medium. There is an established illicit market for certain types of Canadian species, including narwhal tusks, polar bear hides, peregrine falcon eggs and wild ginseng. Black market prices for certain Canadian species are high and have risen significantly between 2015 and 2020.

As noted in the 2015 Report, wildlife crime in Canada appears to be generally conducted by opportunistic, criminally inclined individuals who exhibit low levels of sophistication. However, organized criminal networks appear to be increasingly involved, which include in some cases more sophisticated OCGs also in other illegal activities (e.g., drugs, cigarettes,). Similarly, updated analysis and monitoring found that the proceeds generated by this activity have increased between 2015 and 2020 and that wildlife that is being illegally trafficked is increasingly transported with legal flora and fauna products. Such co-mingling of legal and illicit goods is becoming increasingly common making identification and interception of illegally acquired goods more difficult. With the volume of such trade by sea and through the mail, coupled with the corruption in destination countries, criminals are able to use different methods of money laundering depending of the commodities.

A notable example had four individuals meeting the threshold of an organized crime group convicted of conspiring over many years to smuggle narwhal tusks from the Canadian Arctic across the New Brunswick-Maine border into the United States.[42] Payments made to a Canadian supplier were used to illegally import protected tusks for re-sale in the United States. Funds used to purchase the narwhal tusks were laundered by transporting, transmitting, or transferring cheques and money orders from the United States to Canada, intending that the money be used for further illegal imports of narwhal tusks. It is estimated that up to $2 million of narwhal tusks were sold throughout the conspiracy.

[42] For a description of this case, see the US Department of Justice new release entitled "Narwhal Tusk Trafficker Convicted of Conspiracy and Money Laundering." Accessible at: http://www.justice.gov/opa/pr/2014/February/14-enrd-165.html.

Chapter 4: Assessment of Terrorist Financing Threats

Overview

Terrorism remains a leading threat to Canada's national security.[43] Countering terrorism, including its financing, at home and abroad is a key priority for the Government of Canada.

This assessment of terrorist financing threats is based on threat groups identified by the United Nations Security Council as well as a careful review of intelligence and information from Canadian security and intelligence agencies. In no instances should it be used as basis or justification for discriminatory behavior or action toward specific communities in Canada or abroad. Measures taken by government or private sector entities to mitigate risks related to terrorist financing should be considered on a case-by-case basis and recognize that many Canadians have ties to communities around the world which they maintain, and that while there are risks, these relationships are not, in and of themselves, a vector for terrorist financing and money laundering.

Canada has listed 77 terrorist entities[44] under its *Criminal Code* and 36 terrorist entities under the *Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism*. Members or supporters/sympathizers of some of these listed entities may be Canadian citizens or have been present in Canada at one point or another. Their activities have often focused on providing financial or material support to terrorist entities based outside of Canada. Although their focus has been more on terrorist financing and less on conducting terrorist attacks in Canada, Canada is not immune to such attacks and, over the years, a few attacks have been carried out while others have been thwarted. Canadian interests[45] have also been affected by terrorism-related incidents that have occurred abroad. Recent attacks in Canada by ideologically motivated extremists have consisted of low-sophistication, high impact tactics that did not involve or require a known broader network of resources. These emerging risks are detailed separately below.

Not all 113 listed terrorist entities pose a terrorist financing threat to Canada since not all of these entities have financing or support networks in Canada. Consequently, an entity posing a terrorist threat to Canada does not necessarily pose a terrorist financing threat to Canada, or if so, the level of threat may not be the same. On the one hand, some terrorist groups and associated individuals pose a significant terrorist attack threat to Canada at home and abroad, while the terrorist financing threat in Canada is lower. On the other hand, some entities pose a very high or high terrorist financing threat but a lower terrorist attack threat to Canada.[46] Similarly, while Canadian entities need to remain aware of risks when operating abroad or remitting funds to certain geographic areas of the world, this does not necessarily mean that threat groups operating in those areas conduct terrorist financing activities in Canada.[47]

[43] Public Safety Canada. 2018 Public Report on the Terrorism Threat to Canada (publicsafety.gc.ca)

[44] As of June 2021.

[45] Throughout this report, Canadian interests refer to Canadian citizens and permanent residents that are in Canada or overseas, Canadian-owned physical assets in Canada or overseas, as well as Canada's economic and political interests.

[46] It should be noted, however, that this assessment only focused on terrorist financing threats and not terrorist attack threats.

[47] In its 2018 Terrorist Financing Assessment, FINTRAC provides for instance information on certain terrorist organizations and areas abroad where they operate, but only organizations that are known or suspected to be conducting terrorist financing in Canada are assessed as part of the National Inherent Risk Assessment.

A number of terrorist financing methods have been used in Canada and have involved both financial and material support for terrorism, including the payment of travel expenses and the procurement of goods.[48] The transfer of suspected terrorist funds to international locations has been conducted through a number of methods including the use of MSBs, banks and registered charities, as well as smuggling bulk cash across borders. In some cases, high-value goods such as electronics are directly brought over to jurisdictions of concern by individual travelers, who then sell these goods to finance terrorism abroad.

Based on public reporting by the Government of Canada (for example, FINTRAC's Terrorist Financing Assessment: 2018, and Public Safety Canada's 2018 Public Report on the Terrorism Threat to Canada), other international jurisdictions (for example, the U.S. Department of the Treasury 2022 National Terrorist Financing Risk Assessment), and intergovernmental organizations (such as the Financial Action Task Force's reporting), combined with protected information and analysis by Government of Canada officials on the potential for Canadians to send money or goods abroad to fund terrorism, the following countries were assessed to be the most likely locations where such funds or goods would be received: Afghanistan, Egypt, India, Lebanon, Jordan, Qatar, Pakistan, Palestinian Territories, Somalia, Syria, Turkey, United Arab Emirates, and Yemen.

Preliminary Assessment of Ideologically Motivated Violent Extremism (IMVE)

Ideologically motivated violent extremism (IMVE) is a subset of terrorism and is a particular ideology that can lead to terrorist activity. This is an emerging risk that the Government of Canada is seeking to address, and as such a separate discussion of IMVE financing can be found in this section. IMVE is often driven by a range of grievances and ideas from across the traditional ideological spectrum. This generally includes a narrative that describes who is part of the threatened group, who is part of the threatening group(s), the broader conditions that underpin the threat as well as the justification for the use of violence against the perceived threat. The resulting worldview consists of a personalized narrative which centres on an extremist's willingness to incite, enable and or mobilize violence. IMVE extremists can draw inspiration from a variety of sources including books, images, lectures, music, online discussions, videos, previous IMVE attacks, propaganda, conspiracy theories and conversations.

The Government of Canada distinguishes four different categories of IMVE: xenophobic violence, anti-authority violence, gender identity-driven violence and other grievance-driven violence.[49] CSIS resources have been shifting towards the threat of IMVE, to counter its rise. The Director of CSIS publicly stated 2022 that approximately 50% of the Service's counter terrorism resources are now dedicated to investigating IMVE.[50]

Ideologically motivated violent extremists often act without a clear affiliation to an organized group or external guidance, but are instead shaped by the echo-chamber of hate online that normalizes and advocates violence.[51] Traditional IMVE groups with more structured leadership and defined objectives have been largely—although not completely—supplanted by loosely networked, transnational movements with amorphous goals that co-exist across the IMVE milieu.

Recent attacks in Canada consisted of low-sophistication, high impact tactics that did not involve or require a broader network of resources. FINTRAC has observed a number of patterns in IMVE individuals, both those acting alone and as part of a larger group. The financial behavior of lone IMVE actors is similar to that of lone actors in other types of violent extremism. Lone actors primarily used personal funds, such as those received from employment income or family members, to carry out attacks. They commonly used electronic money transfers to both send and receive funds, made cash withdrawals, and carried out regular debit and credit activity to send funds.

[48] In the Canadian context, terrorist financing is often addressed as a broader "resourcing" issue, that is, terrorist resourcing has been used to describe all methods and means—from both licit and illicit origins—used by terrorist organizations to support their operations and infrastructure. While money or its equivalents are most often part of the process, these methods need not involve financial instruments or transactions at all, and could include the theft or smuggling of end-use goods, aggregations of donations, or the direct provision of equipment to terrorist cells, or even individuals using themselves as vehicles to conduct acts of violence, such as in the case of lone wolves or foreign fighters.

[49] CSIS Public Report 2019, April 2020.

[50] Special Joint Committee on the Declaration of Emergency evidence and Public Order Emergency Commission Public Hearing November 21, 2022.

[51] This was the case for many violent actions undertaken by violent extremists in Canada, such as the 2014 Moncton shooting, the 2017 Quebec Mosque Shooting and the 2018 Toronto van attack.

Further, many lone actors were observed to have sent money transfers to unknown third parties. Lone actors were also observed using their own funds to buy weapons, either through online chain stores or in person.[52]

While certain entities which contribute to propagating violent ideologies are known to have conducted some forms of fundraising, there have been no clear links that such funds were used to conduct violent actions in Canada. A certain number of groups which fall under the IMVE definition have been added to the list of terrorist entities in Canada.[53] This includes entities such as Atomwaffen Division, the Base and the Proud Boys. Information on these organizations can be found below, and as understanding of these organizations grow, more information will be added to Public Safety's list of "Currently listed entities".

Based on the analysis of IMVE-related transaction reporting, FINTRAC notes that organized IMVE groups in Canada use both personal and business accounts to conduct their financial activities. Personal and business account transactions showed connections between listed entities in Canada and companies charged with certain crimes. Using personal accounts, organized groups largely relied on electronic money transfers and cash deposits for their fundraising activities. These transfers typically involved small amounts. The majority of funds were suspected to be used to buy firearms and gear, as well as for donations and membership fees. FINTRAC observed several IMVE-related payments to personal accounts that indicated crowdfunding activity.[54]

Finally, FINTRAC assesses that individuals in Canada may fund international IMVE networks, while not necessarily being members of organized groups themselves. These individuals typically used payment processing companies and MSBs to make international funds transfers. While these transactions tended to be small, recurring transfers to multiple nodes of the same international network in different countries, they totaled significant amounts. Financial support to IMVE entities also took the form of one-time donations. Funds were typically sent to pay membership fees, purchase merchandise and gear, and to make general donations to IMVE groups internationally. Additionally, some of the beneficiaries forwarded the funds to recruiters for far-right militias and other similar groups.[55]

More information on IMVE and financing risks is available in FINTRAC's Special Bulletin on Ideologically Motivated Violent Extremism: A Terrorist Activity Financing Profile.

Looking forward in the context of the IMVE threat landscape, CSIS sees no short-or medium-term decline in IMVE activity across Canada. Not all extremists, however, are willing to engage in an act of serious violence. Some may strive to inspire or encourage (through a range of discourse including words and propaganda), or facilitate (such as providing financial support) others to engage in acts of serious violence. Other extremists may attempt to exploit public events (such as protests or demonstrations). CSIS notes that while past IMVE attackers are often self-funded, requiring relatively limited financial resources, their broader networks and online communities may profit from like-minded supporters and sympathizers.

Discussion of the Terrorist Financing Threat Assessment Results

After a thorough review of publicly available and classified information related to terrorist groups with links to Canada, the terrorist financing threat posed by actors associated with specific listed terrorist entities as well as foreign fighters were assessed (see Table 2 below). These profiles were considered either due to intelligence suggesting these groups received the largest amount of Canadian funding out of listed entities, or due to the emerging risks these entities pose, specifically, IMVEs.

[52] FINTRAC, July 2021, Special Bulletin on Ideologically Motivated Violent Extremism: A Terrorist Activity Financing Profile

[53] Public Safety Canada: Currently listed entities.

[54] FINTRAC, July 2021, Special Bulletin on Ideologically Motivated Violent Extremism: A Terrorist Activity Financing Profile.

[55] Ibid.

Table 2

Terrorist Financing Threat Groups of Actors[56]

Al Qaeda in the Arabian Peninsula	Extremist groups supporting violent means to establish an independent state within India
Al Qaeda Core	Foreign Fighters
Al Qaeda in the Islamic Maghreb	Hamas
Al Shabaab	Hayat Tahrir Al-Sham
Aryan Strike Force (ASF)	Hizballah
Atomwaffen Division	Islamic State in Iraq and the Levant (ISIL)
The Base	Russian Imperial Movement
Blood & Honour (B&H)	Three Percenters
Combat 18 (C18)	Proud Boys

For groups that were fully assessed, experts used the following six rating criteria to assess the terrorist financing threat posed by the actors associated with the groups and foreign fighters with links to Canada:

1. Sophistication: the extent of the threat actors' knowledge, expertise and overall sophistication to conduct sustainable, long-term and large-scale terrorist financing operations in Canada without being detected by authorities.
2. Capability: the extent of the threat actors' network, resources and overall capability to conduct terrorist financing operations in Canada.
3. Scope of terrorist financing: the extent to which the threat actors have a network of supporters and sympathizers within Canada and globally.
4. Estimated fundraising: the estimated value of their terrorist financing activities in Canada.
5. Diversification of methods: the diversity and complexity of terrorist financing methods related to the collection, aggregation, transfer and use of funds in Canada.
6. Suspected use of funds: the extent to which funds raised in Canada or overseas by terrorist actors are suspected to be used against Canadian interests in Canada or overseas.

Further information on some of these groups and their financing networks in Canada is provided below.

A preliminary assessment of financing linked to ideologically motivated violent extremist threat actors was also conducted. Given the preliminary nature of the evidence and information on the existence of financing activities in this area and the heterogeneity of the groups and individuals it encompasses, it was decided not to provide a formal assessment of the financing aspect of these threats actors at this time. This is however an emerging threat that experts will continue to monitor. The Government of Canada will continue to develop additional intelligence on these important emerging risks, and will seek to provide additional details on the methods used by extremists to fund their activities in future publications.

More information on terrorist financing and related areas of concern is available in FINTRAC's Terrorist Financing Assessment: 2018.

[56] Understanding of terrorist financing risks specifically linked to Listed Ideologically Motivated Violent Extremist (IMVE) terrorist entities is still developing. At this time, we are providing a summary of their activities..

Impacts of COVID-19

COVID-related fraud and online scams present new opportunities for terrorist organizations. A shift to digital platforms and financial products may also present new opportunities for terrorist organizations to generate and move funds.

Al Qaeda Core and Affiliated Groups

Al Qaeda's activities are not centralized and consist instead of a network of affiliates such as Al Qaeda in the Arabian Peninsula (AQAP) and Al Qaeda in the Islamic Maghreb (AQIM), which receive general directions from Al Qaeda Core (Afghanistan). Despite a certain decline in Al Qaeda Core's capability, it remains an important threat. Most of the global fundraising networks of Al Qaeda Core and affiliated groups operate in the Middle East and Africa. Methods of funding have included kidnapping for ransom, taxation of assets in geographic areas under their control, such as oil and gas, and the usage of charities to receive donations. Intelligence reports indicate that fundraising activity in Canada is limited and does not represent a consequent source of funding for Al Qaeda and affiliated groups due to simple and limited terrorist financing methods.

Al Shabaab is a Sunni militant Islamist group aiming to create an Islamist state in Somalia, to expel all foreign forces, overthrow the federal government of Somalia and to purge the country of any practices it considers un-Islamic. It is recognized by Al-Qaeda as its official branch in Somalia. Al Shabaab has a diversified global fundraising network, although most of its funds come from the area it controls. Despite some territorial losses in recent years, it has maintained relatively sophisticated and diversified funding capabilities and demonstrated considerable resilience. In East Africa and particularly in Somalia, Al Shabaab continues to generate income from the zones it controls, notably through the local taxation of businesses, transportation infrastructure and commodities as well as by the appropriation of livestock from the local population. Their fundraising techniques include international remittances channels, online solicitations and diverting funds from charitable campaigns.

Aryan Strike Force (ASF)

Aryan Strike Force, also known as ASF, was founded in the United Kingdom between 2006 and 2010. It is a neo-Nazi group that aims to carry out violent activities to overthrow governments, start a race war, and eradicate ethnic minorities.

The ASF describe themselves as a white nationalist organization with the goal to protect the honour of their women, children, and the future of their race and nation, using violence as a necessary tool to achieve its goals. ASF subscribes to the philosophy of decentralized leaderless resistance and has had chapters in the United Kingdom and the United States, and contacts in Eastern Europe, South America, South Africa, and Canada.

Members of the group have been convicted of crimes in the United Kingdom and the United States related to the production of chemical weapons, preparing and possessing material useful to commit acts of terrorism, facilitating the transfer of bomb-making instructions, and attempting to secure illegal firearms. The ASF had planned a suicide bombing attack on counter-protestors during a November 2016 white supremacist rally in Pennsylvania.

The group is associated with Combat 18, the armed branch of Blood & Honour. Both are listed entities in Canada that have carried out violent actions including murders and bombings. The ASF was listed as a terrorist entity on June 25, 2021.

For a discussion on the financing risks and methodologies of ASF and other listed IMVE terrorist organizations, please see the *Preliminary Assessment of Ideologically Motivated Violent Extremism (IMVE)* above.

Atomwaffen Division

Atomwaffen Division, also known as AWD, National Socialist Order, or as NSO, was founded in the United States in 2013. AWD is an international neo-Nazi terror group, which has since expanded to the United Kingdom, Canada,

Germany, and elsewhere. The group calls for acts of violence against racial, religious, and ethnic groups, and informants, police, and bureaucrats, to prompt the collapse of society.

AWD has held training camps, also known as hate camps, where its members receive weapons and hand-to-hand combat training. AWD members have carried out violent acts at public rallies, including the August 2017 Unite the Right rally and associated protests of the rally in Charlottesville, Virginia.

In July 2019, the co-leader of AWD, an American citizen, was banned from Canada by the Immigration and Refugee Board after it was determined that he was a member of an organization that has or will engage in terrorist activities. The AWD was listed as a terrorist entity on February 3, 2021.

For a discussion on the financing risks and methodologies of AWD and other listed IMVE terrorist organizations, please see the *Preliminary Assessment of Ideologically Motivated Violent Extremism (IMVE)* above.

The Base

The Base is a neo-Nazi organization founded in 2018. The group was primarily active in the United States and promotes a nihilistic and accelerationist rhetoric— an ideology embraced by white supremacists who have determined that a societal collapse is both imminent and necessary. The group advocates for direct action, especially in the form of violence, to create chaos, incite a race war, and establish a white ethno-state. The Base has distributed manuals for lone-wolf terror attacks, bomb making, counter-surveillance, and guerilla warfare to its members.

Members of the group plotted to carry out attacks at a January 2020 rally in Virginia, United States. The group also organized training camps in weaponry and military tactics around North America. The network specifically seeks to recruit individuals with military experience so that they can leverage their training. The Base was listed as a terrorist entity on February 3, 2021.

For a discussion on the financing risks and methodologies of The Base and other listed IMVE terrorist organizations, please see the *Preliminary Assessment of Ideologically Motivated Violent Extremism (IMVE)* above.

Blood & Honour (B&H) and Combat 18 (C18)

Blood & Honour (B&H) is an international neo-Nazi network whose ideology is derived from the National Socialist doctrine of Nazi Germany. B&H was founded in the United Kingdom in 1987 and grew during the 1990s, establishing branches throughout Europe by the end of the decade. B&H attacks have occurred in North America and in several European Union member states. Combat 18 (C18) is the armed branch of B&H. Combat 18 has carried out violent actions, including murders and bombings.

In January 2012, four B&H members in Tampa, Florida, were convicted of the 1998 murder of two homeless men who were killed because the group considered them "inferior." In February 2012, members of B&H and C18 firebombed a building occupied mostly by Romani families, including children, in Aš, Czech Republic.

B&H and C18 were listed as terrorist entities on June 21, 2019.

For a discussion on the financing risks and methodologies of the B&H, C18 and other listed IMVE terrorist organizations, please see the *Preliminary Assessment of Ideologically Motivated Violent Extremism (IMVE)* above.

Islamic State in Iraq and the Levant (ISIL)

The Islamic State in Iraq and the Levant (ISIL), or Daesh, is a predominantly Sunni jihadist group that seeks to establish a single transnational Islamic state. Although it was initially known as Al-Qaeda in Iraq, ties with the organization were severed by Al-Qaeda leadership in 2014. Since then, ISIL's financing developments have been in a state of constant change. Recent years were marked by a decline in the territories controlled by ISIL[57] and in its general revenue sources, but the group still remains an important terrorist financing threat. It is still in a position, for instance, to seek sympathy from individuals abroad who may attempt to provide funds or conduct lone-actor attacks. Nonetheless, the group financing capability in Canada remains low and has usually concentrated on providing financial support to extremist travelers (see below).

Foreign Fighters/Extremist Travelers

More attention has been given in recent years by Canada and other countries to individuals referred to as "foreign fighters" or "extremist travelers" ("Canadian extremist travelers" or CETs hereafter) who have travelled to other countries to participate in terrorism-related activities. Being somewhat of a new trend observed in relation to various terrorist organizations (e.g., ISIL, Al Shabaab), this was singled-out in 2015 as an area worth assessing on its own. As of early 2014, the Government of Canada was aware of more than 130 individuals with Canadian connections who were abroad and who were suspected of terrorism-related activities, which included involvement in training, fundraising, promoting radical views and planning terrorist violence. More recent estimates show that CET numbers abroad remained stable, with approximately 190 individuals having a nexus to Canada, and close to 60 who have returned.[58] Between 2015 and 2020, the number of individuals travelling abroad from Canada has however greatly declined.

Despite events such as the weakening of ISIL, Canada has not seen significant related influx in the number of CETs returning to the country, nor does it expect to. There are a variety of factors why CETs may not return, such as the lack of valid travel documents, potential fear of arrest upon return, continued commitment to their organization, having been captured, or because they have died.[59]Foreign fighters who had returned to Canada may encourage and recruit aspiring violent extremists in Canada, may engage in fundraising activities, or may even plan and carry out terrorist attacks in Canada. There are also indications that CETs detained abroad may seek to receive funds in order to finance their release from detention.

Hamas

Hamas, or Harakat al-Muqawama al-Islamiyya (Islamic Resistance Movement), is a militant Sunni Islamist organization that emerged from the Palestinian branch of the Muslim Brotherhood in late 1987. Hamas operates predominantly in the Gaza and the West Bank and manages a broad, mostly Gaza-based network of "Dawa" or ministry activities that includes charities, schools, clinics, youth camps, fundraising and political activities.

No significant changes have been observed regarding this group between 2015 and 2020. Globally, Hamas remains a complex and highly organized group that is well-funded, utilizing a number of financing strategies, albeit with a global network of support which is largely based outside of Canada. There are small funding networks for Hamas across Canada, but they appear less organized than in the past. They may seek to leverage or provide funds to foreign charitable organizations with direct or indirect ties to the Hamas.

[57] This is not true for certain of its affiliates, which have instead increased the territories under their control, e.g., in Africa.

[58] CSIS Public Report 2019 - Canada.ca.

[59] Public Safety Canada. 2018 Public Report on the Terrorism Threat to Canada (publicsafety.gc.ca)

Hizballah

Hizballah, a populist Lebanon-based terrorist organization seeking to represent the Shi'a people and Shi'a Islamism, is highly disciplined and sophisticated, with extensive paramilitary, terrorist and criminal fundraising capabilities, while simultaneously receiving significant logistical, military and financial support from Iran. It has a global network of support that spans the Americas, Europe, the Middle-East and Africa. Hizballah has an established fundraising network in Canada. The group's fundraising methods in Canada and abroad are well diversified. In addition to funding received from the Iranian state, funds can be provided by a network of charities or non-profit organizations sympathetic to its cause.[60]

Extremist groups supporting violent means to establish an independent state within India

Extremist groups supporting violent means to establish an independent state within India are still suspected of raising funds in a number of countries, including Canada. In Canada, two organizations, Babbar Khalsa International and the International Sikh Youth Federation, have been identified as being associated with terrorism and remain listed terrorist entities under the Criminal Code. There appears to be a global network but it is unclear how strong it is and the motivations surrounding the support. These groups used to have an extensive fundraising network in Canada, but it now appears to be diminished and consisting of smaller pockets of individuals.

Russian Imperial Movement

The Russian Imperial Movement, also known as RIM, Russkoie Imperskoe Dvizhenie, Russkoe Imperskoye Dvizheniye, RID, Imperial Legion, Russian Imperial Legion, RIL, and Saint Petersburg Imperial Legion, is a nationalist group based in Russia that seeks to create a mono-ethnic state led by a Russian autocratic monarchy.

The group is best known for having members and sympathizers linked to violent activity abroad and seeks to build ties to neo-Nazi organizations in Europe and the United States to offer them paramilitary training and bomb making instructions.

In 2015, RIM co-founded the World National Conservative Movement (WNCM), a transnational movement ideologically aligned against the Western principles of 'liberalism, multiculturalism and tolerance' according to its own manifesto. RIM leaders intended the WNCM to facilitate the sharing of tactical skills across peer organizations and promote their own paramilitary training program. Furthermore, RIM has donated money to foreign neo-Nazi and white supremacist groups associated with the WNCM and provided training to members who have carried out bomb plots in their own countries.

In 2016, RIM provided training to two Swedes who then bombed a bookstore-café, a refugee shelter, and a campground that housed asylum seekers. RIM's paramilitary faction has also been present in conflicts in Ukraine, Syria, and Libya. RIM was listed as a terrorist entity on February 3, 2021.

For a discussion on the financing risks and methodologies of RIM and other listed IMVE terrorist organizations, please see the Preliminary Assessment of Ideologically Motivated Violent Extremism (IMVE) above.

[60] FINTRAC Terrorist Financing Assessment: 2018.

Three Percenters

The Three Percenters, also known as 3%ers, III%ers, Threepers, are a decentralized entity within the broader anti-government militia movement in the United States.

The name "Three Percenters" is a reference to a false belief that the number of Americans who fought against the British during the Revolutionary War amounted to only three per cent of the population at the time. The entity has a presence in the United States and Canada.

Three Percenters have been linked to bomb plots targeting United States federal government buildings and Muslim communities. In November 2015, a Three Percenter was arrested and eventually convicted of shooting and wounding five men at a Black Lives Matter demonstration in Minneapolis, Minnesota.

In 2020, two of the group's leaders directed a failed plot to kidnap the Governor of Michigan that involved acquiring and detonating explosives to divert police attention from the kidnapping, as well as public executions of public officials by hanging them on live television. The Three Percenters was listed as a terrorist entity on June 25, 2021.

For a discussion on the financing risks and methodologies of the Three Percenters and other listed IMVE terrorist organizations, please see the Preliminary Assessment of Ideologically Motivated Violent Extremism (IMVE) above.

Proud Boys

The Proud Boys is a neo-fascist organization that engages in political violence and was formed in 2016. Members of the group espouse misogynistic, Islamophobic, anti-Semitic, anti-immigrant, and/or white supremacist ideologies and associate with white supremacist groups.

The Proud Boys consists of semi-autonomous chapters located in the United States, Canada, and internationally. The group and its members have openly encouraged, planned, and conducted violent activities against those they perceive to be opposed to their ideology and political beliefs. The group regularly attends Black Lives Matter (BLM) protests as counter-protesters, often engaging in violence targeting BLM supporters.

On January 6, 2021, the Proud Boys played a pivotal role in the attack on the U.S. Capitol. Leaders of the group planned their participation by setting out objectives, issuing instructions, and directing members during the attack. The leader of the Proud Boys was arrested two days before the attack as part of a stated effort by U.S. law enforcement to apprehend individuals who were planning to travel to the D.C. area with intentions to cause violence. The Proud Boys was listed as a terrorist entity on February 3, 2021.

For a discussion on the financing risks and methodologies of the Proud Boys and other listed IMVE terrorist organizations, please see the Preliminary Assessment of Ideologically Motivated Violent Extremism (IMVE) above.

Chapter 5: Assessment of Inherent Money Laundering and Terrorist Financing Vulnerabilities

Overview

Geopolitical, socio-economic, governance and legal framework features of a country are important components of a nation's identity and position in the world. Internationally, Canada is recognized as a multicultural and multiethnic country with a stable economy and strong democratic institutions. Although these features of Canada are positive, some can be subject to criminal exploitation. Criminals, including money launderers and terrorist financiers, can be attracted to Canada as a result of inherent vulnerabilities associated with Canada's geography, demographics, stable open economy, accessible financial system, proximity to the United States and well-developed international trading system. It is important to underscore that this updated assessment, as was the case in 2015, still examines the inherent vulnerabilities of various economic sectors and financial products and does not account for the significant mitigation measures that are in place to address these risks.

While being mindful of the contextual vulnerabilities of Canada, experts assessed the inherent money laundering and terrorist financing vulnerabilities of 33 economic sectors and financial products, using the following five rating criteria:

1. Inherent Characteristics: the extent of the sector's economic significance, complexity of operating structure, integration with other sectors and scope and accessibility of operations.
2. Nature of Products and Services: the nature and extent of the vulnerable products and services and the volume, velocity and frequency of client transactions associated with these products and services.
3. Nature of the Business Relationships: the extent of transactional versus ongoing business, direct versus indirect business relationships and exposure to high-risk clients and businesses.
4. Geographic Reach: the exposure to high-risk jurisdictions and locations of concern.
5. Nature of the Delivery Channels: the extent to which the delivery of products and services can be conducted with anonymity (face-to-face, non-face-to-face, use of third parties) and complexity (e.g., multiple intermediaries with few immediate controls).

The assessment indicates that there are a significant number of economic sectors and financial products that are inherently vulnerable to money laundering and terrorist financing. Of the 33 rated areas, the overall money laundering and terrorist financing vulnerability was rated "very high" for five sectors and products, "high" for 18 sectors and products, "medium" for nine sectors and products and "low" for one sector (see Table 3). Inherent vulnerabilities and risks are, however, the subject of mitigation and control measures provided by the AML/ATF Regime, including through preventive measures and effective supervision.

Although the vulnerabilities assessment examined sectors and products individually, it is important to note that the six designated domestic systemically important banks (D-SIBs) are financial conglomerates that dominate Canada's financial sector, and are deeply involved in multiple business lines, including banking, insurance, securities and trust services. The inherent vulnerability of the D-SIBs was explicitly assessed as part of the category of domestic banks and rated very high, while their presence in other sectors was included in the assessment of those sectors. Given their size, scope and reach, and if assessed on a consolidated basis, the inherent vulnerability of the D-SIBS would naturally be very high.

Beneficial ownership, trade fraud, and trade-based money laundering (TBML) remain priority areas for the Government of Canada as it continues to strengthen AML/ATF measures to ensure Canada's Regime remains responsive and effective in appropriately addressing risks. As such, corporations, partnerships, company service providers, express trusts, lawyers,[61] non-profit organizations, and entities related to the trade and import/export sectors, although not subject to reporting obligations under the PCMLTFA, were formally included as part of this assessment since it was determined to be necessary to assess their money laundering and terrorist financing vulnerabilities given their importance and widespread use within Canada. Other sectors and products that are not currently covered under the PCMLTFA will continue to be assessed for money laundering and terrorist financing risks. These include, but are not limited to, payment processors, cheque cashing businesses, crowdfunding, closed-loop pre-paid access,[62] factoring companies,[63] financing and leasing companies, home renovators, and high-value goods dealers.

Table 3

Overall Inherent Money Laundering/Terrorist Financing Vulnerability Rating Results[64]

Very High Vulnerability Rating	
Alternative Remittance MSBs	Express Trusts*
Corporations*	Retail Multi-Services MSBs
Domestic Banks	
High Vulnerability Rating	
Armoured Car Companies	Life Insurance Companies
Brick and Mortar Casinos	Partnerships*
White Label ATM Providers	Real Estate Agents and Developers
Credit Unions and Caisses Populaires	Retail-Single Service MSBs
Dealers in Precious Stones and Metals	Securities Dealers
Foreign Bank Branches	Trust and Loan Companies
Foreign Bank Subsidiaries	Unregulated Mortgage Lenders
Import/Export Companies	Virtual Currencies
Legal Professionals	Registered Charities / Non-Profit Organizations
Medium Vulnerability Rating	
Accountants	Company Services Providers
British Columbia Notaries	Open-Loop Prepaid Cards
Freight Forwarders	Custom Brokerage
Provincial Online Casinos	Wholesale and Corporate MSBs
Independent Life Insurance Agents and Brokers	
Low Vulnerability Rating	
Life Insurance Intermediary Entities and Agencies **	

* 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.
** These entities provide administrative support to insurance agents and brokers and allow for the pooling of commissions and access to insurance company products.

[61] The provisions of the PCMLTFA that apply to the legal profession are inoperative as a result of court decisions and related injunctions. The Government of Canada continues to assess options to work with the legal profession to better include them in Canada's AML/ATF Regime.

[62] Closed-loop pre-paid access is defined as prepaid access to funds or the value of funds that can be used only for goods and services in transactions involved a defined merchant or location (or set of locations). The definition includes gift cards that provide access to a specific retailer, affiliated retailers, or retail chain, or alternatively, a designated locale, such as a public transit system.

[63] Factoring is a form of asset-based financing whereby credit is extended to a borrowing company on the value of their accounts receivable (the latter are sold at a discount price in exchange for money upfront). The factoring company then receives amounts owing directly from customers of the borrower (the debtor). Factoring companies are primarily used to raise capital in the short-term.

[64] This does not include Payment Service Providers and Crowdfunding Platforms, which were added in April 2022.

Inherent Vulnerabilities of Canada

This section provides an overview of the features of Canada that may be vulnerable to being exploited by criminals.

Governance/Legal Framework

Canada is a federal state governed by a Constitution and has a democratic system that provides substantial autonomy to its 13 provinces and territories. The federal government has legislative jurisdiction over criminal law and procedure, while the provinces are responsible for the administration of the courts of criminal jurisdiction including federal courts constituted under section 96 of the Constitution. Canada is also governed by the common law, or rule of precedent, and by a civil law system in the province of Quebec.

Canada is a free and open democratic society, and its citizens are guaranteed certain rights and freedoms under Canadian law. To protect these freedoms, Canada has strong public institutions and a comprehensive system of justice. Although these laws and institutions play a key role in combating crime, the freedoms afforded to Canadians and the legal and procedural safeguards that are in place to protect accused individuals can be exploited by criminals, including money launderers and terrorist financiers.

Geography

Canada is the second-largest country[65] in the world with a land area of 9.9 million square kilometres. Canada has a total of over 200,000 km of coastlines spanning the Pacific Ocean to the west, the Arctic Ocean to the north, and the Atlantic Ocean to the east. Canada shares the longest international border in the world, at over 8,800 km, with the United States to the south and northwest (Alaska). This makes Canada vulnerable to criminal activities conducted across Canada, as well as by land, air or marine modes of transportation through its borders. Detection of criminal activities may be challenging in light of the geographic expanse of Canada.

Economy & Financial System

Canada was the 16th largest economy in the world at the end of 2019 (based upon a ranking of nominal gross domestic product (GDP) with a value of 1,921 billion current international dollars).[66] In the same year, 70 per cent of the economy was devoted to services, while manufacturing and primary sectors accounted for the remaining 30 per cent.[67] All of the relevant economic indicators and discussion below are as of the date of the original writing of this report.

International trade represents more than 65 per cent of Canada's GDP.[68] Canada's economy is closely linked to that of the United States. In 2019, over 75 per cent of Canada's exports went to and through the United States, and over 51 per cent of Canada's imports came from the United States.[69] The three other main export destinations for Canada are the European Union (EU), China, and Japan.[70] The EU, China, and Mexico are the three other main sources of Canadian imports behind the United States.[71]

[65] Financial Action Task Force (FATF) - *Mutual Evaluation Report of Canada* (2016); Central Intelligence Agency - *World Fact Book.* Website content on Canada.

[66] On a purchasing power parity basis (PPP). Source: International Monetary Fund (IMF) October 2020 World Economic Outlook (WEO).

[67] Statistics Canada. Gross Domestic Product at Basic Prices, by Industry. CANSIM: Table 379-0031.

[68] Global Affairs Canada. Canada's State of Trade 2020. July 2020.

[69] Statistics Canada. Canadian International Merchandise Trade Database (CMIT) and Balance of International Payments, Services by Principal Trading Partners (Table: 36-10-0024-01).

[70] Ibid.

[71] Ibid.

Statistics Canada estimates underground economic activity for 2018 (i.e., market-based economic activity that escapes measurement due to its hidden, illegal, or informal nature) totaled $61.2 billion in Canada or about 2.7 per cent of GDP.[72] From 2014 to 2018, the underground share of GDP varied between 2.7 per cent and 2.9 per cent.[73] In a study published in June 2017, the tax gap associated with the underground economic activities on individual income tax estimated the CRA revenue shortfall at about $6.5 billion for 2014. This represents about 4.8 per cent of personal income tax revenues and 0.3 per cent of GDP.[74] However, a 2014 Organization for Economic Co-operation and Development (OECD study provides an international perspective on relative adjustments for the non-observed economy (NOE) across countries, and suggests that Canada has one of the smaller NOE adjustments, below a number of European Union economies.[75]

Canada's financial system is mature, sophisticated, well diversified and plays a key role in the Canadian economy. It is one of the largest and most developed financial systems in the world. As of year end-2018, total assets of financial institutions reached US$10.2 trillion or 626 per cent of GDP.[76]

Canada's banks and other financial institutions operate an extensive network of more than 5,890 branches, and 18,640 bank-owned automated teller machines (ATMs).[77] In 2017, approximately 655 million transactions were logged at bank-owned ATMs, down from 842 million transactions in 2012.[78]

Digital banking is still the main means of conducting banking transactions, where 76 per cent of Canadians do most of their banking using online and mobile banking.[79] Banks also operate through agents or mandataries, mostly in remote areas. Canada also enjoys a high rate of financial inclusion with 99.7 per cent of the population over the age of 15 years old having an account with a formal financial institution and 98 per cent having made or received digital payments in the past year.[80] It is still too early to determine how the pandemic may alter the domestic financial sector in the long run, however the increased adoption of digital financial services has been observed and may lead to a permanent behavioral shift towards digital finance, alternative financial technologies, and non-face-to-face interactions.

While the banking sector in Canada is diverse and includes many service providers, it is relatively highly concentrated and holds over 41 per cent of financial institutions' assets.[81] The banking sector is dominated by six domestic banks that, in the aggregate, hold 97 per cent of bank assets.[82] These six banks are the parents of large conglomerate financial groups and have been designated as D-SIBs by OSFI, Canada's prudential supervisor. The six largest banks and Québec's major credit cooperative group – designated as domestic systemically important financial institution by the province – account for about 90 per cent of deposit-taking sector assets, while the three largest life insurers account for about 70 per cent of total net premiums. These financial institutions play a large role in Canada's financial system.[83]

There are more than 24,000 reporting entities (e.g., banks, casinos, MSBs, securities dealers, real estate agents and developers) that are subject to the PCMLTFA, offering products and services that involve financial transactions that can be vulnerable to illicit activity.[84] Table 4 provides an appreciation of the relative size of the various assessed sectors and products.[85]

---

[72] Statistics Canada. The Daily. Released 2020-10-23. https://www150.statcan.gc.ca/n1/daily-quotidien/201023/dq201023a-eng.htm.

[73] Ibid.

[74] Canada Revenue Agency. *Underground Economy Strategy 2018-2021*. August 2019.

[75] György Gyomai and Peter van de Ven. "The Non-Observed Economy in the System of National Accounts." OECD Statistics Brief. Organisation for Economic Co-operation and Development. June 2014.

[76] International Monetary Fund. Canada: Financial Sector Stability Assessment. IMF Country Report No.19/177. June 2019.

[77] Canada Bankers Association. "Focus: Fast Facts About the Canadian Banking System." Toronto: November 2020.

[78] Ibid.

[79] Ibid.

[80] World Bank. G20 Financial Inclusion Indicators (Canada). 2020. Global Findex database, 2017.

[81] International Monetary Fund. Canada: Financial Sector Stability Assessment. IMF Country Report No.19/177. June 2019.

[82] Ibid.

[83] Ibid.

[84] See the previous section for a detailed money laundering and terrorist financing vulnerability assessment by sector and product.

[85] Chapter 6 provides additional information on the measures currently in place to mitigate risks.

Canada's open and stable economy, a financial system accessible to the majority of Canadians and the high level of global trade involving Canada, are factors that can be exploited by criminals, money launderers and terrorist financiers that are active domestically and internationally. They use a number of methods and schemes to hide their illicit financial transactions to make them look legitimate so they can avoid detection by authorities.

Table 4

Statistics on Assessed Sectors and Products

Sector or Product	Number of Known Entities	Notes
Domestic Systemically Important Banks	6	Banks hold over 41 per cent of the financial institutions' assets; the six largest domestic banks, the D-SIBs, hold 97 per cent of these assets.[86]
Other Domestic Banks[87]	29	
Foreign Bank Subsidiaries[88]	17	
Foreign Bank Branches[89]	32 (28 full service and 4 lending)	
Life Insurance Companies	61 federal and 17 provincially-regulated[90]	Excluding segregated funds, the life and health insurance sector held $565 billion in assets, of which $472 billion was held by federally regulated insurers (end 2019). Three companies held 65 per cent of life insurers' total general fund assets.[91]
Independent Life Insurance Agents and Brokers	99,000 agents[92] [93]	
Trust and Loan Companies	58 federally-regulated trust companies and loan companies and 17 provincially-regulated[94]	Trust and loan companies hold over $451 billion in assets (as of January 31, 2021). The six largest Canadian banks own 95 per cent of these trust and loan companies.[95]
Securities Dealers	1,409[96]	As at the end of 2020, the Canadian securities industry holds approximately $3.4 trillion in client assets (retail and institutional combined).[97] Each D-SIBs operates a full-service and online securities dealer, who collectively account for approximately 75 per cent of the sector's total assets. This sector also includes financial advisors and investment counsellors

[86] International Monetary Fund. Canada: Financial Sector Stability Assessment. IMF Country Report No.19/177. June 2019.

[87] Office of the Superintendent of Financial Institutions (OSFI). Who We Regulate. December 2020.

[88] Ibid.

[89] Ibid.

[90] Canadian Life and Health Insurance Association, CLHIA-ACCAP - Canadian Life and Health Insurance Facts - 2020 (uberflip.com).

[91] Ibid.

[92] Ibid. More than one agent often work within one brokerage.

[93] Of all life insurance entities (i.e., companies and independent brokerages/agents) across Canada, 3,775 of them were also reporting entities under the PCMLTFA, as of April 2021 according to FINTRAC.

[94] International Monetary Fund. Canada: Financial Sector Assessment Program-Technical Note-Insurance Sector: Regulation and Supervision. January 24, 2020; Consultation with OSFI (Dec 2020).

[95] Office of the Superintendent of Financial Institutions Consolidated Monthly Balance Sheet Jan 31,2021: Trust Companies; Financial Data for Trust Companies (osfi-bsif.gc.ca); Office of the Superintendent of Financial Institutions Consolidated Monthly Balance Sheet Jan 31,2021: Loan Companies; Financial Data for Loan Companies (osfi-bsif.gc.ca).

[96] As of November 2020 and provided by FINTRAC.

[97] Provided by the Investment Industry Regulatory Organization of Canada (IIROC).

Sector or Product	Number of Known Entities	Notes
Credit Unions and Caisses Populaires (CUCPs)	233[98]	Credit unions across Canada (excluding Quebec) reported sector assets of $265 billion (November 2020). Groupe Desjardins holds $313 billion in assets (December 2019)[99]
Money Services Businesses	1,858 registered MSBs[100]	MSB sector handles hundreds of billions of dollars in transactions each year. It is estimated that MSBs registered with FINTRAC handle approximately $616 billion a year.
Provincially-Regulated Casinos[101]	17 reporting entities[102]	Canadian casino sector generates over $15 billion in revenue annually.
Real Estate Agents & Developers	80 970 brokerages/businesses[103]. More than 135,000 brokers, agents and salespeople, including 6500 commercial real estate specialists [104]	
Dealers in Precious Metals & Stones	4,151[105]	
British Columbia Notaries	over 190[106]	
Accountants	5,256[107]	
Armoured Car Companies	20-30	
Legal Professionals	Over 130,000 lawyers, 37,000 paralegals, and 3,800 civil-law notaries[108]	
Express Trusts[109]	Estimated millions (over 450,000 trusts registered with CRA)[110]	

[98] Canadian Credit Union Association. System Results. November 2020.

[99] Desjardins – About Us – Quick Facts, December 2020.

[100] As of November 2020 and provided by FINTRAC. It should be noted that the total number of registered MSBs does not include the number of MSB agents. In the Canadian framework, MSB agents are often covered through the MSB which engages/contracts with the agents (depending on the other activities of the MSB agent).

[101] Casinos or gambling activities that are not provincially regulated have not been included in these statistics and the vulnerability assessment of the casino sector. Gambling operations and activities not regulated by a province or territory are illegal under Canada's Criminal Code and are therefore generating criminal proceeds and have been taken into account during the assessment of money laundering threats, in particular under "illegal gambling".

[102] As of November 2020 and provided by FINTRAC.

[103] IbisWorld, CA INDUSTRY (NAICS) REPORT 53121CA, Real Estate Sales & Brokerage in Canada. Home sweet home: An increase in disposable income is expected to bolster residential real estate demand, Lucie Couillard, August 2020.

[104] Figures represent the number of Canadian Real Estate Association (CREA) members. But the total number of agents and brokers is higher as CREA is a voluntary trade association which does not represent all brokers and sales representatives in Canada, https://www.crea.ca/about/organization/.

[105] As of November 2020 and provided by FINTRAC

[106] Ibid.

[107] Ibid.

[108] Federation of Law Societies of Canada, About Us. 2020.

[109] Express trusts are offered by Trust Companies that are subject to the PCMLTFA and therefore are partially covered by AML/ATF measures.

[110] Report on Federal Tax Expenditures - Concepts, Estimates and Evaluations 2020: part 8

Sector or Product	Number of Known Entities	Notes
Corporations	Over 2.6 million for-profit corporations, including almost 4,000 publicly-traded companies[111]	
Company Services providers	8[112]	
Non-profit organizations	162,000[113], including 86,000 federally-registered charities[114]	
Prepaid Access (Open-Loop)	74 companies[115]	Prepaid access, as a payment category, represents a small component of payments used in Canada. Despite the small volume, prepaid transactions was the second fastest growing Point-of-Sale (POS) transaction type in Canada in 2019 with 6% year-over-year growth in value, totaling approximately $20 billion but only accounts for 1.5% POS volume.[116] $4.8 billion in total dollars were loaded onto open-loop prepaid in 2019.[117]
Customs Brokerages and Freight Forwarders	Customs Brokerages: 298 Freight Forwarders: 1,747[118]	
Virtual Currencies	142 businesses registered with FINTRAC for virtual currency activities and 311 registered for virtual currency and other MSB activities[119]	Over 8,300 virtual currencies worldwide accounting for US$1.5 trillion in worldwide market capitalization[120]
White Label ATMs	Over 51,000[121]	

[111] Source: Statistics Canada, Canadian Business Patterns Database, December 2013. The information on publicly-traded companies is drawn from www.tsx.com,www.tsx.com.

[112] Based on internal research.

[113] https://apps.cra-arc.gc.ca/ebci/hacc/srch/pub/bscSrch?q.srchNm=&q.stts=0007&p=1 (85,912 – 30/08/2019)

[114] As of December 2020 and provided by the by the Canada Revenue Agency – Charities Directorate.

[115] According to the Canadian Prepaid Providers Organization (CPPO), Retrieved at https://www.newswire.ca/news-releases/cppo-releases-first-ever-canadian-prepaid-heatmap-as-industry-reaches-almost-5b-in-loads-875845814.html#:~:text=There%20are%2074%20companies%20in%20the%20prepaid%20market%20in%20Canada.

[116] According to Payments Canada's 2020 report: PaymentsCanada_2020CanadianPaymentsMethodsAndTrendsReport_En.pdf

[117] According to the Canadian Prepaid Providers Organization (CPPO), Retrieved at https://www.newswire.ca/news-releases/cppo-releases-first-ever-canadian-prepaid-heatmap-as-industry-reaches-almost-5b-in-loads-875845814.html#:~:text=There%20are%2074%20companies%20in%20the%20prepaid%20market%20in%20Canada

[118] Source: Canada Border Services Agency

[119] As of November 2020 and provided by FINTRAC.

[120] As of February 2021. Retrieved from http://coinmarketcap.com/currencies/views/all/.

[121] As of August 29, 2018. Retrieved from https://cba.ca/abm-market-in-canada. https://cba.ca/abm-market-in-canada.

Demographics

Approximately 87 per cent of Canada's 38 million people live in the country's four largest provinces: Ontario (38 per cent), Québec (23 per cent), British Columbia (14 per cent) and Alberta (12 per cent).[122] The three largest Canadian cities, in terms of population, are Toronto, Montreal and Vancouver. Data from the 2016 Census conducted by Statistics Canada indicates that, that there are about 8.2 million first generation Canadians, which include foreign-born individuals who are now, or once were, immigrants. More than 279 ethnic origins were reported by respondents to the 2016 Census.

Canada is a multiethnic and multicultural country. This results in a very rich and diversified Canadian society. However, it can also become a vulnerability in certain circumstances or situations that criminals can exploit. Certain diasporas have been, in the past, and are still, in some instances, exploited for criminal or terrorism support purposes. Many individuals have immigrated to Canada because of conflicts and poor living situations in their native countries and are therefore concerned about the safety and well-being of family members left behind. Consequently, they often send money and goods back home to help when they can and do that through various means and for different reasons or causes.

All Canadian citizens and permanent residents can, however, be vulnerable in situations where they want to help people in need in foreign countries. For example, they can be extorted while family or friends in those foreign countries are threatened. Others can also be radicalized through propaganda (online or other medium) or by charismatic leaders, and become supportive of causes or ideologies of extremist or terrorist groups fighting in conflict zones. Certain individuals may even adopt extremist and terrorist group ideologies and wish to support those groups financially and/or materially, or even travel to fight overseas to become a foreign fighters.

Discussion of the Results of the Inherent Vulnerabilities Assessment

ML/TF Vulnerabilities of Deposit-Taking Institutions (High to Very High): Of the assessed deposit-taking institutions, domestic banks continue to be rated the most vulnerable (very high), primarily driven by the size of the six designated domestic systemically important bank (D-SIBs).[123] Canada's financial system is stable and highly concentrated. The D-SIBs are still very significant in terms of their transaction volumes, asset holdings and scope of operations, both domestically and internationally, and, on a consolidated basis, are not only involved in banking but also encompass trust and loan companies, life insurance companies, and securities dealers. They offer a large number of vulnerable products and services to a very large client base, which is comprised of a significant amount of high-risk clients and businesses. Banking services are provided through face-to-face and non-face-to-face delivery channels that vary in terms of the degree of anonymity and complexity. There are also opportunities to use third parties and intermediaries (e.g., lawyers and accountants) to undertake banking transactions.

[122] Statistics Canada. Population estimates, quarterly, Q3 2020. Table: 17-10-0009-01.

[123] For more information on DSIBs, see: Superintendent formally designates Canadian D-SIBs and sets minimum loss absorbing capacity requirements (osfi-bsif.gc.ca).

The vulnerability of credit unions and caisses populaires, foreign bank branches and subsidiaries, trust and loan companies also continue to be rated high. These institutions remain significant in terms of their size and scope and are accessible to a broad range of clients. Foreign bank branches are believed to be less accessible to retail clients, with a larger proportion of its business focused on corporate clients (given the $150,000 minimum deposit threshold). All of these institutions offer a range of vulnerable products and services (e.g., checking accounts, wire transfers) and undertake a mix of transactional, ongoing, and third-party business. These vulnerable products and services are available to a client profile, of which a significant amount consists of high-risk clients. Foreign bank subsidiaries often target specific diaspora communities in Canada as well as foreign individuals, which may make them more vulnerable to foreign politically exposed persons (e.g. head of state or head of government; member of the executive council of government or member of a legislature; deputy minister or equivalent rank) and clients with connections to high-risk jurisdictions. Credit unions and caisses populaires operate in more remote Canadian locations that, in some instances,[124] may be exposed to high crime and corruption activities as well as transient workers sending remittances back to their home countries, which may be high risk for money laundering and terrorist financing.

Finally, most of these institutions provide services through face-to-face and non-face-to-face delivery channels, provided online or by telephone, which lends itself to varying degrees of anonymity. There are, however, some foreign subsidiaries that offer banking services exclusively in a non-face-to-face environment. In contrast, credits unions, as a sector, tend to focus more on fostering face-to-face interactions through branch locations, which makes the business relationship less anonymous.

ML/TF Vulnerabilities of the Money Services Businesses Sector (Medium to Very High): As in the previous National Inherent Risk Assessment report, although the MSB sector is broadly vulnerable, the degree of vulnerability is not uniform because of the variation in terms of size and business models found among the MSBs across the sector. Of those assessed, there are two types of MSBs that are most vulnerable. The first consists of the retail multi-service MSBs that have the most dominant presence in Canada. These MSBs in the retail sector offer more than one product or service, and conduct a large amount of transactional business (i.e., wire transfers, currency exchange, and monetary instruments) that have been found to be vulnerable to money laundering and terrorist financing. These products and services are widely accessible and it is assessed that politically exposed persons, clientele in vulnerable businesses or occupations, and clientele whose activities are conducted in locations of concern comprise a significant portion of the clientele profile.

The second type of highly vulnerable MSB are those that use alternative remittance services, including informal value transfer systems and online services dedicated to virtual currency exchanges and transfers that use proprietary platforms to allow connections between merchant and consumer, and facilitate peer-to-peer solutions. The remittance of these funds generally takes place outside of the conventional banking system, although they may occasionally interconnect with formal banking systems. These alternative remittance MSBs are vulnerable because they can allow high-risk clients to wire funds to high-risk jurisdictions through their informal networks. In addition, because they tend to be small, low-profile businesses, it may make them vulnerable to being exploited for illicit purposes. Certain financial technology companies are regulated as MSBs under the PCMLTFA for the services they provide. There has been an observed increase in adoption of digital financial services, which has been accelerated by the COVID-19 pandemic.

[124] For example, areas where extensive oil extraction or mining operations are conducted will often involve transient workers who are frequently well-remunerated in cash. These areas are also known to attract organized crime activities such as drug trafficking.

ML/TF Vulnerabilities of Corporations (Very High) and Company Services Providers (Medium): Although widespread and used for legitimate commerce, corporations retain certain inherent characteristics that make them vulnerable to exploitation for money laundering and terrorist financing. Namely, there is potential to structure entities in a way that conceals the beneficial owner while using them to disguise and convert illicit proceeds. Privately-held corporations continue to be of greatest concern, relative to other forms of legal entities, such as publicly-listed corporations, cooperatives, and not-for-profit organizations. Corporations continue to be used in the international and Canadian context by sophisticated criminals to move and conceal proceeds of crime, often involving foreign-registered and Canadian corporations, professional intermediaries, financial institutions and jurisdictions with reputations for financial secrecy. Foreign-registered companies, particularly those from jurisdictions with reputations for financial secrecy, pose an elevated risk, relative to companies incorporated domestically. Company service providers (CSPs) offering domestic and offshore incorporation services or legal professionals can make it relatively easy to establish corporations expeditiously as part of an illicit scheme, although Canadian companies can nonetheless be formed quickly and inexpensively without the services of a professional.

ML/TF Vulnerability of Express Trusts (Very High): The express trust is a widely used legal arrangement in Canada with a variety of purposes, including wealth management, estate planning, and investment. There were over 450,000 trusts registered with the CRA in 2017.[125] The assets held in and the volume of transactions generated from express trusts are believed to be very significant. The critical vulnerability of the express trust is that it separates control of the assets held in the trust from the beneficial ownership, which can make it difficult to ascertain the identity of the parties to the trust or to freeze and seize assets held in the trust. Discretionary trusts are at the highest risk of misuse as the trustee can exercise their discretion in managing the assets of the trust on behalf of the beneficiary. This makes discretionary trusts more flexible in terms of being able to perform financial transactions conducive to money laundering, such as facilitating flow-through transactions to other jurisdictions, which has been observed in Canada.

High-net worth clients frequently employ trusts for various purposes (i.e., wealth, estate and tax planning). The client profile of express trusts may also include those who value the anonymity and asset shielding that trusts can provide (e.g., protection from civil litigation, regulatory and criminal action, divorce and bankruptcy proceedings). Express trusts have global reach, potentially exposing these trusts to high-risk jurisdictions. Canadians can establish Canadian trusts in Canada or abroad, using domestic or foreign-based trustees, and non-residents can do the same in Canada. Canadian express trusts are predominantly established through or with the help of trust companies, lawyers and accountants. The delivery channel is frequently face-to-face but there is potential to use multiple intermediaries in more complex arrangements.

TF Vulnerabilities of Registered Charities and Non-Profit Organizations (High):[126] This sector is very large, comprising over 162,000 organizations in 2018, of which approximately 86,000 were registered charities. The organizations of greatest concern are those engaged in 'service' activities (education, social services, health, development and housing) that operate in close proximity to an active terrorist threat. This encompasses organizations that operate both in high-risk jurisdictions, including in areas of conflict with an active terrorist threat, as well those that operate domestically, but within a population that is actively targeted by a terrorist movement for support and cover. Some organizations possess characteristics that make them vulnerable to terrorist financiers, including raising and disbursing funds and gifts-in-kind, enjoying the public trust, and being cash-intensive. However, the government recognizes that many Canadians have ties to communities around the world which they maintain, and that while there are risks, these relationships are not, in and of themselves, evidence of terrorist financing and money laundering.

Many financial transactions conducted by these organizations may be performed via delivery channels involving a high degree of anonymity (e.g., anonymous donations) and involving some level of complexity, such as when multiple intermediaries are involved. In some instances, the use of cash, international transfers and weak

[125] Report on Federal Tax Expenditures - Concepts, Estimates and Evaluations 2020: part 8.

[126] The vulnerabilities assessment for non-profit organizations for terrorist financing is presented here while the assessment for money laundering is included as part of the section on corporations.

governance structures may make the original source of funds difficult to determine. It may also be difficult to know how the funds or resources will be used once transferred to partner organizations or third parties, including agents.

ML/TF Vulnerabilities of Partnerships (High): Similar to corporations, the key vulnerability of partnerships is that they can be structured to conceal their beneficial owners, which criminals can exploit to hide their illicit proceeds. Partnerships can be used by criminals to commingle illicit funds with legitimate business income, and to hold and transfer proceeds of crime as part of money laundering schemes. Many types of businesses can operate as a partnership, making them highly flexible and able to integrate with multiple sectors of the economy, including the financial and legal sectors. Partnerships can be formed by other legal entities, including corporations and other partnerships, to further obscure the ultimate beneficial owner(s). There is potential exposure to high-risk jurisdictions, as Canadian partnerships can operate overseas and foreign partnerships can register to operate in Canada. Foreign-registered partnerships from countries with reputations for financial secrecy can pose an elevated risk.

The formation of partnerships can be done directly between the partners involved, however it could also involve intermediaries, which would make it harder to ascertain beneficial ownership. More complex partnership arrangements may involve the use of professionals, such as lawyers or accountants, for advisory services, opening the possibility of such professionals being used, wittingly or unwittingly, to help create a secretive ownership structure for illicit purposes. Although partnerships, corporations and express trusts can all be used to obscure beneficial ownership, evidence suggests partnerships are used far less frequently for money laundering compared to corporations and express trusts.

ML/TF Vulnerabilities of Brick and Mortar Casinos (High): Brick and mortar casinos continue to represent a high level of inherent money laundering and terrorist financing vulnerability. Casinos conduct a large amount of business across Canada, most of which is highly transactional and cash-intensive. Casinos provide a limited number of vulnerable products and services, but the volume of transactions that are undertaken with these products and services continues to be large. Furthermore, VIP floors of casinos can represent notable vulnerability, as the clientele typically have significant funds and include PEPs or other higher-risk individuals. Casinos' business relationships with clientele are mostly transactional but there are some ongoing relationships (approximately 10 per cent of clientele have an ongoing relationship with a brick and mortar casino). Casino clientele continue to include PEPs, non-residents (e.g., tourists) and clientele in vulnerable businesses and professions. Some casinos offer clients the ability to transfer funds electronically, meaning that funds could be sent to high-risk jurisdictions. Clients can conduct gaming activity in casinos relatively anonymously, although casinos are monitored and some activities require face-to-face interaction with casino staff.

ML/TF Vulnerabilities of Provincially-Regulated Online Casinos (Medium): This sector includes five online casinos operating in Ontario, British Columbia, Quebec, Manitoba and Alberta, as well as the online lotteries and Parlay sports betting activities of the Atlantic provinces. Online casinos continue to provide a limited number of vulnerable products and services, which constitute the majority of the sector's business operations. Online casinos have both transactional and ongoing client relationships. The client profile of online casinos likely includes clients in vulnerable occupations and businesses. The geographic reach of these online casinos is very limited, as the services offered are confined to users based in the province offering the service. 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 still makes it difficult to determine who is in control of the account.

ML/TF Vulnerabilities of the Legal (High) and Accounting[127] *(Medium) Sectors:* Both sectors have a large number of practitioners across Canada that have specialized knowledge and expertise that may be vulnerable to being exploited wittingly or unwittingly for illicit purposes. In the legal domain, this expertise encompasses establishing trust accounts, forming corporations and legal trusts, and carrying out financial, real estate and securities-related transactions, while in accounting this expertise predominantly encompasses financial and tax advice and can include providing help and advice around company and trust formation. Both professions offer vulnerable services to a range of individuals and businesses and can act as third parties in transactions. The client profile of the legal sector is observed to include a combination of PEPs, clients in vulnerable businesses and professions, and clients whose activities are conducted in locations of concern. The client profile of accountants would include high net worth clients, PEPs and vulnerable businesses (e.g., cash-intensive ones). It is believed that accountants have little exposure to high-risk jurisdictions, given that it is mostly domestically focused. Both professions mainly interact directly and in face-to-face setting with their clients, minimizing anonymity. In contrast to accounting services, the provision of legal services is protected by solicitor-client privilege, which can make the business relationship more opaque to competent authorities and other parties to financial transactions.

ML/TF Vulnerabilities of the Life Insurance Sector (Low to High): The life insurance business in Canada is very large and it generates a large volume of policy related transactions. Life insurance companies offer a variety of vulnerable products and services, including wealth management and estate planning. Life insurance companies have ongoing, direct relationships with their clients. It is suspected that there is some interaction with PEPs and other high-risk clients. Within the sector, there are three conglomerates that account for 70 per cent of total net premiums in Canada but have significant operations in foreign countries. Canada only accounts for approximately a third of their overall business, so they may do business with high-risk foreign clients and jurisdictions. Life insurance companies rely on third parties and independent brokers to sell their products. Although transactions are frequently conduced face-to-face, the use of independent agents (i.e., use of an intermediary) adds complexity to the delivery channel.

ML/TF Vulnerabilities of the Securities Sector (High): The securities sector is significant in Canada and accepts large volumes of funds for investment purposes that are usually conducted in the form of wire transfers from bank accounts. The industry is made up of integrated firms (in the six largest banks), institutional firms and retail firms. The six largest banks in Canada make up the majority of security dealers in Canada, and conduct 75 per cent of transactions by volume. The securities sector offers a range of products and services that are vulnerable, including brokerage accounts, a variety of investment products, and wire transfers. These continue to constitute a significant portion of the sector's operations.

Clients include individuals, corporate entities, pension funds, and domestic and foreign institutional accounts. The sector has a combination of transactional and ongoing account relationships. The client profile includes non-residents, high net worth clients, and PEPs in Canada and abroad, although a significant portion of the clientele are not believed to be high risk clients. Operations are not restricted to domestic transactions; the sector continues to have international reach and involve businesses in high-risk jurisdictions. Most securities transactions are less anonymous, requiring face-to-face interactions. However, online brokerages have continued growing since the 2015 Report, and they provide an opportunity for greater anonymity in this area. The nature of the delivery channels can be complex, as it can involve representation by third parties, including lawyers.

[127] 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 Proceeds of Crime (Money Laundering) and Terrorist Financing Act (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.

ML/TF Vulnerabilities of the Real Estate Sector (High): Real estate brokers, agents and developers provide vulnerable products and services, including the development of land, the construction of new buildings and their subsequent 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, lawyers, mortgage providers, insurers and appraisers. The majority of real estate transactions are typically completed face-to-face and are not complex. However, in some markets, transactions are becoming more complex given the use of technology (for identification and signing of electronic documents), as well as the use of third parties and complex corporate ownership structures to conduct transactions.

Other factors that can make real estate transactions more complex include the use of shell companies for property purchased as investments, as opposed to residence, as well as the use of assignment clauses in the Contracts to Purchase and Sell, which allow another buyer (the "assignee") to take over the buyer's rights and obligations before the original buyer takes possession of the property. Real estate brokers, agents and developers can be exposed to high risk clients, including PEPs, foreign investors (including from locations of concern) and individuals in vulnerable occupations and businesses. The sector is vulnerable to laundering of proceeds generated from foreign corruption.

ML/TF Vulnerabilities of Unregulated Mortgage Lenders (High): Although deposit-taking and financial institutions previously discussed (e.g. 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 tens of billions of dollars in mortgage assets. The entities which are not regulated for AML/ATF purposes include Mortgage Finance Companies (MFCs),[128] Mortgage Investment Corporations (MICs), syndicated mortgages or other private lenders such as private corporations, individuals and mutual-fund trusts. They 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 individual or businesses who wish to invest funds to finance the loans.

The 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 (the real estate sector, legal sector, the financial sector and private or institutional investors). The sector is exposed to high-risk clients, including PEPs, foreign investors (including from locations of concern) and individuals in vulnerable occupations and businesses. Some unregulated lenders/private lenders promote their services to individuals more likely to work in vulnerable businesses (e.g., cash-intensive ones). 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 face-to-face, non-face-to-face transactions have increasingly become the norm.

ML/TF Vulnerabilities of Dealers in Precious Metals and Stones (DPMS) (High): There continues to be a large number of DPMS located across Canada (approximately 4,149 DPMS), ranging from very large to very small dealers. These dealers are highly accessible to domestic clients and, in some cases, are accessible to international clients (e.g., through online sales). Many DPMS conduct a large volume of business in high-value goods, some of which are commodities that are vulnerable to money laundering and terrorist financing. The highest vulnerability is ascribed to precious metals such as gold, 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. High value finished jewellery also present some vulnerabilities, including being purchased as luxury goods part of criminal lifestyle. Their level of vulnerability is however generally lower than for commodified metals and stones, especially when such jewellery is sold at retail where an important part of their value is lost. At the low end of the vulnerability spectrum are finished jewellery products of low value sold at retail, which are not effective mechanisms to transfer value.

[128] Of note however, entities such as some MFCs have to comply with Guideline B-20 of the Office of the Superintendent of Financial Institutions, which include AML requirements when they underwrite and administer mortgages packaged and sold to regulated financial institutions or securitized through government-sponsored programs.

DPMS have largely transactional relationships with their clients and there are opportunities for clients to conduct cash transactions with a high degree of anonymity. It is also believed that the client profile continues 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.

ML/TF Vulnerabilities of Virtual Currencies (High): The virtual currency sector is growing in terms of assets and volume of transactions and it continues to employ a variety of complex business/delivery models, involving a range of participants, some of which are evolving rapidly. The sector is becoming integrated with the formal financial sector, including banks, payment providers, and exchanges that are traditional MSBs. The sector provides several types of vulnerable products and services, including virtual currencies, initial coin offerings, and mixers and tumblers.[129] Convertible virtual currencies, which constitute an important part of the sector, continue to be the most vulnerable, largely because of the increased anonymity that it can provide as well as its ease of access and high degree of transferability. Virtual currency providers appear to have largely transactional relationships with their clients in addition to some ongoing relationships.

Given some recent cases, criminal elements appear to be attracted to the level of anonymity provided by convertible, decentralized virtual currency. Notably, there is a potential to be accessed globally, transferred across borders rapidly and outside of traditionally regulated channels or peer-to-peer, circumventing the financial system entirely while avoiding in some cases proper know your customer requirements. Regulatory requirements relating to virtual assets continue to differ across international jurisdictions, and have recently come into force in Canada. Virtual currency can be exchanged, purchased or sold online and some virtual currency may permit anonymous funding (funding using cash or prepaid cards, or third-party through virtual exchangers that do not properly identify the funding source). The anonymity and complexity can pose significant challenges for law enforcement to determine the beneficial owner of the virtual currency, especially as some virtual currencies are being developed and used to enhance anonymity (e.g., privacy coins).

ML/TF Vulnerabilities of Import/Export Companies (High): Import and export companies range in complexity and scale of operations. Their role as a driver of international trade creates opportunities to abuse global trade chains and financial institutions through trade-based money laundering, and to conceal these activities by obfuscating the true parties to trade transactions, as well as the source of funds. For example, import/export companies can conceal the true parties to a TBML scheme through opaque beneficial ownership. Another key method involves layering 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, often through special economic zones (SEZs) to conceal both the origin and destination of goods as well as the counterparties to the trade. There are nearly 5,400 SEZs today, more than 1,000 of which were established between 2014 and 2019. At least 500 more zones (approximately 10 per cent of the total) have been announced and are expected to open in the coming years.[130] The absence of strict regulations and transparency of the SEZs which is beneficial for legitimate businesses, also make them highly attractive for illicit actors who take advantage of this relaxed oversight to launder the proceeds of crime and finance terrorism.

While there are concerns that legitimate import/export companies are vulnerable (by buying and selling goods sourced from proceeds of crime), it is also problematic that many of these companies may be complicit or criminally controlled fronts or shells companies, designed to offer services to OCGs, thereby acting as professional money launderers. Countries with high rates of TBML are frequently located in trading hubs along key international trade routes with a high concentration of import and export companies (e.g., China, Hong Kong, United Arab Emirates).[131]

[129] "Mixers and tumblers" refer to a service that increases the anonymity and privacy of virtual currency holders.

[130] UNCTAD: World Investment Report 2019.

[131] Canada Border Services Agency, Royal Canadian Mounted Police, Financial Transactions and Reports Analysis Centre of Canada. *Trade Based Money Laundering Overview. Presented to the Commission of Inquiry into Money Laundering in British Columbia*. April 2020.

ML/TF Vulnerabilities of White Label ATMs (*High*): White label ATMs (WLATM) are not financial institutions covered under the *Bank Act* and are typically operated by individuals and small businesses outside the banking and credit union industry. The sector's business model is complex (network connectors, ATM sellers, and owners) and is integrated with other sectors such as financial institutions, payment network providers, armoured car services, and equipment manufacturing businesses. This sector has a fairly complex structure since many different players are involved in the business model. This allows criminal infiltration, and there is law enforcement evidence of organized crime groups controlling some businesses involved in the WLATM market. WLATMs can only be used for cash withdrawals but the critical vulnerability is that WLATMs can be owned and operated by criminals who can load the WLATMs with large amounts of illicit proceeds. In addition, given that WLATMs are located in less monitored locations, criminals may be more inclined to use them to withdraw funds using stolen payment cards. Often found in cash-based businesses, small retail establishments, gas stations, bars, and restaurants; WLATMs may be utilized by OCGs during the placement stage of money laundering.

Armoured Car Companies (High): Armoured car companies' services are used by financial institutions, businesses and private individuals to securely transport cash, monetary instruments and valuable goods. There are 12 armoured car services companies listed in Canada, with 2,239 employees, and they provide services on a domestic and global scale (with larger entities having significant global reach). The sector's structure is not particularly complex. Their scale of operations, and the cash-intensive nature of their clientele, allow for them to knowingly or unknowingly play a role in obscuring the origin of funds and provide anonymity for their clientele. The cash logistics and cash management services offered by these companies enable armoured car companies to collect funds, pool them into a central corporate account, and then wire funds to customer accounts as well as provide secure storage outside the formal banking sector. This makes reconciliation and determining the source of funds extremely challenging. These gaps 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 clientele 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, private business or personal addresses.

ML/TF Vulnerabilities of Open-Loop Prepaid Access (Medium): The use of prepaid cards continues to grow rapidly in the Canadian economy but it still represents a small fraction of transactions. While there has been an observed growth of seven per cent year over year, it only accounts for two to three per cent of use at point of sale. Open-loop products are offered across Canada and can be loaded with cash and can be used as a payment method almost anywhere credit and debit cards are accepted. These products can be used to withdraw cash and to undertake person-to-person transfers in Canada and abroad. The business relationship with clients is transactional and cards are issued to individuals physically present in Canada. Given the nature of the product, clients can be high-risk, including those in vulnerable occupations and businesses. Some open-loop cards can be purchased and loaded relatively anonymously while others that are reloadable have higher loading limits require proof of identification. While they are still relatively portable across borders, the environment for issuing these cards in Canada has evolved and there is reduced anonymity which reduces the risk they pose.

Customs Brokerages and Freight Forwarders (Medium): There are 1,747 freight forwarders and 298 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. 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.

Chapter 6: Results of the Assessment of Inherent Money Laundering and Terrorist Financing Risks

All assessed economic sectors[132] and financial products were found to be potentially exposed to inherent money laundering risks while a more limited number were found to be exposed to inherent terrorist financing risks. This chapter presents the results of the assessment of inherent money laundering and terrorist financing risks by sector and by product, which are represented in a number of scenario charts to allow for comparisons between the level (i.e., very high, high, medium or low rating) of inherent money laundering or terrorist financing risks for each of them. Lists of related methods and techniques of money laundering and terrorist financing or their underlying indicators as well as examples of specific inherent money laundering and terrorist financing risk scenarios[133] are provided to further demonstrate how threat actors have exploited or could exploit particular sectors and products.

These indicators should not be treated in isolation, as on their own, they may not be indicative of money laundering or other suspicious activity. They should be assessed by reporting entities in combination with what they know about their client and other factors surrounding the transactions to determine if there are reasonable grounds to suspect that a transaction or attempted transaction is related to the commission or attempted commission of a money laundering offence.

Inherent Money Laundering Risks

By matching the money laundering threats with the vulnerable sectors or products, the assessment revealed that 19 sectors and products[134] are exposed to very high inherent money laundering risks involving threat actors (e.g., organized crime groups and third-party money launderers) laundering illicit proceeds generated from ten main types[135] of profit-oriented crime.

As stated earlier in this report, some of the more sophisticated domestic OCGs and transnational OCGs operating in Canada pose the greatest money laundering threat and, therefore, the greatest money laundering risk, as they are involved in multiple criminal activities, listed below in Table 5, that generate large amounts of illicit proceeds. The majority of these groups use professional money launderers in an effort to avoid detection by authorities since these launderers are generally not involved in the actual predicate offences and have the expertise to develop schemes that make use of multiple money laundering methods and techniques that often involve different sectors, products and services.

Bulk cash smuggling or the use of cash couriers, within Canada and across the Canadian border, is a money laundering method that is frequently used, including by professional money launderers, as the first step in the money laundering process and does not involve any sector, product or service. TBML is another technique used by professional money launderers and OCGs that poses many detection and investigative challenges since it often involves many players and sectors including different types of corporations, deposit-taking financial institutions, MSBs, and brokers that are generally located in various jurisdictions.

[132] It should be noted that the vulnerability and risk to money laundering in regards to non-profit organizations was taken into account as part of the assessment of the money laundering vulnerability and risk for corporations, while a separate and more specific vulnerability to terrorist financing assessment of the non-profit organization sector was conducted.

[133] Money laundering or terrorist financing risk scenarios presented in this Chapter are based on money laundering and terrorist financing expert knowledge and sometimes draw from actual cases or are a composite of multiple cases.

[134] These sectors and products (from highly to very highly vulnerable) are: Brick and Mortar Casinos, Credit Unions and Caisses Populaires, Trust and Loan Companies, Virtual Currencies, Legal Professionals, Foreign Bank Subsidiaries, Securities Dealers, Corporations (including non-profit organizations), Alternative Remittance MSBs, Retail Multi-Service MSBs, Domestic Banks, as well as Express Trusts.

[135] The ten profit-oriented crimes generating the most proceeds and posing a high to very high threat are: human smuggling, payment card fraud, tobacco smuggling and trafficking, mass marketing fraud, mortgage fraud, capital markets fraud, illicit drug trafficking, counterfeiting and piracy, corruption and bribery, and commercial trade fraud.

Figures 1-9 provide a graphic representation of all inherent money laundering risk scenarios involving the exploitation by money laundering threat actors of various sectors and products or services, and Table 5 lists all the types of criminal offences that generate illicit proceeds that can then be laundered. The numbers 1 to 10 on the X-axis (i.e., horizontal axis) of Figures 1-9 should be cross-referenced with Table 5. To facilitate visualization of risk levels, Table 5 combines money laundering threats with equivalent threat ratings. By extension, data points on the X axis may also include more than one money laundering threat. For example, loan sharking and extortion pose the same threat level and are included within number 4 of Figures 1-9 below.

Table 5
Types of ML Threats (from Low to Very High) Used in Figures 1-9

Number on X axis (horizontal)	Types of ML Threats
1	Illegal Fishing
2	Firearms Smuggling and Trafficking
3	Wildlife Crime
4	Extortion; Loan Sharking
5	Human Trafficking; Currency Counterfeiting
6	Pollution Crime; Tobacco Smuggling and Trafficking; Tax Evasion/Fraud
7	Robbery and Theft: Identity Fraud; Counterfeiting and Piracy
8	Human Smuggling; Payment Card Fraud
9	Mass Marketing Fraud; Mortgage Fraud; Capital Markets Fraud; Illegal Gambling
10	Illicit Drug Trafficking; Corruption and Bribery; Commercial (Trade) Fraud; Third-Party Money Laundering

The overall inherent money laundering risk rating for each sector or product was assigned a normalized numerical value of 0 to 1 and is represented on the Y-axis (i.e., vertical axis) and the results on the charts are based on the following colour code and numerical values.[136]

Rating Colour Code

Rating Colour Code	Normalized Risk Rating Value
Very High	>0.875
High	0.626-0.875
Medium	0.375-0.625
Low	<0.375

Some areas have the same money laundering risk rating value and therefore share the same series of points on the charts (e.g., Foreign Bank Subsidiaries and Securities Dealers in Figure 1) and are therefore combined in the legend.[137]

[136] The same applies to the terrorist financing risk charts provided later in this Chapter.

[137] The same applies to the terrorist financing risk charts provided later in this Chapter.

Figure 1a

Inherent ML Risks in Deposit-Taking Financial Institutions and Securities Dealers by Type of ML Threats

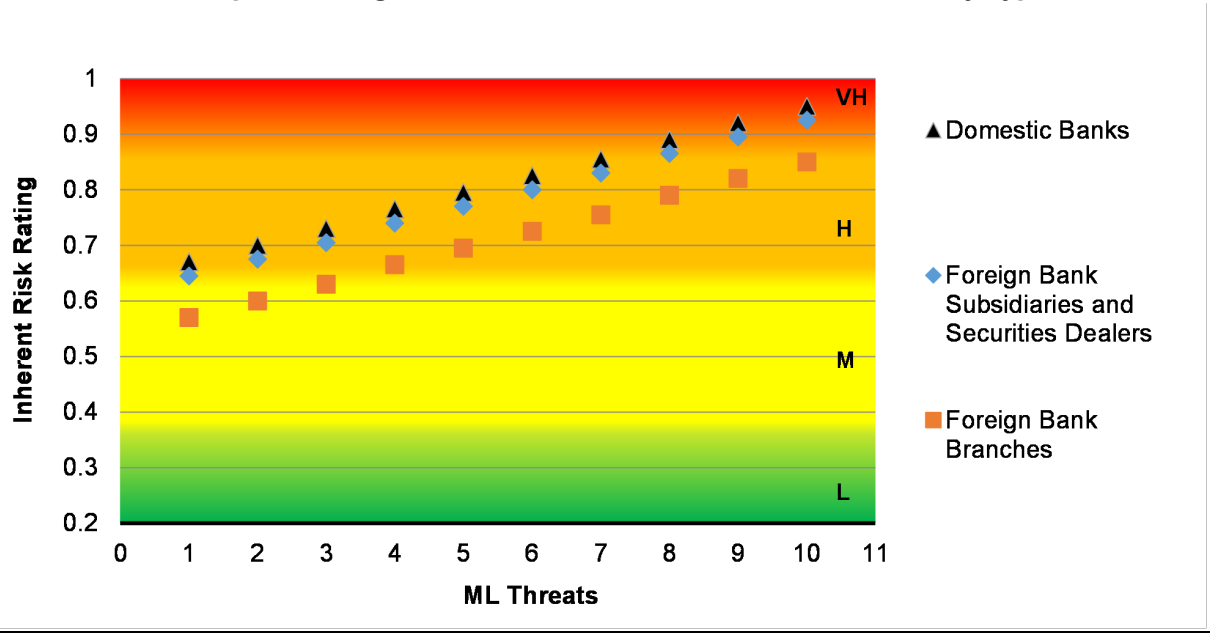
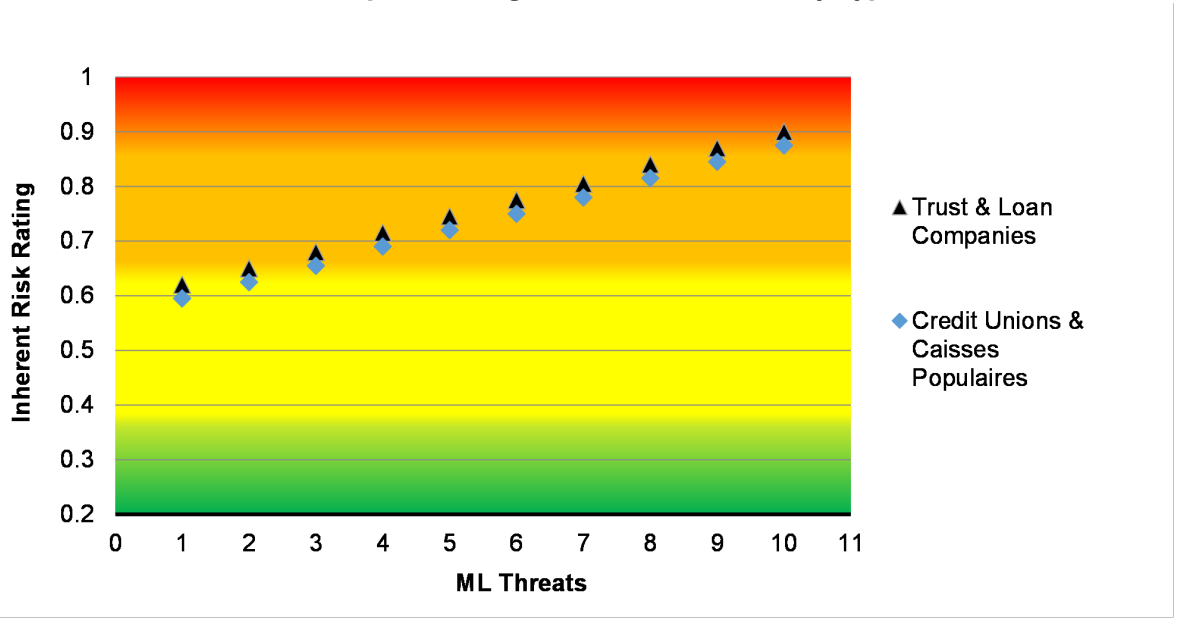


Figure 1b

Inherent ML Risks in Non-Bank Deposit-Taking Financial Institutions by Type of ML Threats



Deposit-taking financial institutions

As illustrated in Figures 1a & 1b, the majority of money laundering risk scenarios involving the banking sector, securities dealers, trust and loan companies, credit unions, and caisses populaires are rated high with a few in the medium or very high range.

Deposit-taking financial institutions are well known to be used for the placement and layering stages of money laundering, for example, through the use of personal and business deposit accounts; domestic wire transfers and international EFTs; currency exchanges; and monetary instruments such as bank drafts, money orders and cheques (i.e., personal and travelers'). In addition, professional money laundering networks with links to Canada mainly rely on TBML and criminal informal value transfer systems (IVTS) to launder the proceeds of transnational OCGs. Criminal IVTS and TBML heavily rely on the formal financial system, and particularly on products and services offered by the banking sector.

Main money laundering methods and techniques used to exploit these products and services include the following:

- Structuring of cash deposits or withdrawals and smurfing (multiple deposits of cash by various individuals and low-value monetary instruments purchased from various banks and MSBs);
- Rapid movement of funds between personal and/or business deposit accounts within the same financial institution or across multiple financial institutions, as well as comingling of proceeds of crime with legitimate business revenues;
- Use of nominees (individuals and businesses);
- Large deposits of cash and monetary instruments followed by the purchase of bank drafts or EFTs to foreign individuals;
- Exchanges of foreign currencies to Canadian currency and vice-versa;
- Refining (i.e., converting large cash amounts from smaller to larger bills); and
- Non face-to-face deposits (e.g., online transactions, night deposits, armoured cars).

Typical inherent ML risk scenario involving deposit-taking financial institutions

Members of an OCG involved in drug trafficking, counterfeiting, tobacco smuggling, and human trafficking generate, on a weekly basis, large amounts of cash and also receive international EFTs for some of their criminal activities. Given the large amount of illicit proceeds they generate, they have hired a professional money launderer who is coordinating a number of money laundering activities with the assistance of money mules, nominees, and smurfs.

Money pick-ups are organized and sometimes involve foreign travel, hence the illicit cash is often smuggled into Canada. The same individuals or others are instructed to, over a number of days, deposit cash, using ATMs (during the day or at night), under the $10,000 reporting threshold into various personal and business accounts held at multiple deposit-taking financial institutions. Some are then instructed to purchase bank drafts or issue cheques in the name of identified nominees who then deposit them into other accounts. Funds are then transferred to other individuals or businesses through domestic wire transfers or international EFTs, the latter in instances when individuals or businesses located in foreign countries are part of the money laundering schemes.

At the direction of the professional money launderer, some individuals are also responsible for conducting currency exchanges and refining activities before depositing cash into personal or business accounts, or just handing over the resulting cash to the professional money launderer or other identified individual(s).

Trust and loan companies offer additional services that can be mainly used in the layering stage of money laundering. For example, trust and lending accounts can be used to conceal the sources and uses of illicit funds, as well as the identity of the beneficial and legal owners. Criminals who are customers or account beneficiaries usually want to remain anonymous in order to move illicit funds or avoid scrutiny. Therefore, they may seek a certain level of anonymity by using a professional's trust accounts, creating private investment companies, offshore trusts, or other investment entities that hide the true ownership or beneficial interest of the trust. Typically, when offshore trusts are used in money laundering schemes, the back and forth movement of funds will be observed between various accounts in Canada and other countries.

Securities Dealers

Products and services offered by the securities sector have been mainly used in the layering stage of money laundering. The following methods and techniques have been observed in the securities sector:

- Deposits of physical certificates (little information is available to the broker to confirm the source of the funds used to purchase the shares or how the client obtained them);
- Securities traded over the counter (OTC) are exchanged directly between entities rather than through an organized stock exchange such as the Toronto Stock Exchange (TSX). OTCs range in their reporting activities, with the "highest tier" OTC securities meeting the stringent financial reporting standards, and the "lowest tier" OTC securities able to provide little or no financial information;
- Early redemption of securities;
- Requesting proceeds of securities sale in the form of negotiable instruments;
- Transfers of funds between accounts held at multiple institutions;
- Frequent changes of ownership;
- Frequent trading and liquidation of low-priced securities; and
- Use of off-book transactions, registered representatives, offshore accounts and nominees.

Inherent ML risk scenario involving stock manipulation:

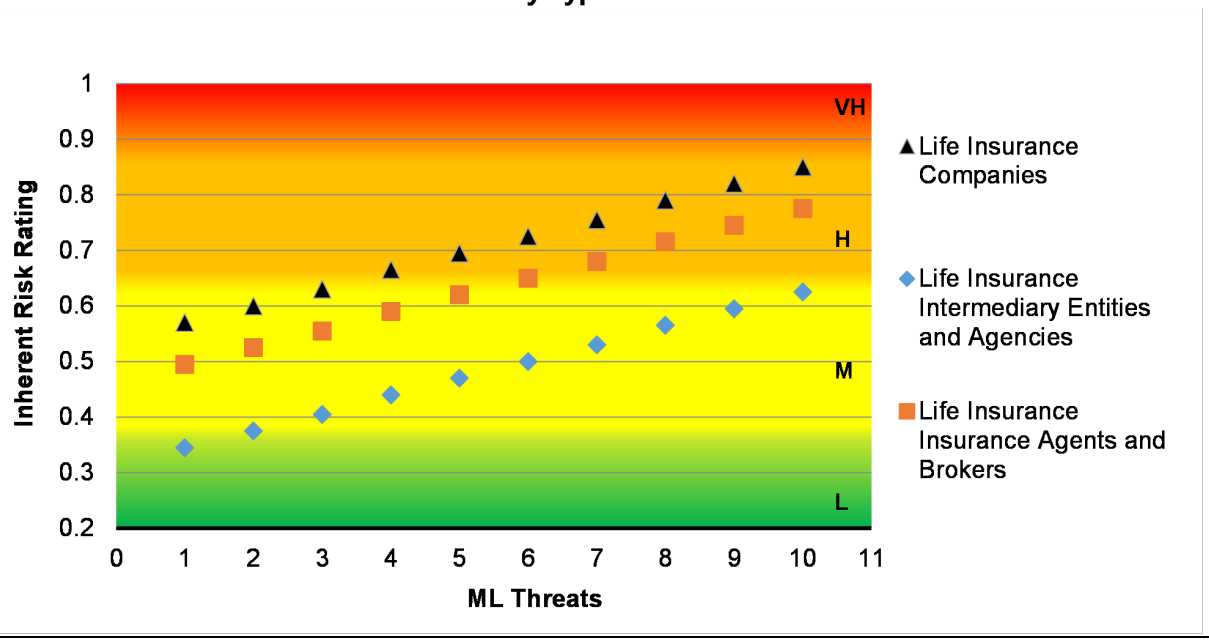
In a stock manipulation case (i.e., capital markets fraud), after the share price was artificially increased, the perpetrators of the fraud used nominees to deposit physical certificates of that company into brokerage accounts. It is suspected that the physical certificates were given to the nominees in an off-market transaction. The shares were sold on the open market shortly after the deposits. The funds were quickly removed from the brokerage accounts and wired offshore to individuals suspected to be responsible for the stock manipulation scheme.

Inherent ML risk scenario involving over-the-counter securities:

A subject of an investigation purchased over one million shares in a company traded over the counter in an off-market transaction for less than a third of the market price. An investment company sold the shares through an integrated firm (i.e., a major financial institution) on the behalf of the investigative subject. The terms of the sale of these shares were suspected to be predetermined by the investigative subject and the purchasing party, in order to transfer the criminal proceeds. The shares were sold the next day at market price, which enabled the share purchaser to receive a 300 per cent return on their investment in one day, and provided a seemingly legitimate explanation for the source of the criminal proceeds.

Figure 2

Inherent ML Risks in the Life Insurance Sector by Type of ML Threats

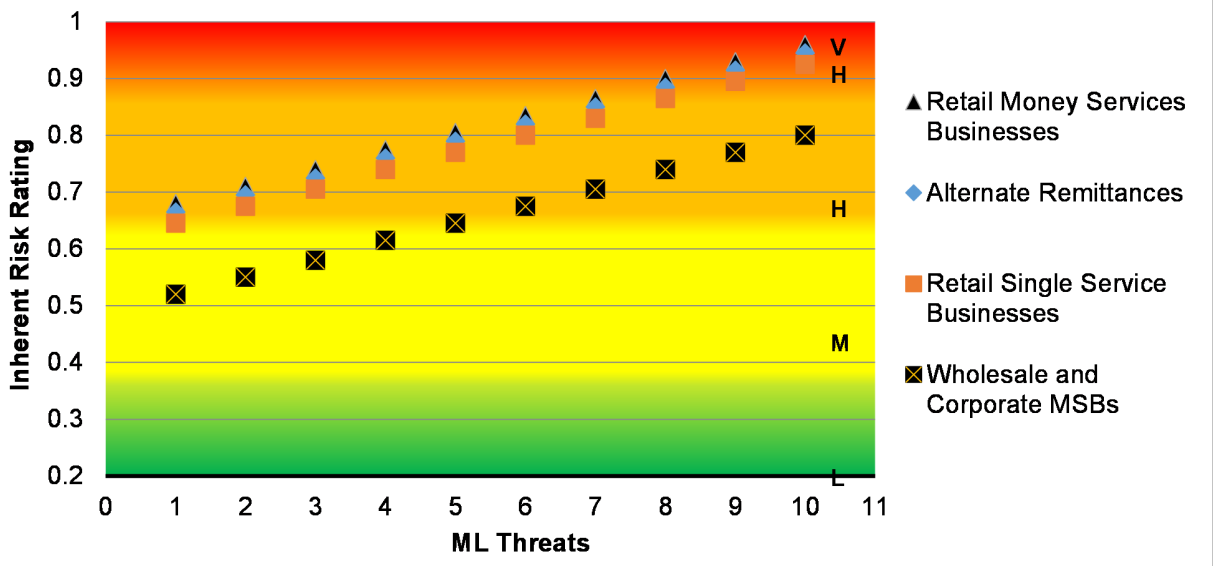


As illustrated in Figure 2, money laundering risk scenarios involving life insurance companies and/or individual agents/brokers are rated medium to high. Given that life insurance intermediary entities and agencies mainly provide administrative support to advisors, allow commission pooling opportunities, provide access to insurance company products, and do not generally deal directly with clients, they are exposed to low to medium inherent money laundering risk scenarios.

The following money laundering methods and techniques have been identified in this sector and mainly involve life insurance companies and/or individual agents/brokers:

- Early redemption/surrendering of life insurance products with single premium payments and/or high cash values;
- Premium payments made by third parties;
- Use of offshore policies and professional advisors;
- Direct co-option of life insurance industry representatives by criminal elements (e.g., through infiltration, corruption.);
- Anonymous account ownership/beneficiary;
- Repeated/rapid changes to account ownership/beneficiaries;
- Multi-party/source financial transactions;
- Large cash transactions – although this sector allows for very few cash transactions;
- Rapid deposit/payment and withdrawal/redemption; and
- Multiple below-threshold (structured) transactions – mainly in relation to money laundering layering stage once proceeds have been placed in other sectors, for the exception of life insurance fraud proceeds that may be directly placed in this sector.

Figure 3
Inherent ML Risks in the Money Services Businesses Sector by Type of ML Threats



The majority of money laundering risk scenarios illustrated in Figure 3 and involving all types of MSBs, with the exception of wholesale and corporate MSBs, are rated high to very high. Inherent risk scenarios associated with wholesale and corporate MSBs mainly fall into the medium to high range, since they offer a more limited number of products and services, predominantly EFTs and bank drafts, to a smaller clientele segment (i.e., corporations).

MSB products and services that are the most often used for money laundering and terrorist financing are international EFTs, currency exchanges and negotiable instruments (e.g., money orders). IVTS and cryptocurrency transfers are increasingly recognized as vulnerable to misuse for laundering proceeds of crime. Cash transactions in this sector continue to be very common and it can therefore be used in the placement stage. Other products and services such as EFTs, money orders, and travelers' cheques can also be used in the layering stage of money laundering, and may have suspected roots in underground banking and professional money laundering. Five main money laundering methods/techniques are relevant for the MSB sector and further described in the following money laundering risk scenarios:

- Structuring or attempting to circumvent MSB record-keeping requirements;
- Attempting to circumvent MSB client identification requirements;
- Smurfing, using nominees, and/or other proxies;
- Proceeds of crime can be placed into the MSB via cash transactions, and negotiable instruments, currency conversions and EFTs can all be exploited in the layering phase of money laundering; and
- Refining (i.e., exchange of small denomination to larger denomination bills).

Inherent ML risk scenario involving monetary instruments and structuring:

In one suspected drug trafficking case, an individual made several dozen separate money order purchases, seemingly to structure them below record-keeping thresholds. These money orders were made payable to an MSB and were negotiated in a variety of cities across North America.

Inherent ML risk scenario involving monetary instruments and an attempt to circumvent client identification requirements:

In one case, an individual purchased dozens of money orders valued in the tens of thousands (CAD), in less than a year. Each transaction was structured below reporting requirements, with most of these funds being sent to individuals outside of Canada. The individual provided inaccurate job title information and misleading address information possibly to add apparent legitimacy to transactions which were not commensurate with the individual's actual employment and income.

Figure 4
Inherent ML Risks related to Casinos by Type of ML Threats

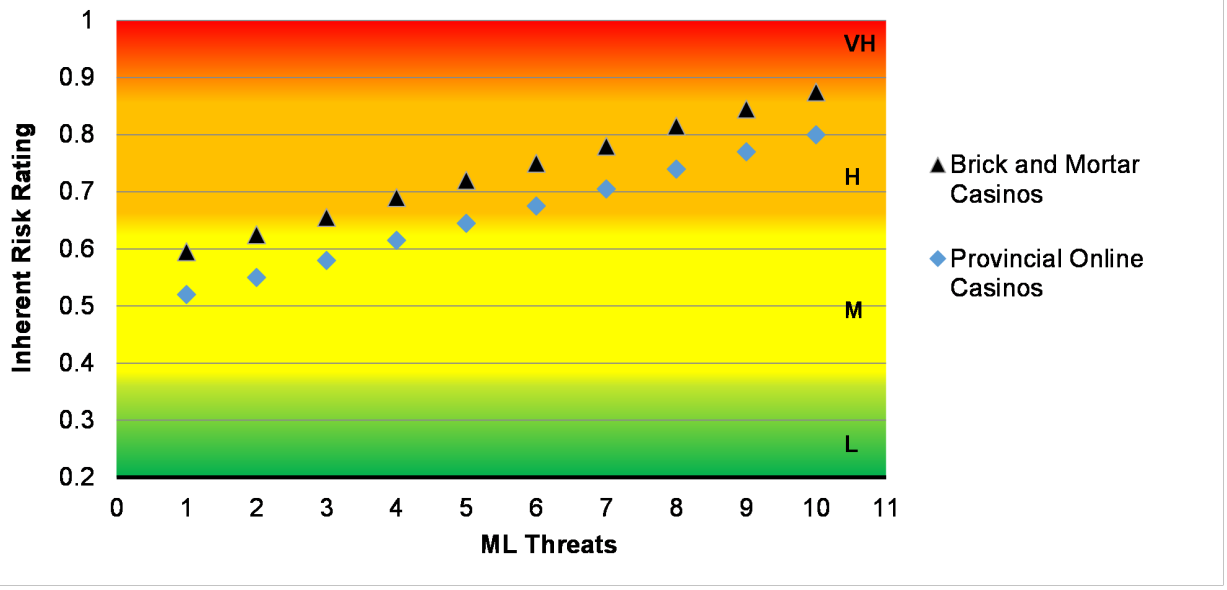


Figure 4 illustrates the different level of money laundering risk scenarios involving brick and mortar casinos, and provincially-regulated online casinos. Given the larger number of products and services offered to clients such as cash purchases of chips, slot machines accepting cash, currency exchanges, self-service ticket redemption machines and so on, brick and mortar casinos are exposed to higher inherent money laundering risk scenarios than provincially-regulated online casinos.

Brick and Mortar Casinos

The most often observed stages of money laundering in brick and mortar casinos are placement and layering and the most common techniques for money laundering are structuring and smurfing. The following methods and techniques have been used in brick and mortar casinos:

- Use of casino value instrument (e.g., chips);
- Refining (i.e., exchange of small denomination to larger denomination bills);
- Currency exchange;
- Structuring;
- Use of front money account;
- Use of bank drafts;
- Loaning proceeds of crime to VIP gamblers;
- Use of credit cards (deposit funds into a credit card account, purchase chips with these funds, cash out the chips, and then use the illicit funds to pay off the credit card account); and
- Line of credit/front money accounts (similar method to use of credit cards, expect illicit funds are used to pay off the line of credit to the casino).

Typical inherent ML risk scenario involving brick and mortar casinos

Members of an OCG involved in multiple criminal activities such as drug trafficking, loan sharking and different types of fraud regularly visit casinos located in one Canadian province and conduct a number of suspected money laundering activities, which include the following:

- Exchanges of small denomination bills for larger denomination bills at the cashier window in amounts under the reporting threshold;
- Buying chips with bills that have a strange smell or appearance (e.g., wrapped in rubber bands, musty smells, unusually dirty);
- Exchanges of a large amount of small denomination bills for casino tickets, and later for large denomination bills;
- Frequent or repeated exchanges at the cashier window large amount of foreign currency (most often USD) for Canadian currency, with minimal or no gaming activity;
- Cash purchases of casino chips in amounts below the reporting threshold;
- Use of multiple cashiers to cash out casino chips in amounts below the reporting threshold;
- Use of money mules to purchase bank drafts from bank accounts funded by a high volume of cash deposits from various sources unknown sources payable to third parties and casinos (deposited into patron gaming fund accounts or used as a form of gaming buy-in);
- Passing of cash, chips or other casino value instrument between related OCG members prior to entering the casino, on the casino floor, at the gaming table, or prior to cashing out;
- Deposits of cash, cheque/bank draft to a front money account, followed by the purchase casino chips, then redemption of the chips for a casino cheque, or withdrawal of all or part of the funds, with minimal or no gaming observed;
- Deposits of small denomination bills to a front money account, followed by withdrawals of the funds in higher denomination bills;
- Cash deposits by a third party to a customer's front money account;
- Credit card purchases of casino chips with minimal or no gaming and then by cash out with a casino cheque, while illicit cash was used to pay the credit card balance; and
- Casino chip purchases, using illicit cash/bank draft, payable to customers engaged in minimal or no game play and then redemption of the chips for a casino cheque.

The "Vancouver Model"

The "Vancouver Model" was originally coined by Professor John Langdale of MacQuarie University and discussed in the 2018 Report by Peter German "Dirty Money: An Independent Review of Money Laundering in Lower Mainland".[138] It is method of laundering money involving wealthy casino patrons seeking to move assets out of a country to avoid government currency controls, in particular China's US$50,000 per year limit. The model follows a typical structure for moving assets and laundering money. The wealthy casino patron provides funds to an underground banker who has a business relationship with professional money launderers in British Columbia. Upon arrival in Canada, the wealthy casino patron is provided cash by Canadian professional money launderers sourced from the proceeds of crime. Once the cash is provided, the foreign underground banker releases the funds in their care to the offshore accounts of the Canadian professional money launderer, or uses them to provide payment in the form of drugs or precursors bound for Canada. The wealthy casino patron uses the cash to gamble at B.C. casinos and upon cashing out receives a casino cheque. In some instances, the casino cheques are used to purchase B.C. real estate.

[138] Peter M. German, "Dirty Money: An Independent Review of Money Laundering in Lower Mainland", March 31, 2018

Provincially-Regulated Online Casinos

Provincially-regulated online casinos can be mainly used in the layering stage of money laundering and may involve methods and techniques described below:

- Criminals collaborating to fix the results of online peer-to-peer games (e.g., poker), in order to transfer money between themselves;
- Multiple people using a single account;
- Using stolen or fraudulent credit cards to open an account;
- Funding gaming accounts using the proceeds of crime (e.g., from a bank account) and requesting a payout after minimal gaming activity;
- Purposefully overloading funds in a gaming account beyond its limit, which triggers an automatic refund to the customer, in the manner requested by the customer (e.g., transfer to bank account, cheque); and
- Funding a gaming account from multiple bank accounts set up by criminal associates.

Figure 5a

Inherent ML Risks related to Other Non-Financial Businesses and Professionals by Type of ML Threats

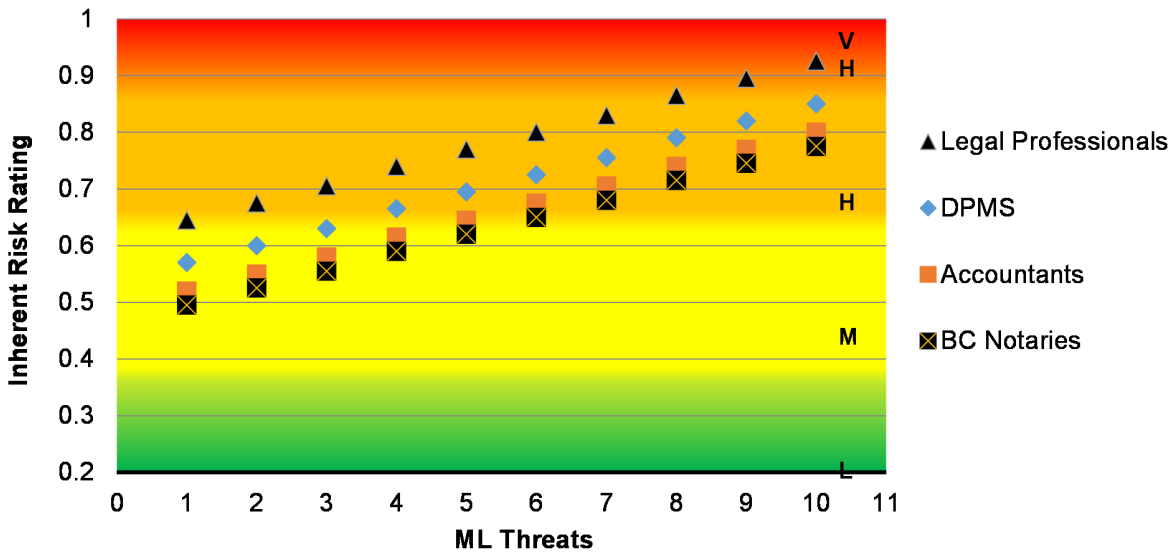
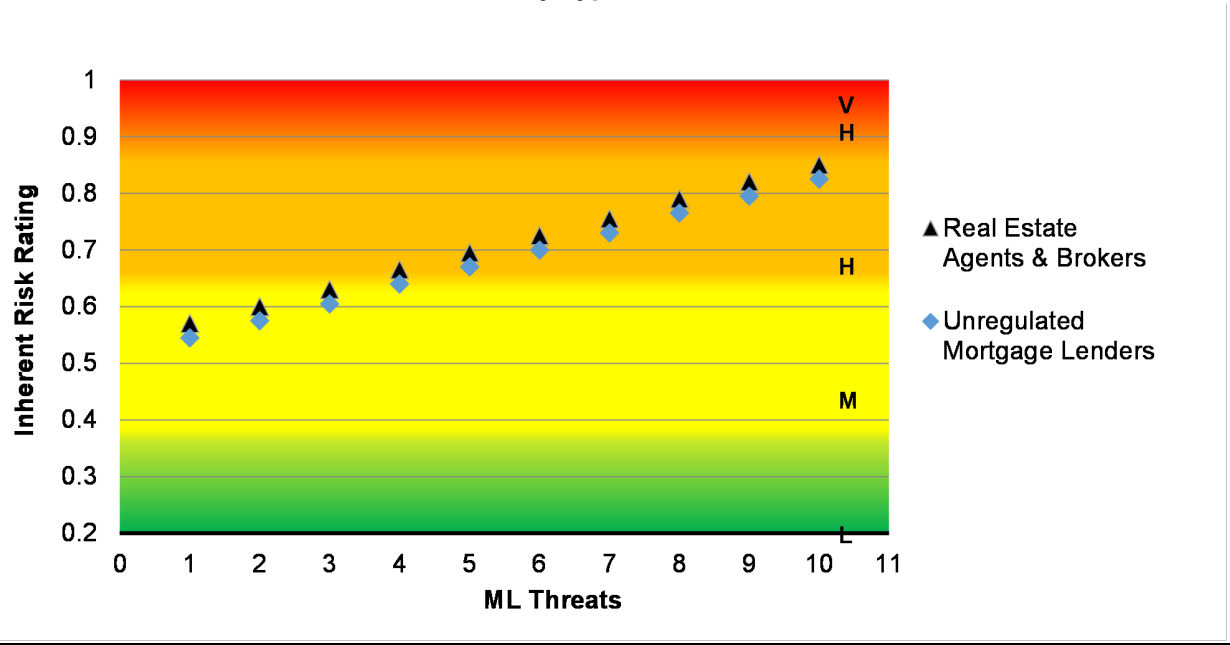


Figure 5b

Inherent ML Risks related to Real Estate Sector by Type of ML Threats



The majority of the non-financial businesses and professionals represented in Figures 5a and 5b are exposed to high money laundering risk scenarios, although a few fall into the medium risk category or very high category in the model.

Legal Professionals and B.C. Notaries

Given the nature of the products and services (e.g., formation and management of corporations and trusts, executing high value transactions and purchases) offered by legal professionals to their clients, they are exposed to high to very high inherent money laundering risk scenarios. Although B.C. notaries offer similar services, their activities are mainly limited to the province and therefore money laundering opportunities are more limited and they are exposed to lower risks (i.e., medium to high).

Legal professionals and B.C. notaries may be used as intermediaries to put distance between criminal activities and the proceeds generated by those activities, and therefore to hide the source and true beneficial owners of such funds, and that, often through complex corporate or trust structures, formed with the assistance of legal professionals. This assistance also adds a veil of legitimacy to the movement of funds and other business operations. Taking enforcement action against complicit legal professionals could also be difficult as there may be claims of solicitor-client privilege.

Inherent ML risk scenario involving the legal profession and trust accounts:

Observed across multiple cases, legal professionals and trust accounts could be used knowingly or unknowingly to launder illicit proceeds. Money laundering activities have been observed to involve a lawyer's trust account where:

- Receiving incoming international wire transfers to the benefit of Canadian trust accounts;
- The use of a trust account in bankruptcy fraud;
- Facilitating purchase or financing of assets, including real estate transactions using proceeds of crime;
- Laundering proceeds of crime using trust accounts as a flow-through account; and

International wire transfers from Canadian trust accounts to accounts in offshore locations such as the British Virgin Islands, the Bahamas and Panama.

Real Estate Sector

The products and services offered by real estate agents and developers provide opportunities to criminals and money launderers.

Some examples of common methods or related indicators used by criminals to launder illicit funds through real estate related transactions may include:

- The under-valuing or over-valuing of property value;
- Rapid successive buying and selling;
- The use of third parties or companies that distance the transaction from the criminal source of funds;
- Hiding or obscuring the source of funds, beneficial ownership, or the buyer's identity (e.g., by using bank drafts, which are not reportable to FINTRAC, where the true payer is not reflected nor is the bank account number);
- Buying or selling using a nominee, corporation, or trust;
- Involving a real estate broker/sales representative or a non-financial professional as the means for accessing the financial system;
- Commingling proceeds of crime with legitimate real estate business revenues such as rental income; and
- Two main money laundering-specific schemes can involve value tampering and/or purchase-renege-refund.[139]

Other money laundering methods and techniques that allow illicit cash into the financial system include cash purchases or large cash down payments, and cash payments especially in the construction, renovation, and upgrading of real estate assets. Real estate transactions usually involve lawyers and their trust accounts, and this can knowingly or unknowingly provide legitimacy and/or obscure the source of funds. Illicit foreign funds can also be used to purchase Canadian real estate properties, including by wiring funds directly to a lawyer trust account.[140] In addition, real estate sales representatives, mortgage brokers and real estate appraisers can be complicit in laundering proceeds of crime through the purchase of real estate or mortgage fraud.

[139] This refers to the activity involving individuals who commit to purchase a property, make a payment towards it, but then change their mind and receive their funds back.

[140] If these funds are sent through an electronic funds transfer (EFT) from abroad, the EFT would be reported to FINTRAC if greater than $10,000 and any amount could also be reported in a suspicious transaction report if money laundering and terrorist financing were suspected.

Unregulated Mortgage Lenders

The money laundering and terrorist financing vulnerabilities of the sector are fundamentally twofold. Lenders may receive payments from the borrowers that are proceeds of crime, or in some cases, they may unwittingly or wittingly provide financing with funds that are proceeds of crime. Furthermore, a combination of both can be used by sophisticated criminal actors who directly control the transacting parties for compounded layering effects and capacities.

Mortgages can be obtained to avoid the suspicion associated with large personal financing of a purchase or to limit a criminal's equity in a property, which can minimize financial losses if the property is forfeited to the crown. Properties purchased using the proceeds of crime or as part of a money laundering scheme may themselves be used for other criminal activities, such as drug production and trafficking (for illegal growth operations and drug productions sites), or sexual exploitation (bawdy houses). Similarly, a mortgage can be obtained to conduct for-profit mortgage fraud.

Issuing real estate loans (often to borrowers in precarious financial positions or unable to secure a loan with another lender) can be a lucrative way to reinvest funds generated from illicit activities, with repayments providing a form of income with an appearance of legitimacy. This is likely to be undertaken in combination with other criminal activities, such as loan sharking. Another area of significant concern are mortgage loan schemes involving different shell entities and nominee structures (often with a transnational component) controlled by the same criminal actors where the objective is to move and layer funds to obfuscate their origins.

Typologies observed related to mortgage lending are:

- Smurfing of illicit funds by making mortgage repayment in cash;
- Use of shell entities to obfuscate the origins of the funds;
- Lending proceeds through unregulated channels to unaware borrowers. This can be done through mortgage loans registered on title but also through an unregistered loan agreement;
- Involvement of mortgages in same day flips of property with property value inflated;
- Usage of a straw buyer (someone with good credit) who agrees or is coerced to put his or her name on a mortgage application on behalf of another person. In return for their participation, straw buyers may be offered cash or promised high returns when the property is sold. Often, straw buyers are deceived into believing they will not be responsible for the mortgage payments;
- Criminals loan themselves money to purchase property, giving the appearance that funds are legitimate and thus derived from real business activity ("loan back");
- "Back-to-back" loan schemes whereby an individual uses assets obtained through criminal activity as collateral to acquire a mortgage;
- A criminal passes proceeds of crime to an associate. The associate then provides a "loan or mortgage" back to the criminal for the same amount with all the necessary "loan and/or mortgage" documentation, creating an illusion that the funds were legitimate; "legitimately"-scheduled payments made on the loan by the criminal reinforce the scheme; and
- A mortgage loan could be used to access funds to finance terrorist activities.

Dealers in Precious Metals and Stones (DPMS)

Precious metals and stones are valuable commodities, which can be easily concealed, exchanged and transported. Proceeds of crime can be placed, layered and integrated into the financial system through the purchase and sale of precious metals and stones, particularly where these are in more commodified formats. However, an individual who purchases precious metals and stones for subsequent resale is ultimately left with cash or other monetary instruments that could require additional transactions through another regulated sector.

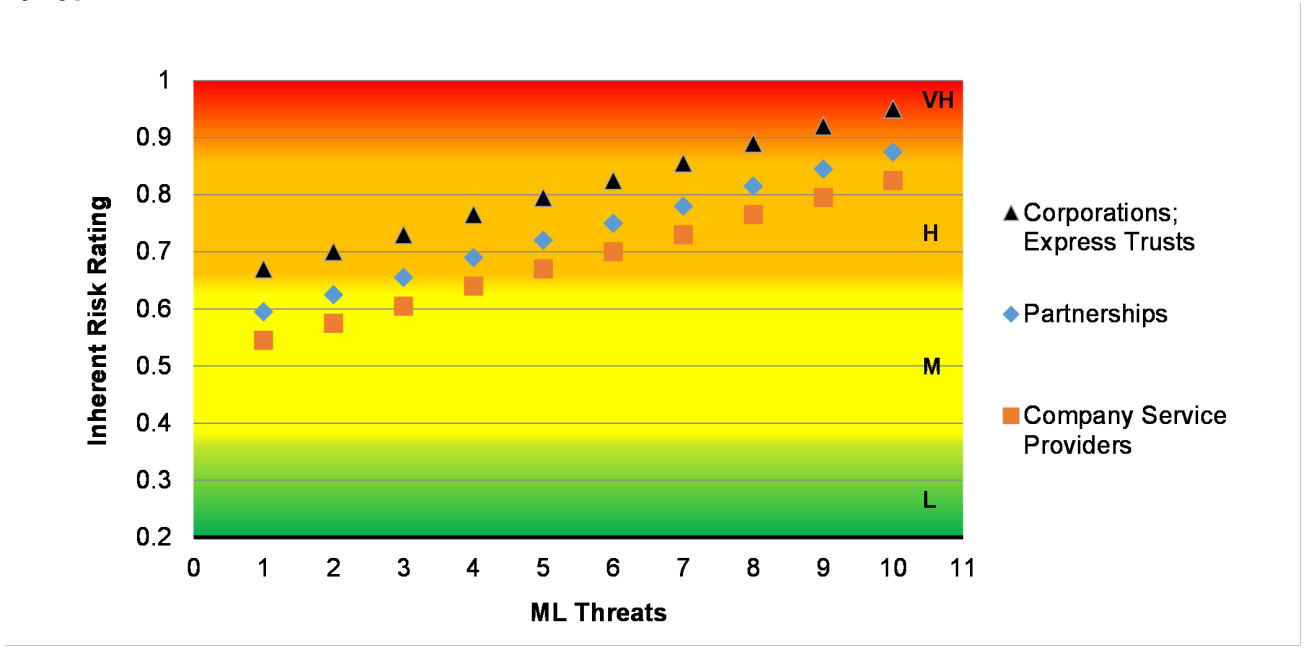
That said, precious metals, precious stones are easily transportable, highly liquid and a highly concentrated bearer form of wealth. They serve as international mediums of exchange and can be converted into cash anywhere in the world. In addition, precious metals, especially gold, silver, and platinum, have a readily and actively traded market, and can be melted into various forms, thereby obliterating refinery marks and leaving them virtually untraceable.

The main money laundering methods observed include:

- Purchase of precious metals and jewellery with the proceeds of crime and subsequent resale;
- Use of DPMS sector businesses as fronts to launder proceeds of crime;
- Use of accounts held with precious metal dealers for laundering the proceeds of crime;
- Direct transactions and purchases of illicit goods;
- Assisting the purchase or anonymizing the purchase or sale of precious metals and jewellery;
- Use of international jurisdictions and entities to purchase and sell precious metals and jewellery acquired with the proceeds of crime;
- The purchase of gold and bullion to act as an alternative currency for criminal activities; and
- The purchase of diamonds to act as an alternative currency for criminal activities.

Figure 6

Inherent ML Risks related to Corporations, Partnerships, Express Trusts, and Company Services Providers by Type of ML Threats



As illustrated in Figure 6, the majority of money laundering risk scenarios involving corporations, partnerships and express trusts are rated medium to very high. Corporations, partnerships and express trusts can be linked to money laundering activities by being used to hide the beneficial owners of illicitly generated funds through very complex structures that can involve multiple jurisdictions and intermediaries. Private corporations continue to feature frequently in FINTRAC money laundering case disclosures to law enforcement.

OCGs use businesses across numerous economic sectors, including construction, transportation, financing and loans, real estate, international trade and cash-intensive businesses to facilitate large-scale money laundering. OCG-controlled businesses may attempt to appear legitimate by making payroll deposits, using online payment platforms, having international operations and employing lawyers and accountants.

As indicated earlier, setting up a corporation, partnership or express trust through intermediaries such as a law firm can be an effective method to conceal beneficial ownership. Corporations can be quickly established and managed by a local company service provider (CSP). Moreover, given the difficulty in differentiating between legitimate and illegitimate financial activity, corporations and partnerships can be effective tools in the layering or integration stages of money laundering. Provincial, territorial or federal incorporation can be done quickly, simply and inexpensively through online government services websites, and the services of a professional (e.g., lawyer, notary) are thus not necessarily required. However, legal professionals may still be sought to assist in establishing more complex corporate structures.

The main money laundering methods observed are:

- Establishing chains of corporate entities and complex ownership structures involving multiple corporations, partnerships and/or express trusts in order to conceal beneficial ownership. Often, this will involve the use of nominees or intermediaries, shell companies and foreign jurisdictions, particularly those with robust corporate secrecy laws. This may be performed by OCGs to launder proceeds from their other criminal activities, or by third-party money launderers on behalf of OCGs;
- Using specialized financial intermediaries and professionals, such as accountants and lawyers, to establish corporate entities and trusts with complex ownership structures;
- Commingling illicit funds with legitimate business income within corporations, and possibly partnerships;
- Facilitating flow-through transactions to other persons or entities, often in foreign jurisdictions. Intelligence suggests that Canadian corporations and express trusts are used both for the exfiltration of proceeds of crime to other jurisdictions, and as a landing spot for foreign proceeds of crime; and
- Depositing proceeds of crime into business accounts registered to corporate entities. Once placed within financial institutions, criminals use domestic wire transfers and negotiable instruments to transfer funds between personal and other business accounts to make funds more difficult to trace.

Figure 7
Inherent ML Risks related to Products Holding Monetary Value by Type of ML Threats

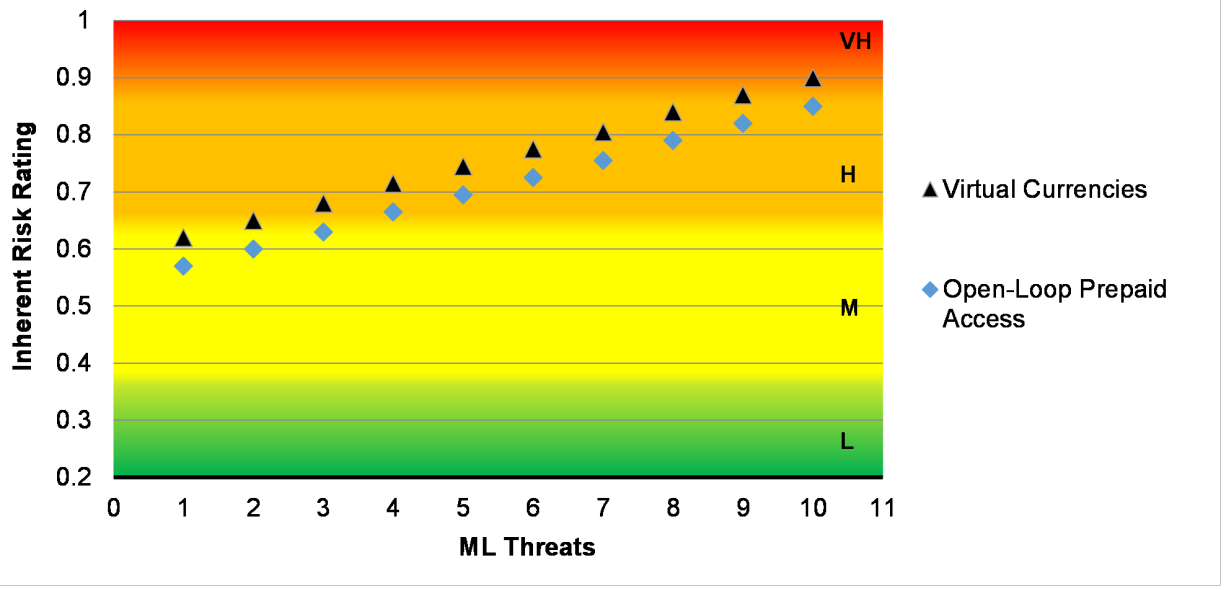


Figure 7 illustrates the level of money laundering risks associated with virtual currencies and open-loop prepaid access products and services. Virtual currencies, in particular convertible ones, are mostly used in high to very high money laundering risk scenarios and can be used in all three stages of money laundering. Open-loop prepaid access products are also mainly used in high ML risk scenarios.

Virtual Currencies

Virtual currency exchanges can be controlled or used by money launderers because of their cash-intensive nature and anonymous services. Criminals can launder their proceeds by buying virtual currency and doing several subsequent layering activities:

- Purchasing goods and services directly with the virtual currency;
- Exchanging the currency again for fiat currency, or obtaining a wire transfer from the exchange company;
- Exchanging one virtual currency to another, several times using different exchange companies and mixers and tumblers, before converting it back to fiat currency;
- Exchanging a virtual currency wallet for fiat currency, transferring the ownership of a wallet;
- Launch initial coin offerings to raise funds, layer, and integrate money obtained through illicit activities.

Some virtual currencies, although not criminally controlled, can be adopted by a criminal network as the form of payment. For example, AlphaBay and Hansa were two of the largest marketplaces on the dark web, allowing customers to buy an array of illicit goods and services with virtual currencies. They were shut down through law enforcement action as a part of Operation Bayonet in the United States, Canada, and Thailand in July 2017. Before they were taken down, both sites had a combined total of over US$1 billion in illicit transactions, with users spread out across the world, including Canada. Both marketplaces offered products and services such as drugs and toxic chemicals, stolen and fraudulent identification documents, counterfeit goods, malware and other computer hacking tools, firearms, and fraudulent services.

Statistics from the Canadian Anti-Fraud Centre (CAFC) highlight a tenfold increase in complaints related to various frauds involving virtual currency and virtual currency ATMs over the past four years. Total complaints have increased from 305 in 2016 to 3,768 in 2019, which includes 1,359 cases that resulted in an individual being victimized (i.e., the complainant was scammed into sending a nefarious entity virtual currency). Total loses as a result of this activity are millions of dollars. As the means of payment in these cases is virtual currency, it presents a high likelihood of money laundering activity in the placement and layering stages.

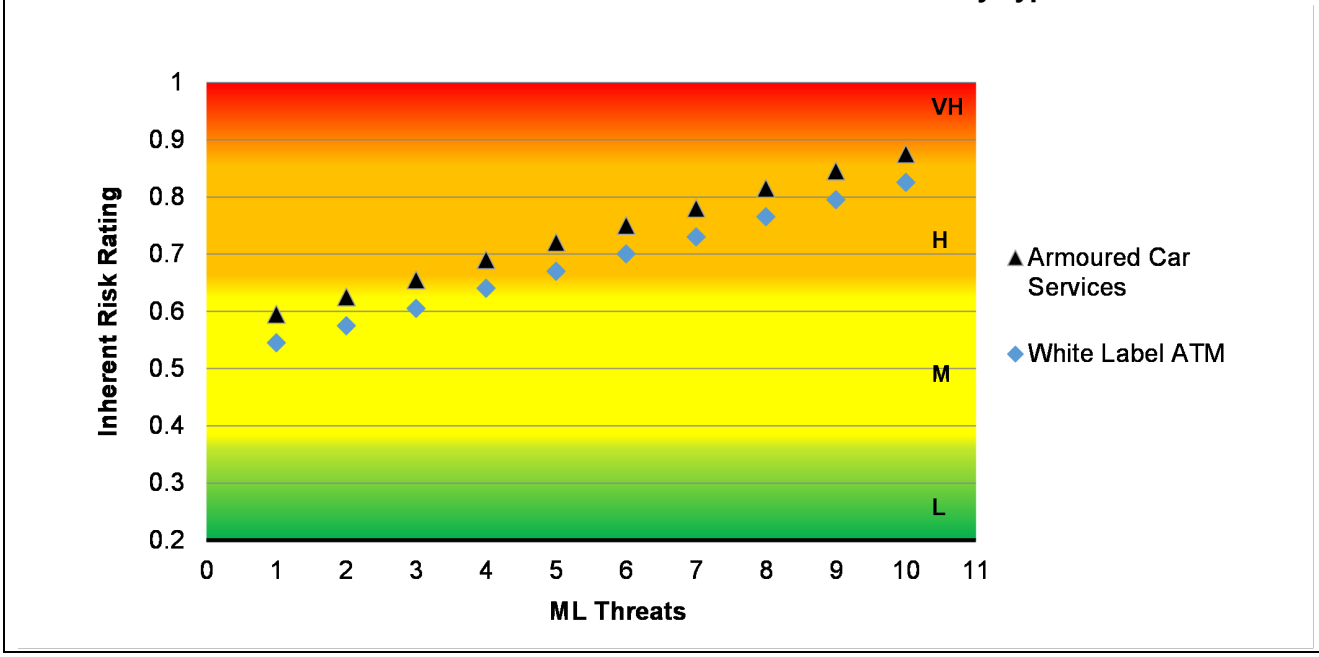
Prepaid Access Products

Because they can be repeatedly loaded with cash and can be used in the same places that regular credit cards are accepted, open-loop prepaid access products can be used for money laundering, particularly in instances when the allowed loading limit is high. The main money laundering methods are demonstrated in the case examples below:

- Law enforcement officials investigated a case which involved over 40 suspects believed to have loaded prepaid cards in another country and then used them to withdraw approximately $350,000 from ATMs in Canada. FINTRAC analysis from 2019 of specific organized crime groups found the presence of complex methods of money laundering that included the use of prepaid cards even among certain groups that primarily relied on self-laundering methods, such as funneling the proceeds of crime through personal accounts.
- In the 2020 Criminal National Intelligence Estimate report, the Criminal Intelligence Service of Canada highlighted the use of prepaid cards as a payment method for fraud schemes, including those involving an individual or group posing as a government representative and demanding payment under threats of arrest or financial consequences.
- A Canadian Internet payment services provider and its foreign subsidiaries were suspected of laundering the proceeds of fraud. Three open-loop prepaid card providers in Canada and the United States were used. Funds were sent from foreign countries to the Canadian Internet payment services provider's bank accounts. The money was then loaded onto prepaid cards for layering in other countries.
- In addition, the U.S. Secret Service has observed "significant" cross-border movement of the proceeds of white-collar crimes and drug crimes from the United States into Western Canada through prepaid cards.

Figure 8

Inherent ML Risks related to Armoured Car Services and White Label ATMs by Type of ML Threats



White Label ATMs

Figure 8 illustrates the different level of money laundering risk scenarios involving white label ATMs. White label ATMs are most often used in the placement stage of money laundering, and the most common money laundering techniques are structuring and smurfing. Companies owning and loading white label ATMs for themselves or for other legitimate businesses may be criminally controlled. The loading of the white label ATMs can be done anonymously and there appears to be limited-to-no-monitoring of the loading activity. Criminals can offer ATM services within different legitimate businesses or set them up in their own businesses. Law enforcement has evidence that some OCGs control some businesses involved in this market. In addition, given that WLATMs are located in more anonymous and less monitored locations, criminals may be more inclined to use them to withdraw funds using stolen payment cards. The following money laundering methods and techniques have been observed:

- White label ATM is loaded with proceeds of crime (illegitimate funds may be commingled with legitimate funds);
- The operator arranges to have the funds withdrawn from their machine or lets funds from machine be gradually depleted;
- A credit from a settlement company for the same amount is transferred to the operator's bank account through third party withdrawals.

Armoured Cars

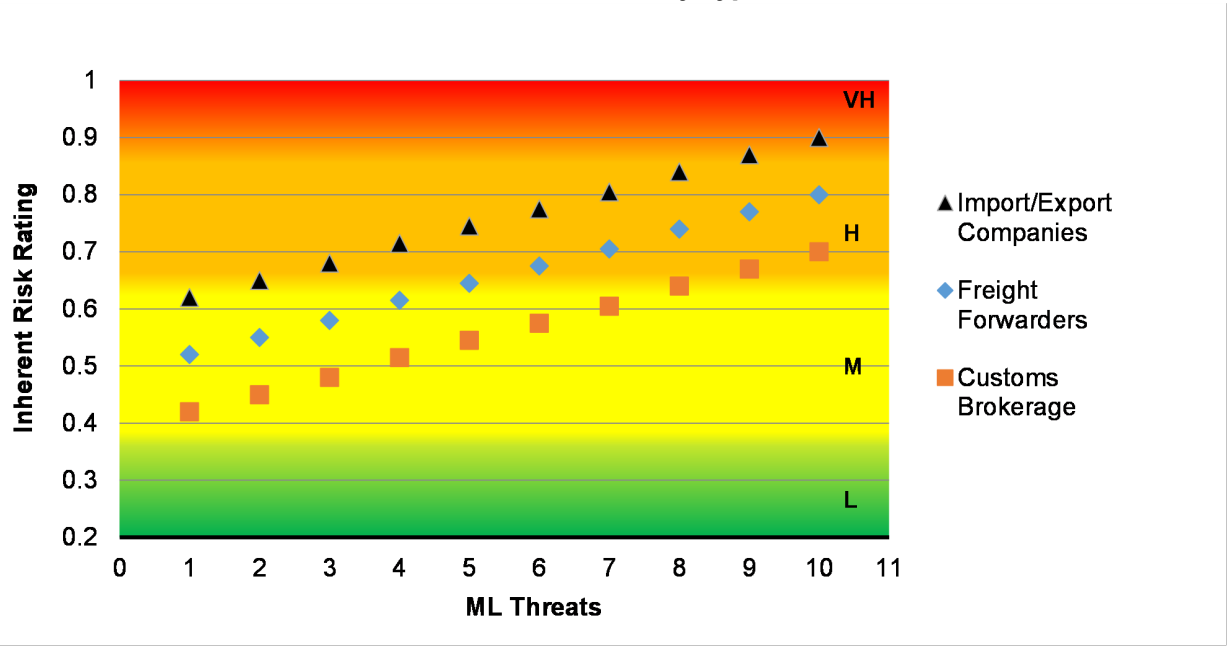
Money laundering in the armored car services sector is most likely to occur through the placement and layering stages. The primary money laundering methods/techniques facilitated by armoured car services could include hiring an armoured car service to:

- Pick up funds from one account/entity, and wire the equivalent value (from the armoured car service's corporate account) to another account/entity, thereby making it difficult to determine the origin of the initial funds (placement phase);
- Conduct cross-border transportation of proceeds of crime, in order to deposit the funds in such a way as to avoid detection (placement stage);
- Move funds from one cash-intensive business to another to obscure the origin of the funds (layering phase); and
- Move high-value goods from one entity to another, including possibly across borders.

The assessment of risk for this sector is based on a qualitative review of their practices and operations. While there are no substantive cases that have been identified in Canada, they do exist in the United States. Understanding that the sector provides services to entities that are identified as high risk as part of this assessment process, as well as its cash intensive nature, and limited oversight and transparency raises the vulnerability that this sector presents despite the lack of domestic case evidence.

Figure 9

Inherent ML Risks related to the Commercial Trade Sector by Type of ML Threats



Import/export companies

Import/export companies may use typical TBML techniques with a particular focus on falsifying elements of the import/export process. TBML involves concealing and legitimizing proceeds of crime by transferring the value of the funds through cross-border import-export transactions, including through the following methods:

- Phantom shipments: Transferring funds in payments for goods that are never shipped, or received or documented either with customs services or commercial transporters (shippers).
- Falsely described goods and services: Misrepresenting the quality, quantity, and/or type of goods or services traded.
- Multiple invoicing: Issuing a single invoice for a legitimate shipment, but sending and receiving multiple payments, or issuing multiple invoices for one shipment of goods.
- Over/under valuation: Valuing goods or services at a price above or below market prices in order to move money or value from the exporter to the importer or vice-versa. Over-invoicing is a common TBML technique; the difference between the declared amount and the actual value of the goods is the volume of illicit funds being transferred between the importer and exporter, or vice versa.

A case example involves an exporter engaged in TBML in Canada under the guise of legitimate exportation of commodities such as scrap metal products. Bank accounts are used by several front and shell companies to move value into and through Canada. The use of import/export companies, front companies and phantom shipments were used to enable the layering phase of money laundering.[141]

[141] RCMP (2020). Case Example provided as part of response to the Joint FATF/Egmont Project on Trade-Based Money Laundering.

Freight Forwarders and Custom Brokers

Although there have been few proven money laundering and terrorist financing cases involving custom brokers and freight forwarders in Canada, these entities may facilitate TBML by acting as a "hidden" intermediary in international trade chains for the purposes of TBML. They maintain a lack of visibility from a customs perspective, yet are able to facilitate customs declarations, which makes the sector conducive to abuse by those seeking to launder through false descriptions of goods either imported or exported.

These entities play an important logistical role for many importers and exporters by managing the movement of their goods from origin to destination markets. Importing and exporting are often just a small aspect of a Canadian company's larger operations, and customs and shipping processes are often extremely complex. Freight forwarders leverage their knowledge and experience of international customs processes, as well as the complex international shipping routes and schedules of goods carriers to bring goods to markets in a timely and cost-efficient manner. However, it also means freight forwarders can use their knowledge of trade chains to conceal suspect shipments from detection. When complicit, both entities are also able to identify vulnerabilities in customs processes, acknowledging that many customs authorities are not able to perform 100 per cent examination of inbound and outbound goods. When they are not complicit, they can be unwittingly used as a facilitator to move illicit goods or facilitate TBML, given that they do not directly handle the shipment themselves and may be misled as to its true nature.

Inherent Terrorist Financing Risks

Depending on the nature and extent of terrorist financing activities in Canada conducted by individuals associated with the different terrorist groups listed in Table 2 (Chapter 4), the breadth of terrorist financing collection/acquisition (i.e., fundraising) and aggregation/transmission methods vary and can involve a limited or extended number of sectors and products/services. In this section terrorist financing threats were matched with sectors that were found to be exposed to inherent terrorist financing. This can be, for example, sectors that have been used in the past to finance terrorism in Canada or from Canada.

The assessment of terrorist financing risks resulted in the identification of four very high terrorist financing risk scenarios that involve a total of six different sectors (i.e., corporations, non-profit organizations and charities, domestic banks, national full-service and smaller retail MSBs and alternate remittances, as well as express trusts) that have been assessed to be very highly vulnerable to terrorist financing, combined with one high terrorist financing threat group of actors.

On the other hand, a total of 53 high terrorist financing risk scenarios were identified that involve, to varying degrees, all 21 sectors and products represented in Figures 10-14 and that were assessed to have a medium to very high vulnerability of terrorist financing. Ten different groups of terrorist financing threat actors rated low, medium and high have or could exploit all or some of those sectors as further explained in the following pages.

The majority of the terrorist financing risk scenarios included in Figures 10-14 were rated lower than for money laundering, and with the exception of the risk scenarios referred to above and rated high or very high, most of them were rated medium.

Each number (i.e., 1-10) on the X axis (i.e., horizontal axis) of Figures 10-14 represents one group of terrorist financing threat actors associated with the different terrorist groups listed in Table 2.

Figure 10a

Inherent TF Risks related to Bank Deposit-Taking Financial Institutions by TF Threat Actors

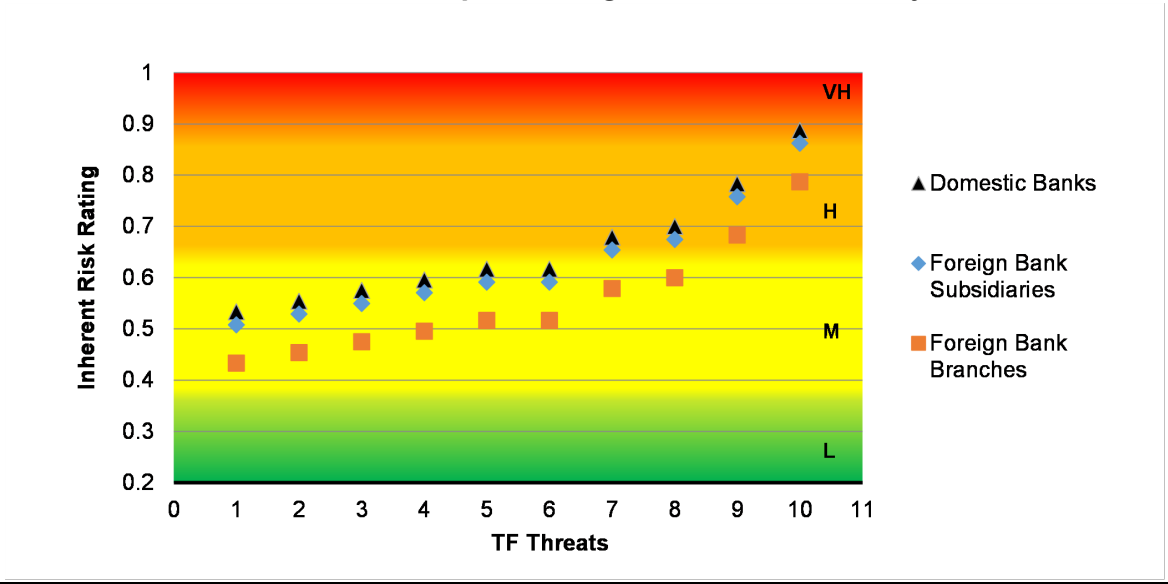
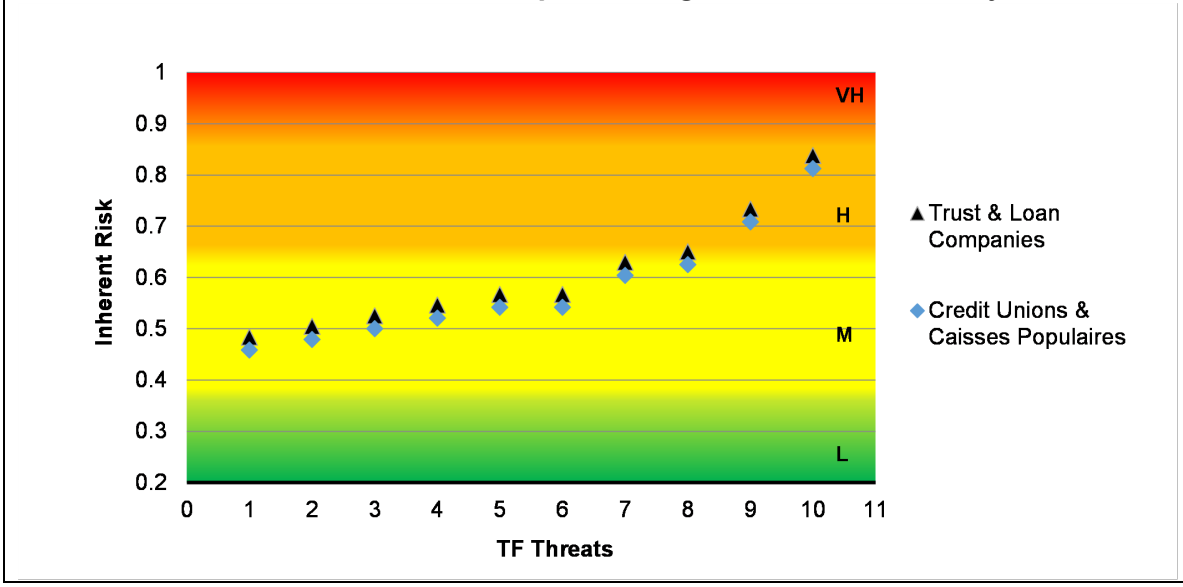


Figure 10b

Inherent TF Risks related to Non-Bank Deposit-Taking Financial Institutions by TF Threat Actors



Deposit-taking financial institutions included in Figure 10 are mainly used in the transmission, as well as sometimes in the aggregation, of funds suspected to be ultimately destined for terrorist groups or individuals, for the majority, active in foreign countries. Similar to money laundering but to support different goals, terrorist financing risk scenarios described below generally involve the use of domestic wire transfers, international EFTs, monetary instruments such as bank drafts, money orders and cheques (i.e., personal, travelers'), personal and business accounts, currency exchanges, trust accounts, as well as loan/mortgage and credit card services. Those operations can be conducted by individuals as well as by legal entities or arrangements such as a non-profit organization or a corporation using banking services at a deposit-taking financial institution.

Inherent TF Risk Scenarios Involving Deposit-Taking Financial Institutions

The majority of terrorist financing actors associated with the terrorist groups listed in Table 2 are suspected of using international EFTs, as one terrorist financing transmission method,[142] to send funds overseas and often in high-risk jurisdictions. Individuals associated with some of those groups may also use domestic wires to move funds within Canada and/or aggregate collected funds (e.g., cash or web-based[143] donations) into one or a few bank accounts (personal or business) before sending the funds overseas. This also means that cash deposits, sometimes conducted by third parties or nominees, may occur when cash donations are obtained through door-to-door solicitation, in charitable events or the use of donation boxes. Cash withdrawals may also occur when, for example, they need funds to pay for their airplane tickets and/or for their terrorist-related expenses. Other terrorist financing methods involve the use of monetary instruments and commingling of illicit funds[144] with legitimate business revenue in Canada.

Other inherent terrorist financing risk scenarios may involve the use of fraudulent loans to raise funds, while email money transfers may be used for the transmission of funds. Credit card fraud, including bust-out schemes[145] and card skimming, have been used by some terrorist financing actors. Business accounts and, in some instances, trust accounts are also suspected of being used to hide the true source or beneficial owner of funds destined for terrorist activity. Finally, some terrorist financing risk scenarios may involve trade-based schemes or the use of businesses as fronts and, therefore would involve the domestic or international movement of funds into and out of business accounts.

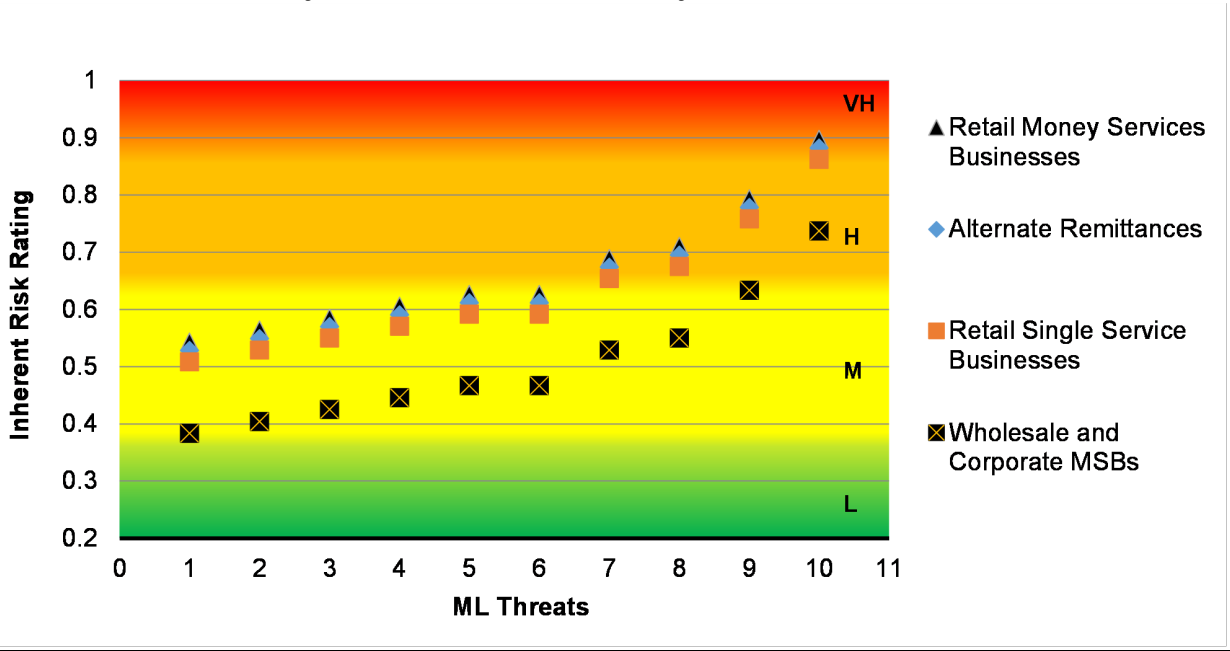
[142] The other main method being used to move funds overseas by many terrorist financing actors is through cash couriers travelling overseas, sometimes themselves and Informal Value Transfer Systems (IVTSs).

[143] Some terrorist financing actors are suspected of having used or still using Internet websites or social media tools (e.g., Facebook, Twitter) to raise funds and such activity sometimes involves what is referred to as crowd funding (i.e., multiple donors contributing funds for the same cause or the same individual). Mobile payment systems have also been used.

[144] Some terrorist financing actors are also known to be involved in criminal activities, mainly thefts (e.g., car theft) and fraud (e.g., credit card, welfare, student loan and visa/passport), generating illicit profits that can then be commingled with the revenue of legitimate businesses they control.

[145] A bust-out scheme involves an individual acquiring credit from a financial institution or business offering credit cards. The credit levels are maintained until the creditor attains a certain level of comfort and increases the credit limit. The available credit is then exhausted by large cash advances and purchases then bogus payments (i.e., using non-sufficient funds cheques) are made to "pay off" the debt in full. The credit limit is then restored by the creditor and the fraudster again takes advantage and exhausts the available credit a second time before the financial institution or business realizes that the payments made were bogus. No further payments are made to the account and the debtor declares bankruptcy. Another twist to this scheme is often the use of stolen or fake identity to obtain credit in the first place.

Figure 11
Inherent TF Risks in the Money Services Businesses Sector by TF Threat Actors

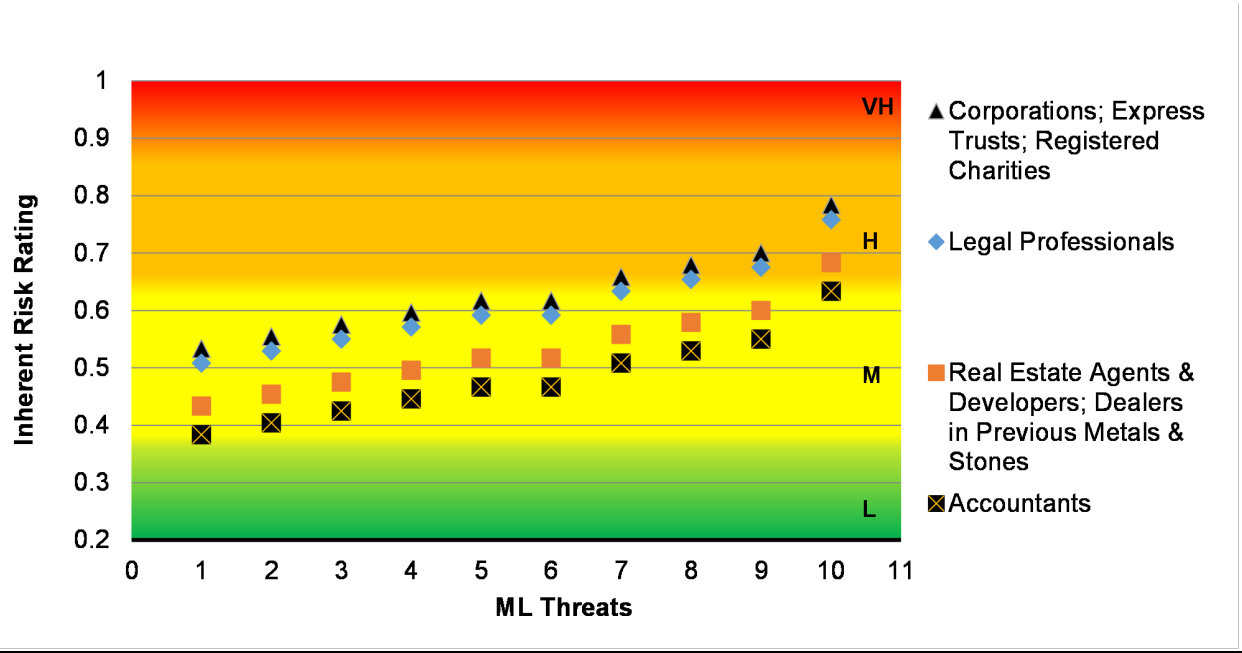


Similar to deposit-taking financial institutions, the products and services offered by MSBs such as currency exchanges, domestic wire transfers, international EFTs and money orders are often used in terrorist financing risk scenarios (rated medium to very high) involving the majority of terrorist financing actors listed in Table 2. Although all types of MSBs illustrated in Figure 10 can be used for terrorist financing activities, it is suspected that national full-service, small independent and smaller retail MSBs are most often used. This is mainly due to the fact that national full-service MSBs operate globally and offer money transfer services to multiple foreign jurisdictions, while smaller retail MSBs offering currency exchanges, domestic wire transfers and international EFTs services are typically agents of national full-service MSBs. Operators of small independent MSBs may move funds to high-risk foreign jurisdictions and possibly have links to informal money value transfer operators. Some of the jurisdictions where funds are sent to or received from may be considered high-risk due to ongoing conflicts and/or the presence of terrorist organizations or other factors.

Terrorist financing actors using web-based donations through social media or crowd funding methods may receive online payments or transfers conducted through Internet-based MSBs.

Figure 12

Inherent TF Risks related to Express Trusts and Non-Financial Businesses & Professionals by TF Threat Actors



As illustrated in Figure 12, the majority of terrorist financing scenarios involving corporations, express trusts, legal professions and non-profit organizations were rated medium to very high. Terrorist financing risk scenarios involving accountants, real estate agents & developers, as well as dealers in precious metals and stones were rated medium to high.

Corporations

As indicated previously, there are inherent vulnerabilities within corporations, particularly private ones, which make them attractive for misuse in order to facilitate money laundering. However, these characteristics can also make them attractive in terrorist financing risk scenarios as fronts to move funds destined for terrorist groups or individuals, or to commingle illicit funds with legitimate business revenue, or to use in trade-based schemes. In addition, in the broader context of terrorist resourcing, the procurement of goods is also considered a form of terrorist financing and would involve various types of corporations. Most terrorist financing actors associated with the terrorist groups listed in Table 2 use businesses in some terrorist financing schemes.

Express Trusts

The inherent vulnerability of express trusts to conceal beneficial ownership information can make them attractive to terrorist financing. Express trusts can be used to facilitate transactions in support of terrorist financing, including flow-through transactions from Canada to abroad, or vice versa.

Legal Professionals and Accountants

Trust accounts, in particular those that are set up by legal professionals, are known to have been used in terrorist financing risk scenarios. There have also been some instances in the past where individuals providing accounting services facilitated fraudulent schemes generating funds to support suspected terrorist financing activities.

Registered Charities and Non-Profit Organizations

An interpretive note to FATF Recommendation 8 states:

> "Some NPOs [non-profit organizations] may be vulnerable to terrorist financing abuse by terrorists for a variety of reasons. NPOs enjoy the public trust, have access to considerable sources of funds, and are often cash-intensive. Furthermore, some NPOs have a global presence that provides a framework for national and international operations and financial transactions, often within or near those areas that are most exposed to terrorist activity. In some cases, terrorist organisations have taken advantage of these and other characteristics to infiltrate some NPOs and misuse funds and operations to cover for, or support, terrorist activity."[146]

As such, in the context of terrorism and terrorist financing in Canada, the registered charities and non-profit organizations operating overseas are most vulnerable, as funds or goods may be abused at the point of distribution by the charity or partner organizations. Charities may also unwittingly support terrorist organizations abroad by paying taxes and tolls to operate in certain areas, when these are directly or indirectly controlled by the terrorist organizations. Organizations that operate domestically, within a population that is actively targeted by terrorist movement for support and cover, are also exposed to terrorist financing risks, as resources generated in Canada may be transferred internationally to support terrorism if the organization does not conduct sufficient due diligence or provide sufficient oversight of donees, or exercise direction and control over the end-use of its resources.

Inherent TF Risk Scenarios Involving Charities and Non-Profit Organizations

The terrorist financing methods used in the majority of terrorist financing risk scenarios involving Canadian and foreign charities and non-profit organizations (referred to collectively as organizations below) can be summarized as the following:

- Diversion of funds: an organization, or an individual acting on behalf of an organization, diverts funds to a known or suspected terrorist entity;
- Infiltration by bad actor: Individual(s) from a terrorist entity or affiliated with a terrorist entity take control of a once legitimate organization (e.g. its board, treasury) to support terrorism.
- Affiliation with terrorist entity: an organization, or individual acting on behalf of an organization, maintains operational affiliation with a terrorist organization or supporter of terrorism, putting the sector at risk of abuse for purposes including general logistical support to the terrorist entity;
- Abuse of programming: organization-funded programs meant to support legitimate humanitarian purposes are manipulated at the point of delivery to support terrorism;
- Support of recruitment: organization-funded programs or facilities are used to create an environment which supports and/or promotes terrorism recruitment-related activities; and
- False representation and sham organizations: under the guise of charitable activity, an organization or individual raises funds, promotes causes and/or carries out other activities in support of terrorism.

The most commonly observed terrorist financing method relates to the abuse of organizations to support terrorism by the diversion of funds. In this method, funds raised by organizations for humanitarian programs (e.g., disaster relief, humanitarian relief, cultural centers, relief of poverty, advancement of education, advancement of religion) are diverted to support terrorism at some point through the organization's business process. Essentially, the diversion of funds occurs when funds raised for charitable purposes are re-directed to a terrorist entity.

[146] FATF Recommendations 2012.pdf.coredownload.inline.pdf (fatf-gafi.org). The Recommendations were last updated February 2023.

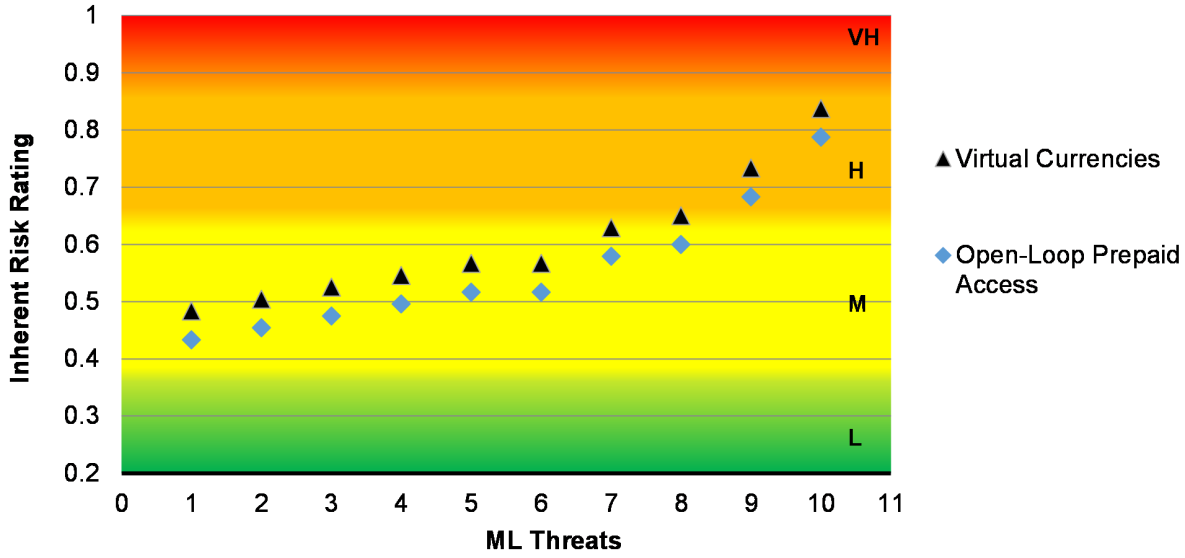
The diversion of funds method can be divided into cases where the diversion was carried out by actors internal to the organization as well as external to the organization. Internal actors are named individuals of the organization, such as directing officials and staff. External actors, however, are merely associated to the organization as third parties, such as fundraisers and foreign partners.

The majority of the terrorist financing actors associated with the terrorist groups listed in Table 2 have used registered charities.

Dealers in Precious Metals and Stones

Terrorist financing actors have purchased precious metals and stones to transfer value without being detected by authorities. Another method to avoid detection is to use precious metals and stones entities as front companies to move funds between different jurisdictions.

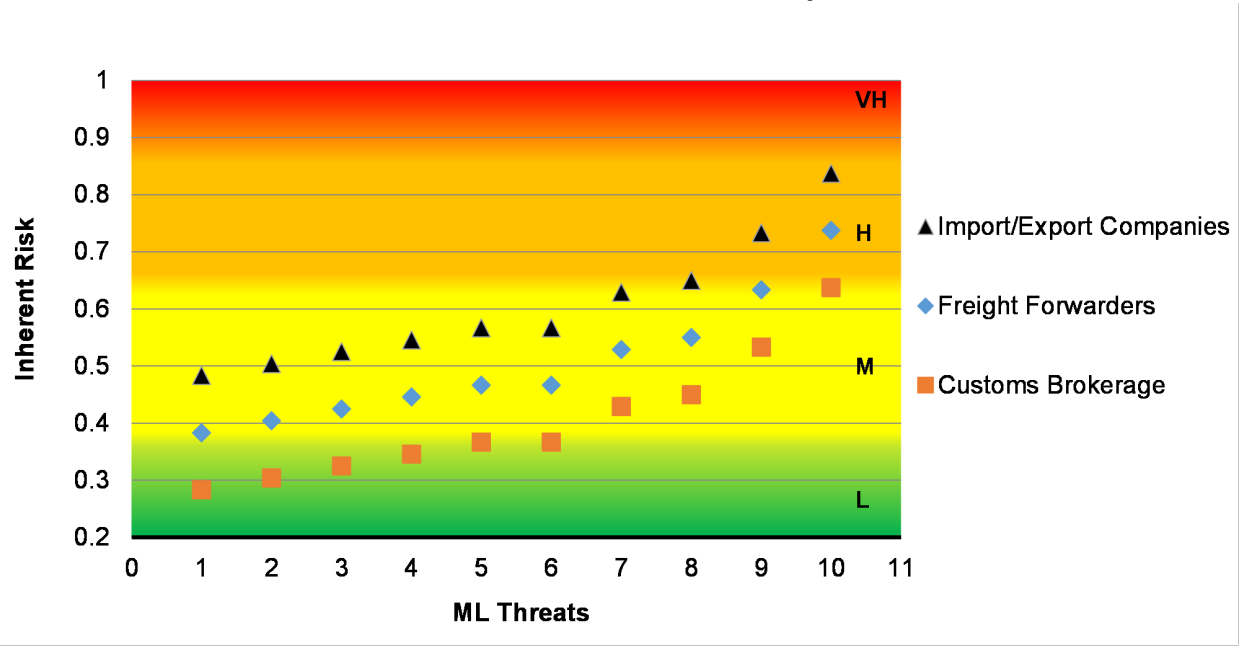
Figure 13
Inherent TF Risks related to Products Holding Monetary Value by TF Threat Actors



Terrorist financing risk scenarios involving virtual currencies and prepaid access products have been rated medium to high, as shown in Figure 13. Some terrorist financing actors have been reported to use Bitcoins as part of their terrorist financing activities and may use other virtual currencies. Virtual currencies are usually used with the objective to enhance anonymity when moving funds, which can make new privacy coins attractive to terrorist financing actors. Although only a few terrorist financing cases in Canada have involved the use of open-loop prepaid access products, other jurisdictions have also reported such use.

Figure 14

Inherent TF Risks related to Entities Involved in International Trade by TF Threat Actors



Terrorist financing risk scenarios involving the trade sectors have been rated from low to high. Vulnerabilities identified in this space are generally similar to those observed for money laundering, with import/export companies being among the main parties involved in moving funds and goods and freight forwarders/custom brokers playing a facilitator role. Import and export companies may be used as front entities to transfer funds to higher risks areas where terrorist organizations operate. They may also be used to move goods across borders to either directly support terrorist activities or use the proceeds generated from the sale of these goods to fund the terrorist organizations.

Evolution of the Risk Landscape in Canada

Since conducting its first National Inherent Risk Assessment in 2015, Canada has continued to broaden and deepen its understanding of the money laundering and terrorist financing risks landscape in Canada.

This update assessed one new money laundering threat not included in the 2015 Report – the threat of illegal and unregulated fishing. While this does not represent an important vector of money laundering in Canada, some level of criminal activities with an element of sophistication were noted, which can generate proceeds that need to be laundered.

Some threats assessed in the 2015 Report have also changed in this update, with some impact on the outcomes of the different risks scenarios. While the threat levels increased for illegal gambling, tax evasion and wildlife trafficking, they decreased for illegal tobacco smuggling and trafficking. This was generally a reflection of changes in the average sophistication and capability exhibited by the threat actors involved. For example, concerns around tax evasion have increased following growing trends around the usage of complex offshore corporate structures and accounts and the leveraging of expertise from facilitators such as accountants, lawyers and financial advisors.

In many cases, threat levels remained constant, but new trends were noted. Criminal actors continue to leverage new technologies and the changing environment such as the COVID-19 situation to design and perpetuate new types of fraud. New Internet scams have been observed, for example around initial coin offerings targeting investors or pandemic-relief programs, and the usage of virtual currencies and prepaid cards to launder proceeds from these activities are increasingly common. Illicit drug trafficking remains one of the main and most important money laundering threats in Canada. Recent years have seen the emergence and considerable growth of the fentanyl market, with one trend being the increasing use of virtual currencies to procure drugs via the dark web.

Although not reporting entities under the AML/ATF Regime: corporations, partnerships, express trusts, armoured car companies, unregulated mortgage lenders, import/export companies, freight forwarders and custom brokers were also assessed as part of this risk update for their inherent vulnerabilities to money laundering and terrorist financing.

The common vulnerability of corporate and legal entities (i.e., trusts) to hide beneficial ownership information remains a significant element of Canada's money laundering and terrorist financing risk landscape. This issue highlights the importance of greater beneficial ownership transparency, a key priority to enhancing the AML/ATF Regime.

Another significant element of the risk landscape relates to Canada's exposure to TBML, as evidenced by the assessment of vulnerable sectors involved in international trade and the threats posed by commercial trade fraud and third-party money launderers, whose money laundering methods include the use of TBML.

This update also illustrates the effects of rapid increases in housing prices in some parts of the country on the risk landscape in Canada. Housing price escalation has made for-profit mortgage fraud more lucrative, and increased the incentive and attractiveness of conducting criminal activities and money laundering in the real estate sector. Increased economic activity in the real estate sector and rapid housing-price growth have created opportunities for criminals to launder funds, both through the purchase of properties and by acting as alternative lenders to unsuspecting borrowers who may have trouble accessing traditional mortgage financing.

Finally, the COVID-19 pandemic has demonstrated the adaptability the Canadian financial sector with more consumers adopting digital channels as well as new financial services and products being made available by emerging technologies. The pandemic has also shown that bad actors, both criminals and terrorist organizations, continue to adapt to changing vulnerabilities, which highlights the importance for national authorities and the private sector to understand evolving risks on an ongoing basis.

Next Steps

This updated risk assessment promotes a greater shared understanding of inherent money laundering and terrorist financing risks in Canada. The assessment will help to continue to enhance Canada's AML/ATF Regime, further strengthening the comprehensive approach it already takes to risk mitigation and control domestically, including with the private sector and with international partners. The Government of Canada will update the inherent risk assessment and publicly share the revised results on an ongoing basis.

The Government of Canada expects that this report will also be used by financial institutions and other reporting entities to contribute to their understanding of how and where they may be most vulnerable and exposed to inherent money laundering and terrorist financing risks. FINTRAC will continue to include relevant information related to inherent risks in their guidance documentation to assist financial institutions and other reporting entities in integrating such information in their own risk assessment methodology and processes so that they can effectively implement controls to mitigate money laundering and terrorist financing risks. Members responsible for the oversight of the Regime will also use the valuable lessons learned from this exercise to set priorities for policy development and operational efforts in our ongoing efforts to combat money laundering and terrorist financing.

Annex: Key Consequences of Money Laundering and Terrorist Financing

Societal Consequences

- Increased criminal activity
- Increased social and economic power to criminals
- Increased victimization, from emotional trauma to physical violence
- Increased rates of incarceration
- Reduced confidence in private and public sector institutions

Economic Consequences

- Increased economic distortions (consumption, saving, and investment) that affect economic growth
- Reduced domestic and international investment
- Higher illicit capital inflows and higher legitimate capital outflows
- Unfair private sector competition
- Distorted market prices
- Increased bank liquidity and solvency issues, which may affect the integrity of the financial system
- Reputational damage relating to the economy and the sectors at issue (particularly the financial sector)

Political Consequences

- Eroding of public institutions and the rule of law
- Greater perceived attractiveness for illicit money laundering and terrorist financing activities (“safe haven”)
- Loss of credibility and influence internationally
- Lower government revenues
- Negative public perception in the government’s ability to deal with money laundering and terrorist financing activity (weak on crime)

Glossary

Alternative remittance MSBs: money services businesses that involve the use of alternative remittance services taking place outside of the conventional banking system (although they may interconnect with it). There are four sub-segments of alternative remittance MSBs: virtual currency/block-chain exchanges and transfers, peer to peer mobile solutions, payment processing e-wallet tech, and non-traditional value transfer systems.

Beneficial owner: the natural person who ultimately owns or controls a corporate or legal arrangement and/or the natural person on whose behalf a transaction is being conducted. It also includes persons who exercise ultimate effective control over a legal person or arrangement.

Closed-loop pre-paid access: prepaid access to funds or the value of funds that can be used only for goods and services in transactions involved a defined merchant or location (or set of locations). The definition includes gift cards that provide access to a specific retailer, affiliated retailers, or retail chain, or alternatively, a designated locale, such as a public transit system.

Criminalized professionals (or White Collar Criminals): Are individuals who holds or purports to hold a professional designation and title in an area dealing with financial matters who uses their professional knowledge and expertise to commit or wittingly facilitate in a profit-oriented criminal activity. Criminal professionals would include lawyers, accountants, notaries, investment and financial advisors, stock brokers, and mortgage brokers.

Domestic banks: Canadian banks that are authorized under the Bank Act to accept deposits, which may be eligible for deposit insurance provided by the Canadian Deposit Insurance Corporation.

*Express trusts (legal arrangements): l*egal arrangements refer to express trusts where the settlor intentionally places assets under the control of a trustee for the benefit of a beneficiary or for a specified purpose. There are two general types of express trusts: (1) testamentary trusts that are created on the day the settlor passes away, in order to transfer the settlor's estate to beneficiaries; and (2) inter vivos trusts that are created during the lifetime of the settlor in order. In the context of money laundering and terrorist financing, the express inter vivos trust is the most relevant.

Factoring company: factoring is a form of asset-based financing whereby credit is extended to a borrowing company on the value of their accounts receivable (the latter are sold at a discount price in exchange for money upfront). The factoring company then receives amounts owing directly from customers of the borrower (the debtor). Factoring companies are primarily used to raise capital in the short-term.

Foreign bank branches: foreign institutions that have been authorized under the Bank Act to establish branches to carry on banking business in Canada.

Foreign bank subsidiaries: foreign institutions that have been authorized under the Bank Act to accept deposits. Foreign bank subsidiaries are controlled by eligible foreign institutions.

Foreign fighters: individuals who travel abroad to fight with and show allegiance to a terrorist group. They operate in countries which are not their own and their principal motivation is ideological rather than material reward.

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

Inherent money laundering and terrorist financing risk: the risk that is present in the absent of any controls to mitigate those risks.

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

Internet-based MSBs: these businesses offer money services and related products online, primarily payment and money transfer services. The number of such entities is smaller in comparison to the other groups, but it is a growing segment of the MSB business.

Money laundering and terrorist financing threats: a person or group of people that have the intention, or may be used as facilitators, to launder proceeds of crime or to fund terrorism.

Organized criminal group: a structured group of three or more persons acting in concert with the aim of committing criminal activities, in order to obtain, directly or indirectly, a financial or other material benefit.

Life insurance companies: foreign and domestic entities that have been authorized to conduct life insurance business in Canada.

Life insurance intermediary entities and agencies: entities that provide administrative support to insurance advisors and allow for the pooling of commissions and access to insurance company products.

Independent life insurance agents and brokers: individuals who are licensed to sell life insurance products. Some agents and brokers deal directly with some insurance companies, while others work through to intermediary entities and agencies to access insurance products.

Money mules: individuals who facilitate fraud and money schemes, often unknowingly (e.g., moving money through international electronic funds transfers on behalf of criminals). They tend to exhibit very low levels of sophistication and capability and are essentially directed to undertake certain actions to launder the funds.

National full-service MSBs: the largest and most sophisticated MSBs that have a national presence, offering a full range of products and services at the retail and wholesale levels.

Nominees: individuals with ties to the threat actors who may be used periodically by criminals to assist in money laundering. Nominees are essentially directed by the criminals on how to launder the funds. The methods used tend to be basic and can be used to launder smaller amounts of proceeds of crime.

Small independent MSBs: operate through informal networks, although a few may have formal banking arrangements in order to conduct electronic funds transfers; these are small, predominantly family-owned operations, whose technical capabilities tend to involve smaller, stand-alone systems.

Smaller retail MSBs: the business is focused on retail transactions, having stand-alone computer systems and street-level retail outlets across Canada. Of these, one sub-group offers currency exchanges only, typically in small values, and are often found in border towns (e.g., duty free shops) and the other sub-group offers currency exchanges, but may also offer money orders and EFTs, typically as an agent of a national full-service MSB.

Smurfing: a money laundering technique involving the use of nominees (i.e., multiple individuals) to conduct structuring activity sometimes at the same time or within a very short period of time.

Structuring: the act of making cash deposits and/or purchasing monetary instruments under authorized thresholds to avoid reporting requirements at banks and MSBs.

Transnational organized crime: an organized crime group that operates transnationally for the purpose of obtaining a financial or other material benefit wholly or in part by illegal means, while protecting their activities through a pattern of corruption and/or violence, or while protecting their illegal activities through a transnational organizational structure and the exploitation of transnational commerce or communication mechanisms.

Wholesale and corporate MSBs: provide money services and related products, predominantly EFTs and bank drafts, primarily to corporations, on a wholesale basis.

List of Key Acronyms and Abbreviations

Acronyms	**Abbreviations**
ACMLTF	Advisory Committee on Money Laundering and Terrorist Financing
AML/ATF	Anti-Money Laundering and Anti-Terrorist Financing
CRA	Canada Revenue Agency
CSIS	Canadian Security Intelligence Service
CSP/TSP/TCSP	Company Services Provider/Trust Services Provider/Trust and Company Services Provider
DPMS	Dealers in Precious Metals and Stones
D-SIB	Domestic Systemically Important Bank
EFT(R)	Electronic Funds Transfer (Report)
FATF	Financial Action Task Force
FINTRAC	Financial Transactions and Reports Analysis Centre of Canada
FMSB	Foreign Money Service Business
GAC	Global Affairs Canada
GDP	Gross Domestic Product
IMVE	Ideologically Motivated Violent Extremists
ISED	Innovation, Science and Economic Development Canada
IVTS	Informal Value Transfer Systems
ML/TF	Money Laundering and Terrorist Financing
MMF	Mass Marketing Fraud
MSB	Money Services Business
RE	Reporting Entity
RCMP	Royal Canadian Mounted Police (RCMP)
PPSC	Public Prosecution Service of Canada
OCG	Organized Crime Group
OSFI	Office of the Superintendent of Financial Institutions
PCMLTFA	*Proceeds of Crime (Money Laundering) and Terrorist Financing Act*
PEP	Politically-Exposed Person
POC	Proceeds of Crime
PSPC	Public Services and Procurement Canada
TBML	Trade-Based Money Laundering
Terrorist Groups	
AQ	Al Qaeda
AQAP	Al Qaeda in the Arabian Peninsula
AQIM	Al Qaeda in the Islamic Maghreb
AS	Al Shabaab
Hamas	Harakat al-Muqawama al-Islamiyya
ISIL	Islamic State in Iraq and the Levant (also known as Daesh)
JN	Jabhat Al-Nusra