ASSESSMENT OF INHERENT RISKS OF MONEY LAUNDERING AND TERRORIST FINANCING IN CANADA

2015

Department of Finance Canada
Ministère des Finances Canada

Canada

Table of Contents

Foreword by the Minister of Finance

Our Government is deeply committed to keeping Canadians safe and our country secure and prosperous.

That is why we are committed to helping ensure the safety and security of all Canadians by giving law enforcement and security agencies the tools they need to protect Canadians from the ever-evolving threat of terrorism and organized crime.

To this end, in Economic Action Plan 2015, our Government provided additional investigative resources to our law enforcement and national security agencies to allow them to keep pace with the evolving threat of organized crime and terrorism, including addressing the issues of terrorist financing and money laundering.

Canada's existing anti-money laundering and anti-terrorist financing regime is strong and comprehensive, comprising 11 federal departments and agencies, eight of which are receiving dedicated funding of approximately $70 million annually.

It's a regime that is constantly adapting in both scope and ability, as it must in an uncertain world, subjected to the highest standards of scrutiny and review both domestically and by international peers. It balances the need for public safety with preserving the core principles of the civil liberties that make Canada a beacon of liberal democracy.

It supports the work of law enforcement and intelligence agencies, and is a key part of Canada's efforts to counter terrorism and transnational organized crime.

And it extends to the approximately 31,000 reporting entities—from money services businesses and casinos right up to life insurance companies and banks.

However, we know that we are now on the front lines of a real, urgent and dangerous conflict.

That is why we continue to work through the Financial Action Task Force (FATF)—a body Canada helped create nearly 30 years ago that sets standards and promotes effective implementation of legal, regulatory and operational measures for combating money laundering and terrorist financing, to develop common international standards that help us stay ahead of criminals on a global scale while making our own regime even stronger.

In the fight to counter terrorist financing and money laundering, we can only secure our nation's security and the integrity of our financial system by taking the fight beyond our borders, and we are only as strong as our weakest link. Our leadership on the international stage reflects our commitment to strengthen that global chain.

And we continue to strengthen our own link within it.

That is why the Department of Finance, consistent with international standards outlined by the FATF, has led a whole-of-government initiative to develop the *Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada* report to better identify, assess and understand inherent money laundering and terrorist financing risks in Canada on an ongoing basis.

This work is an important initial assessment of our existing risk framework that helps us to better understand and identify money laundering and terrorist financing activities in Canada.

This work will be a valuable tool for our regime partners, for reporting entities, and for all Canadians who want to equip themselves with a greater awareness of trends and challenges.

It will inform ongoing and future action at a policy level, and provide critical risk information to industry so that we can effectively tackle the challenges we face together in protecting Canadians and our country.

We know that working with regime partners, reporting entities and the private sector more broadly is essential to maintaining the strength of the regime.

And we know that our partners need the benefit of our insights to undertake their own risk analysis, and introduce the operational changes required to make a strong system even stronger.

Canadians expect our Government to take these terrorist threats very seriously. We will not allow terrorism to undermine our way of life or that of others around the world. Canadians reject the use of terrorist violence, no matter where it takes place.

And that is why we will continue to remain vigilant in our battle against money laundering and terrorist financing to protect our communities, and the lives of Canadians.

The Honourable Joe Oliver, P.C., M.P.
Minister of Finance
Ottawa, July 2015

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 has conducted an assessment to identify inherent money laundering and terrorist financing (ML/TF) risks in Canada. This report also includes a process to update this assessment over time. The 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.

Canada has a comprehensive AML/ATF regime that provides a coordinated approach to mitigating the inherent risks identified in this assessment and combating money laundering and terrorist financing more broadly. The AML/ATF regime is operated by 11 federal regime partners, eight of which receive dedicated funding totalling approximately $70 million annually.[1] 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, prosecution and the seizure of illicit assets; and the implementation of measures to ensure the ongoing improvement of the AML/ATF regime.

This report is meant to provide critical risk information to the public and, in particular, to the approximately 31,000 entities that have reporting obligations under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA), whose understanding of inherent, foundational risks is vital in applying the preventive measures and controls required to effectively mitigate these risks. The Government of Canada encourages these entities to use the findings in this report to inform their efforts in assessing and mitigating risks. Understanding Canada's risk context and the main characteristics that expose sectors and products to inherent ML/TF risks in Canada is important in being able to apply measures to effectively mitigate them.

This report also responds to the revised Financial Action Task Force's (FATF) global AML/ATF standards calling on all members to undergo an assessment of ML/TF risks. This report will be considered as part of the upcoming FATF Mutual Evaluation of Canada, which will assess Canada against these global standards.

The inherent risk assessment consists of an assessment of the ML/TF threats and inherent ML/TF vulnerabilities of Canada as a whole (e.g., economy, geography, demographics) and its key economic sectors and financial products, while taking into account the consequences of money laundering and terrorist financing. The overall inherent ML/TF risks were assessed by matching the threats with the inherently vulnerable sectors and products through the ML/TF 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 ML/TF risks.

[1] The eight funded partners are the Canada Border Services Agency, the Canada Revenue Agency, the Canadian Security Intelligence Service, the Department of Finance Canada, the Department of Justice Canada, the Financial Transactions and Reports Analysis Centre of Canada, the Public Prosecution Service of Canada and the Royal Canadian Mounted Police. Foreign Affairs, Trade and Development Canada, Industry Canada, the Office of the Superintendent of Financial Institutions, Public Safety Canada and Public Works and Government Services Canada make important contributions to the regime.

The ML threat assessment examined 21 criminal activities in Canada that are most associated with generating proceeds of crime that may be laundered. It also examined the ML threat emanating from third-party money laundering, which includes money mules, nominees and professional money launderers. The ML threat was rated very high for corruption and bribery, counterfeiting and piracy, certain types of fraud, illicit drug trafficking, illicit tobacco smuggling and trafficking, and third-party money laundering. Transnational organized crime groups (OCGs) and professional money launderers are the key ML threat actors in the Canadian context. Many of these threats are similar to those faced by several other developed and developing countries.

The TF threat was assessed for the groups and actors 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 abroad to various terrorist groups. Despite these activities, the TF threat in Canada is not as pronounced as in other regions of the world, where weaker ATF regimes can be found and where terrorist groups have established a foothold, both in terms of operations and financing their activities.

The inherent ML/TF vulnerabilities are presented for 27 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 for-profit corporations), certain types of money services businesses and express trusts were rated the most vulnerable, or very high. The vulnerability was rated high for 16 sectors and products, medium for five sectors and products and low for one sector. Many of the sectors and products are highly accessible to individuals in Canada and internationally and are associated with a high volume, velocity 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 ML/TF 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 ML risks involving threat actors (e.g., OCGs and third-party money launderers) laundering illicit proceeds generated from 10 main types of profit-oriented crimes. The assessment also identified five very high inherent TF risk scenarios that involve five different sectors that have been assessed to be very highly vulnerable to terrorist financing, combined with one high TF threat group of actors.

This risk assessment is an analysis of Canada's current situation and represents a key step forward in providing the basis for the AML/ATF regime to promote a greater shared understanding of inherent ML/TF risks in Canada on an ongoing basis. 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.

Introduction

Money laundering and terrorist financing (ML/TF) compromise the integrity of the 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 OCGs. 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 *Canadian Charter of Rights and Freedoms* and the privacy rights of Canadians. 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 11 federal departments and agencies, each responsible for certain elements of it, as well as other departments and agencies that support the regime's efforts, coordinated by the Department of Finance Canada.[2] 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 almost 31,000 Canadian financial institutions and designated non-financial businesses and professions (DNFBPs)[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.

The regime's understanding of ML/TF risks plays a key role in its ability to effectively combat these illicit activities. That understanding helps to support the policy-making process to more 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 applies its risk-based approaches and mitigates its risks. Overall, the regime's understanding of risks helps to ensure that it is focused on adequately mitigating the risks of greatest concern to Canada.

[2] The 11 federal AML/ATF regime partners are: the Canada Border Services Agency, the Canada Revenue Agency, the Canadian Security Intelligence Service, the Department of Finance Canada, the Financial Transactions and Reports Analysis Centre of Canada, Foreign Affairs, Trade and Development Canada, the Department of Justice Canada, the Office of the Superintendent of Financial Institutions, the Public Prosecution Service of Canada, Public Safety Canada and the Royal Canadian Mounted Police. Industry Canada and Public Works and Government Services Canada also support the work of the regime.

[3] Financial Transactions and Reports Analysis Centre of Canada. *Results Through Financial Intelligence*. Annual Report 2013. Ottawa, 2013.

Given the central role that the understanding of risk plays in the regime, the Government of Canada has built on existing practices to develop a more comprehensive assessment to identify and assess ML/TF risks in Canada.[4] This assessment consists of a foundational risk assessment and a process to periodically update the results. This report presents the results of the assessment of inherent ML/TF risks in Canada. These are the fundamental risks in Canada, which the AML/ATF regime seeks to control and mitigate. The 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 main characteristics that expose these sectors and products to ML/TF risks in Canada. Properly understanding these inherent risks is critical in being able to identify and apply measures to effectively mitigate them. In this regard, the Government expects that this report will be used by financial institutions and other reporting entities to better understand how and where they may be most vulnerable and exposed to inherent ML/TF risks and to ensure that these risks are being effectively mitigated. It will also be used by policy makers and operational agencies to set priorities and assess the effectiveness of measures to address ML/TF risks.

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

The content of the report reflects what was available and deemed pertinent up to December 31, 2014, and it excludes some information, intelligence and analysis for reasons of national security.

[4] In addition to the 11 federal regime partners, the Bank of Canada, Defence Research and Development Canada (an agency of the Department of National Defence), Environment Canada, Industry Canada, the Ontario Provincial Police and the Sûreté du Québec contributed to the risk assessment.

Chapter 1: Risk Mitigation

Canada has a comprehensive AML/ATF regime that provides a coordinated approach to mitigating the inherent ML/TF risks identified in this assessment and combating money laundering and terrorist financing more broadly. This chapter briefly reviews 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.

The AML/ATF regime is operated by 11 federal regime partners, eight of which receive dedicated funding totalling approximately $70 million annually. The eight funded partners are the Canada Border Services Agency (CBSA), the Canada Revenue Agency (CRA), the Canadian Security Intelligence Service (CSIS), the Department of Finance Canada, the Department of Justice Canada, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), the Public Prosecution Service of Canada (PPSC) and the Royal Canadian Mounted Police (RCMP). Although not receiving dedicated funding, Foreign Affairs, Trade and Development Canada (DFATD), the Office of the Superintendent of Financial Institutions (OSFI) and Public Safety Canada make important contributions to the regime.

The regime is also supported by other federal departments, such as Industry Canada and Public Works and Government Services Canada (PWGSC), as well as provincial financial sector and other regulators and provincial and municipal law enforcement agencies. Within the private sector, there are almost 31,000 Canadian financial institutions and DNFBPs with reporting obligations under the PCMLTFA playing a critical frontline role in efforts to combat money laundering and terrorist financing.

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

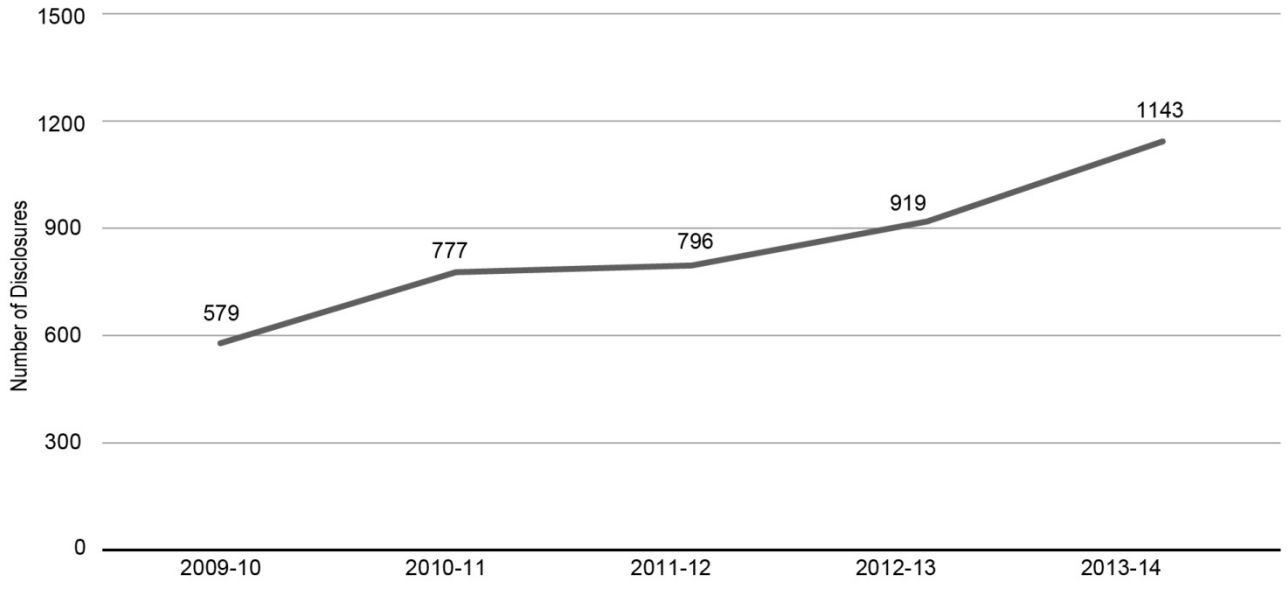
The first pillar consists of the regime's policy and legislative framework as well as its domestic and international coordination, which is led by the Department of Finance Canada. The PCMLTFA is the legislation that establishes Canada's AML/ATF framework, supported by other key statutes, including the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

The PCMLTFA requires prescribed financial institutions and DNFBPs, known as reporting entities, to identify their clients, keep records and establish and administer an internal AML/ATF compliance program. The PCMLTFA creates a mandatory reporting system for suspicious financial transactions, large cross-border currency transfers and other prescribed transactions. It also creates obligations for the reporting entities to identify ML/TF 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 disseminated to regime partners and the general public. The information disseminated under the PCMLTFA can be intelligence used to support domestic and international partners in the investigation and prosecution of ML/TF related offences. The information can also be in the form of trend and typology reports used to educate the public, including the reporting entities, on ML/TF issues.

Chart 1 below provides the annual number of cases disclosed by FINTRAC to regime partners from 2009–10 to 2013–14. For example, in 2013–14, FINTRAC made 1,143 disclosures to regime partners. Of these, 845 were associated with money laundering, while 234 dealt with cases of terrorist activity financing and other threats to the security of Canada. Sixty-four disclosures dealt with all three areas.

Chart 1
FINTRAC Case Disclosures from 2009–10 to 2013–14[5]



Given the number of regime participants and the complexity of the issues, the effective regime-wide coordination of strategic, policy and operational matters is important. 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, including through formal mutual legal assistance led by the Department of Justice Canada.

[5] Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). *Deter and Detect Money Laundering and Terrorist Financing*. FINTRAC Annual Report 2014. Ottawa, 2014.

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 Financial Action Task Force (FATF), the G-7, the G-20, the Egmont Group of Financial Intelligence Units and, most recently, the counter-financing work stream of the Anti-Islamic State of Iraq and the Levant (ISIL) Coalition.[6]

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 36 FATF members and the more than 180 countries in the global FATF network through peer reviews and public reporting. The FATF also leads international efforts related to policy development and risk analysis, and identifies and reports on emerging ML/TF trends and methods. This work helps to ensure that countries have the appropriate tools in place to address ML/TF risks. Canada also provides expertise and funding to increase AML/ATF capacity in countries with weaker regimes, including through the Counter-Terrorism Capacity Building Program and the Anti-Crime Capacity Building Program, which are led by DFATD.

(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, specifically the financial institutions and DNFBPs, that are the gatekeepers of the financial system in implementing the various measures under the PCMLTFA, and the regulators, principally FINTRAC and OSFI, which supervise them.

The transparency of corporations and trusts contributes to preventing and detecting money laundering and terrorist financing, including the requirements for financial institutions to identify the beneficial owners of the corporations and trusts with whom they do business. Provincial and federal corporate laws and registries and securities regulation also contribute to preventing and detecting money laundering and terrorist financing in Canada.

(iii) Disruption

The final pillar deals with the disruption of money laundering and terrorist financing. Regime partners, such as CSIS, the CBSA and the RCMP, supported by FINTRAC's intelligence gathering and analysis activities, undertake financial investigations in relation to money laundering, terrorist financing and other profit-oriented crimes. The CRA also plays an important role in investigating tax evasion and its associated money laundering, and in detecting charities that are at risk and ensuring that they are not being abused to finance terrorism. The PPSC ensures that crimes are prosecuted 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. PWGSC manages all seized and restrained property for criminal cases prosecuted by the Government of Canada. The CBSA enforces the Cross-Border Currency Reporting Program, and transmits information from reports and seizures to FINTRAC.

[6] The Anti-ISIL (ISIS) Coalition consists of 60 countries that are working together to counter the threat of ISIS, including its financing.

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 DFATD, respectively. Canada currently has 90 terrorist-related listings under this process.[7]

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 and is in keeping with its legislative mandate, while respecting the Constitutional division of powers, the *Canadian Charter of Rights and Freedoms* and the privacy rights of Canadians.

The Parliament of Canada undertakes a comprehensive review of the PCMLTFA every five years and the Office of the Privacy Commissioner of Canada is required to conduct a privacy audit of FINTRAC every two years. Among other periodic reports,[8] reviews and audits, the regime's performance is statutorily mandated to be reviewed every five 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.

The Government announced a series of measures to enhance the AML/ATF regime in its 2014 *Economic Action Plan* (the budget), which received Royal Assent in June 2014. These legislative and regulatory changes will strengthen customer due diligence requirements, improve compliance, monitoring and enforcement, strengthen information sharing and disclosure, and authorize the Minister of Finance to issue countermeasures against jurisdictions and foreign entities that have weak ML/TF controls. To strengthen Canada's targeted financial sanctions regime, enhancements will also be made to reduce the burden imposed on the private sector to implement financial sanctions.

Canada is 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 is committed to take appropriate action to mitigate the ML/TF risks identified in this assessment and to continue to assess 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 ML/TF risks. FINTRAC and OSFI will include relevant information related to inherent risks in their respective 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 ML/TF risks. Members of the oversight of the regime will also use the results of the risk assessment to inform policy and operations as part of the ongoing efforts to combat money laundering and terrorist financing.

---

[7] As of December 31, 2014.

[8] See, for example, the Department of Finance Canada's 2014–15 *Report on Plans and Priorities*, which explains the AML/ATF regime's spending plans, priorities and expected results, available at http://www.fin.gc.ca/pub/rpp/2014-2015/st-ts-04-eng.asp#st4, as well as its *Departmental Performance Report*, available for 2013–14, at http://www.fin.gc.ca/pub/rpp/2014-2015/st-ts-04-eng.asp#st4.

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

Overview

The Government of Canada has developed an assessment to identify and understand inherent ML/TF 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. The assessment provides the basis to think critically and systematically about ML/TF risks on an ongoing basis, and to promote a common understanding of these risks. This chapter provides an overview of the risk assessment methodology.

Scope of the Methodology

The methodology assesses the inherent ML/TF 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 main characteristics that expose sectors and products to inherent ML/TF risks in Canada is important in 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 threat actors exploiting inherent vulnerabilities to launder illicit proceeds or fund terrorism and the consequences should this occur.

Key Definitions

ML/TF threat: a person or group who has the intention, or may be used as a witting or unwitting facilitator, to launder proceeds of crime or to fund terrorism.

Inherent ML/TF 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 ML/TF: the negative impact that money laundering and terrorist financing has on a society, economy and government.

Likelihood of ML/TF: the likelihood of ML/TF threat actors exploiting inherent vulnerabilities.

The ML threat was assessed separately from the TF threat. Although there is some overlap, the nature of these criminal activities is different, warranting separate assessments. In contrast, the assessment of the ML/TF vulnerabilities did not require such separation since ML/TF 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 ML/TF threats and inherent vulnerabilities were identified and categorized. For these categories, criteria were developed to rate the extent of the ML/TF threats and the inherent ML/TF vulnerabilities. These ratings were then used to assess the likelihood of money laundering and terrorist financing, 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 ML/TF 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

During a series of workshops, experts from Canada's AML/ATF regime used their expertise and knowledge to assess the ML/TF 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 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 ML threat in Canada was assessed for 21 criminal activities that are most associated with generating proceeds of crime in Canada as well as the threat from third-party money laundering. The ML threat was rated for each criminal activity against four rating criteria: the extent of the threat actors' knowledge, skills and expertise 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 ML activity; and the magnitude of the proceeds of crime being generated annually from the criminal activity. The ML threat rating results are presented in Chapter 3.

The TF threat in Canada was assessed for 10 terrorist groups as well as for foreign fighters, defined as those who travel abroad to support and fight alongside terrorist groups. The TF threat of these groups was assessed against six rating criteria: the extent of the threat actors' knowledge, skills and expertise to conduct terrorist financing; the extent of the threat actors' network, resources and overall capability to perform TF operations; the scope and global reach of their TF 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 TF 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 ML/TF vulnerabilities were assessed for 27 economic sectors and products. The areas were assessed against five rating criteria: 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.

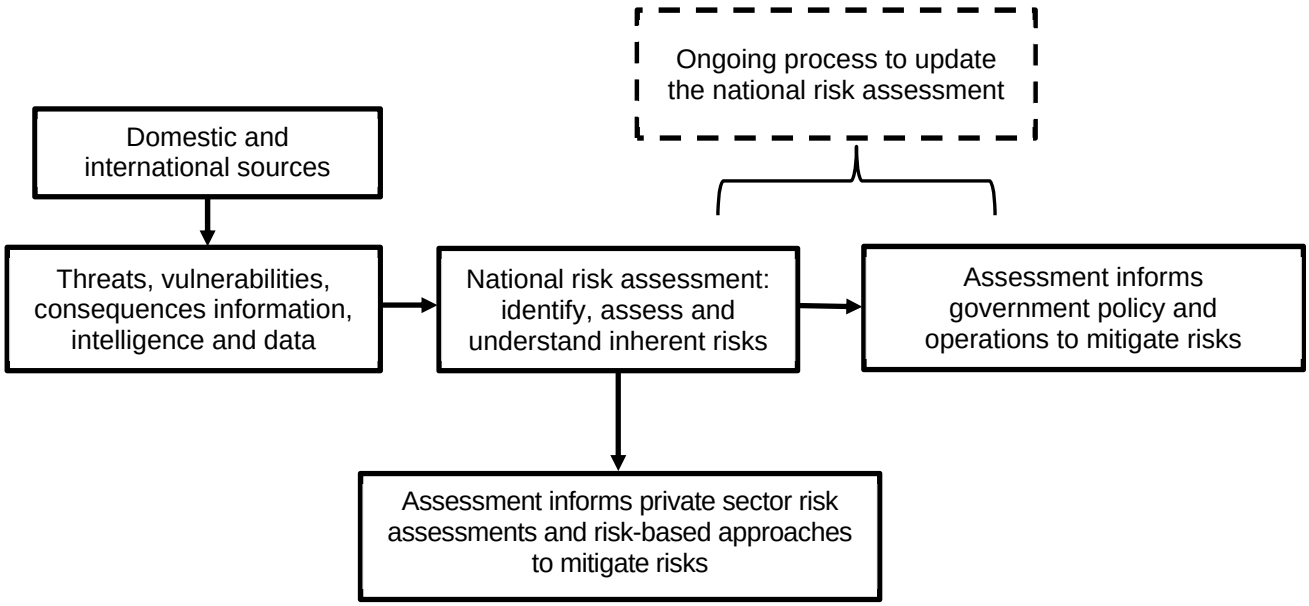
Assessing the Inherent ML/TF Risks

The inherent ML/TF 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 ML/TF threats with the inherently vulnerable sectors and products through the ML/TF methods and techniques that are used by threat actors to exploit these sectors and products. Inherent ML/TF 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 ML/TF risks in Canada.[9] 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 ML/TF risks in Canada. This framework is summarized below in Chart 2.

Chart 2
Canada's ML/TF Risk Assessment Framework



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

Chapter 3: Assessment of Money Laundering Threats

Overview

The ML 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[10] and organized crime groups (OCGs).[11] According to the Criminal Intelligence Service Canada, there are over 650 OCGs operating in Canada. Of these threat actors, transnational OCGs are the most threatening both in terms of generating the most proceeds of crime and in the intensity of efforts to launder the proceeds. The most powerful transnational OCGs in Canada, consisting of factions with ties to Italy and Asia, and 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 domestically and internationally (e.g., Mexican and Columbian drug cartels).

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 ML 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 ML threat in Canada. In addition to professional money launderers, unwitting and witting facilitators appear 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.

[10] 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, accountants, notaries, investment and financial advisors, stock brokers and mortgage brokers.

[11] The majority of OCGs operate and concentrate their activities in the British Columbia lower mainland, Southern Ontario and the greater Montreal region, or, more specifically within these regions, in Canada's three largest cities: Vancouver, Toronto and Montreal.

The conduct of larger-scale profit-oriented crime often has a significant international dimension and tends 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 the 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 to facilitate the movement of illicit goods and proceeds into and out of Canada. These threat actors 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 ML threat for 21 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, DNFBPs 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 ML threat, eight were rated high, four were rated medium and one was rated low.

Table 1
Overall Money Laundering Threat Rating Results

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

Very High Money Laundering Threats

ML Threat from Capital Markets Fraud: Securities fraud, including investment misrepresentation and other forms of capital markets fraud-related misconduct, such as illegal insider trading and market manipulation, occurs in Canada. Over one-quarter of Canadians believe that they have been approached with a possible fraudulent investment opportunity.[12] 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. For instance, in 2009, two Canadians were arrested and charged with fraud, theft and money laundering for orchestrating a Ponzi-style investment fraud that resulted in defrauding about 2,000 investors of between $100 million and $200 million. 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 perpetrate the fraud. Alongside the sophisticated fraudulent schemes, there are sophisticated ML schemes designed to integrate and legitimize the fraud-related proceeds into the financial system. ML 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[13] and nominees[14].

ML Threat from Commercial (Trade) Fraud: The transnational OCGs and the terrorist actors and networks that generate the most illicit proceeds from commercial fraud are very sophisticated and capable, with the knowledge, expertise and international relationships to manipulate multiple trade chains and trade financing vehicles, often operating under the cover of front and/or legitimate companies. The sophistication and capability in terms of conducting the commercial fraud also extends to laundering its proceeds. The threat actors in this space appear to use multiple sectors in Canada and internationally to launder the proceeds. Actors are also suspected to use 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. In one Canadian case, border agents detected a scheme that appeared to involve trade fraud and trade-based money laundering. Under this scheme, a criminal organization allegedly manipulated shipping documents and engaged in fraudulent transactions to overbill (invoice) a colluding foreign importer for a commodity. Once imported, the foreign importer would pay the exporter the inflated amount, consisting of the legitimate proceeds from the sale of the commodity and illicit proceeds.

---

[12] Canadian Securities Administrators (CSA). *2012 CSA Investor Index*. October 16, 2012.

[13] 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.

[14] 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.

ML Threat from Corruption 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. The ML threat from corruption and bribery is rated very high principally due to the size of the public procurement sector and the opportunities that this presents to illegally obtain high-value contracts. In addition to corrupt activities carried out domestically, some Canadian companies have also been implicated in the paying of bribes to foreign officials to advance their company's business interests. OCGs that have the ability to infiltrate the public procurement process have the sophistication and capability to launder large amounts of illicit funds, using a variety of ML sectors and methods, including banks, money services businesses (MSBs), high-end goods, investments and front companies. Lawyers, accountants, professional money launderers and public officials may also be used to facilitate the laundering of corruption-related proceeds.

ML Threat from Counterfeiting and Piracy: The prevalence of counterfeit and pirated products in Canada has grown significantly over the past decade, in terms of both the amount and the selection of products available for sale. China is the primary source of counterfeit products imported into Canada. Toronto, Montreal and Vancouver are the key entry points for these products. OCGs appear to have established links and have tapped into global illicit distribution channels, allowing them to bring increasingly more counterfeit products into Canada. Given the sophistication and capability needed for counterfeiting operations, actors involved in these operations appear to be highly sophisticated and capable in terms of laundering the proceeds from counterfeit goods. Having the sophistication and capability to transfer funds in a clandestine way domestically and internationally would appear to be fundamental to the sustainability of the operations given the large numbers of individuals that expect payment throughout the supply chain. All indications suggest that the counterfeit and pirated goods market is substantial and continues to grow rapidly in Canada.

ML Threat from Illicit Drug Trafficking: The illicit drug market is the largest criminal market in Canada, with cannabis, cocaine, amphetamine-type stimulants and heroin comprising a significant share of this market. Although numerous threat actors engage in drug trafficking, transnational OCGs are the most threatening and are the most powerful actor in this market. Transnational OCGs exhibit a very high level of sophistication, capability and scope in their ML 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 also have access to professional money launderers and facilitators (such as money mules[15] and nominees), and often have control over a number of companies (front and/or legitimate) as part of their ML operations. OCGs use a large number of ML methods, including the use of multiple sectors, commingling of illicit funds within legitimate businesses, domestic and foreign front and shell companies, bulk cash smuggling, trade-based money laundering, virtual currencies and prepaid cards.

[15] Money mules are those who facilitate fraud and ML schemes, often unknowingly (e.g., moving money through international EFTs 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.

ML Threat from Mass Marketing Fraud (MMF): MMF is very prevalent in Canada and the scams associated with MMF have been growing in frequency and sophistication over time. Toronto, Montreal, Vancouver, Calgary and Edmonton are considered to be main bases of operation for MMF schemes. Common types of scams in Canada include service scams, prize scams and extortion scams. In March 2014, law enforcement arrested 23 individuals in Montreal in connection with allegedly orchestrating a telemarketing scheme. The scheme defrauded thousands of victims, mostly senior citizens, of at least $16 million. The majority of MMF connected to Canada is carried out by OCGs, which use a range of ML methods and sectors, including smurfing, structuring, the use of nominees and money mules, shell companies, MSBs, the informal banking system and front companies. Although reported losses averaged about $60 million annually from 2009 to 2013 and totalled $73 million in 2014,[16] 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.

ML Threat from Mortgage Fraud: Mortgage fraud occurs across Canada, but it is most prevalent in large urban areas in Quebec, Ontario, Alberta and British Columbia. Mortgage fraud schemes are often undertaken to facilitate another criminal activity (e.g., illicit drug production and distribution, money laundering) or directly for profit. OCGs conduct the vast majority of mortgage fraud in Canada. To carry out this crime, OCGs are believed to rely on the assistance of witting or unwitting professionals in the real estate sector, including agents, brokers, appraisers and lawyers. OCGs frequently use straw buyers to orchestrate the mortgage fraud. OCGs conducting mortgage fraud schemes are, for the most part, suspected to be highly sophisticated and capable in terms of the associated ML activity. Professional money launderers have been used to launder mortgage fraud-related proceeds. It is suspected that criminally inclined real estate professionals, notably real estate lawyers, are used to facilitate money laundering. OCGs involved in mortgage fraud 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 Money Laundering: Large-scale and sophisticated ML operations in Canada, notably those connected to transnational OCGs, frequently involve third-party money launderers, namely professional money launderers, nominees or money mules. Of the three, professional money launderers pose the greatest threat both in terms of 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. 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 ML operations. As a group, they use many different methods and techniques, sometimes within the same scheme, to launder money that is challenging to detect. The professional money launderers are of principal concern since they are often the masterminds behind large-scale ML schemes and are frequently used by the most powerful transnational OCGs in Canada. Nominees and money mules are less of a threat, but nonetheless important because they may be critical in carrying out or facilitating ML schemes, both large and small.

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

ML Threat from Tobacco Smuggling and Trafficking: The largest quantity of illicit tobacco found in Canada originates from the manufacturing operations based on Aboriginal reserves that straddle Quebec, Ontario and New York State. Given the profitable nature of the illicit tobacco trade, there is significant organized crime involvement in the smuggling and trafficking of illicit tobacco across the Canada-U.S. border. The OCGs involved in the illicit tobacco trade are some of the most sophisticated and threatening in Canada. These OCGs have the sophistication and capability to 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 the illicit tobacco smuggling and trafficking. In addition to the proceeds of crime generated from the reserve-manufactured illicit tobacco trade, proceeds of crime are generated from counterfeit cigarettes imported from overseas (primarily from China); 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.

High Money Laundering Threats

ML Threat from Currency Counterfeiting: The large-scale production of Canadian counterfeit currency is primarily undertaken by OCGs. OCGs generally 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. They appear to 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 is believed 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 are suspected to be very sophisticated and capable in terms of laundering the proceeds of crime arising from human smuggling. A review of suspected ML cases largely related to human smuggling indicates that OCGs may use a variety of sectors and methods to launder the proceeds, including front companies, legitimate businesses, banks, MSBs and casinos.

ML Threat from Human Trafficking: Canada is primarily a destination country for human trafficking, and domestic human trafficking for sexual exploitation is the most common form of human trafficking in Canada.[17] 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 any real levels of sophistication or capability in terms of laundering their sex trafficking-related proceeds. It is suspected that most of their activity would centre 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 ML 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.

[17] 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 is prevalent in Canada and it is a concern given that stolen identities are often used to support the conduct of other criminal activities. The OCGs conducting identity crime are well-established and 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 2014, Canadians reported over $10 million in losses to identity crime.[18] It is important to note that identity crime also facilitates the conduct of other criminal activities that generate significant proceeds of crime.

ML Threat from Illegal Gambling: Illegal gambling in Canada consists of private betting or gaming houses, unregulated video gaming and lottery machines, and unregulated online gambling. 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 in it. OCGs conduct these activities in a sophisticated manner. For traditional bookmaking betting activities, OCGs use pyramid-style schemes to protect more senior members of the pyramid. Bookmakers will only accept cash to benefit from its anonymity. For online gambling, OCGs have based the network servers to run illegal gambling sites in jurisdictions where online gambling is legal. It is assumed that the OCGs operating in this space have the capability to use a variety of sectors and methods to launder the proceeds of crime. The main forms of illegal gambling proceeds are cash and possibly high value goods (in instances where gamblers may have run out of cash).

ML Threat from Payment Card Fraud: In Canada, credit card fraud has increased significantly over the last five years while debit card fraud has decreased significantly over that period. "Card not present" fraud comprises the largest value of all categories of credit card fraud in Canada followed by credit card counterfeiting.[19] As with other frauds, OCGs are heavily involved in payment card fraud. Organized crime involvement in payment card fraud can involve card thefts, fraudulent card applications, fake deposits, skimming or card-not-present fraud. Most OCGs in this space are sophisticated and have specialized technological knowledge. OCGs that operate payment card theft networks are suspected to, in large part, exhibit very high levels of sophistication and capability in terms of laundering the payment card fraud-related proceeds. 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. In 2013, Canadians reported close to $500 million in payment card fraud-related losses.[20]

[18] Canadian Anti-Fraud Centre. *Monthly Summary Report—December 2014*.

[19] Card-not-present fraud is 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.

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

ML Threat from Pollution Crime: Pollution crime in Canada comes in a variety of forms and is principally undertaken by OCGs, companies and individuals. 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. Given the sophisticated nature of activities and operations, it is assumed 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. In the case of waste management, the OCGs appear to demonstrate a very high degree of sophistication and capability to operate waste management businesses in a manner that generates illegal profit and is used for money laundering.

ML Threat from Robbery and Theft: Smaller-scale thefts and robberies are 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. The most sophisticated and capable tend 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 ML perspective. It is believed that these OCGs use a range of trade-based fraud and related ML 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 ML schemes given the large amounts of proceeds generated by these networks and the challenges of laundering proceeds that are generated across multiple jurisdictions.

Medium Money Laundering Threats

ML Threat from Firearms Smuggling and Trafficking: The illicit firearms market in Canada appears to be dominated by unsophisticated, criminally inclined individuals and OCGs (primarily street gangs operating in metropolitan areas) as well as a small number of sophisticated OCGs. Very few OCGs are involved in the trafficking or smuggling of firearms for the purpose of achieving large profits. Instead, 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. These OCGs may use their established ML infrastructure to launder the proceeds arising from their firearms trafficking activities, which generally focus on exploiting a number of different sectors using a variety of methods.

ML Threat from Extortion: Over 2,000 incidents of extortion in Canada were reported to police in 2013.[21] Extortion is often conducted in conjunction with or in furtherance of other crimes, such as drug trafficking, illegal gambling and human trafficking. Some OCGs systematically use extortion as a tool to obtain money and property in exchange for the protection of certain businesses; to control the distribution of illicit drugs; to force the payment of illegal gambling debts; or to gain access to ports of entry. Some terrorist groups have been known to use extortion to gain power over individuals to further their objectives, including by extorting funds from diaspora communities in Canada. The OCGs and terrorist groups in this space vary in their levels of sophistication, capability and scope for laundering extortion-related proceeds or raising funds to support terrorism. Structuring and smurfing, the commingling of illicit funds and casino refining activities may be used to launder proceeds of extortion.

ML Threat from Loan Sharking: Loan sharks in Canada appear to target low-income individuals, problem gamblers, illicit drug seekers and cash-strapped entrepreneurs. Conducting loan sharking activities requires working capital, financial aptitude and a capacity to enforce debt collection. 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. OCGs and independent operators conducting this criminal activity are suspected to exhibit a relatively high level of sophistication and capability in terms of being able to launder the proceeds emanating from illicit loans. Some cases indicate that loan sharks use a variety of ML methods to launder their proceeds, including through casinos and financial institutions as well as through the real estate and construction sectors.

ML Threat from Tax Evasion / Tax Fraud (hereafter referred to as 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. Tax evasion is frequently carried out by opportunistic individuals, commonly using relatively unsophisticated techniques to evade taxes, such as falsifying or fabricating documentation to misrepresent their tax situation. To facilitate tax evasion, unscrupulous tax preparers have been known to 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). Since tax evasion generally involves ordinary individuals using tax evasion techniques of low sophistication, the ensuing money laundering is also believed to be unsophisticated. In cases of large (or multiple) refunds that have been generated by sophisticated tax evasion schemes, more sophisticated ML techniques may be observed.

Low Money Laundering Threats

ML Threat from Wildlife Crime: 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 over the last five years. Wildlife crime in Canada appears to be largely conducted by opportunistic, criminally inclined individuals. Individuals conducting wildlife crime are suspected to exhibit low levels of sophistication, capability and scope in terms of laundering wildlife crime-related proceeds. The proceeds tend to be fairly modest (with some exceptions) and the laundering activity appears to be focused on immediately placing or integrating the proceeds for personal use, and limited to one sector.

[21] Statistics Canada. "Police-Reported Crime Statistics in Canada, 2013." *Juristat* article. July 2014.

Chapter 4: Assessment of Terrorist Financing Threats

Overview

Terrorism is the leading threat to Canada's national security.[22] Countering terrorism, including its financing, at home and abroad is a key priority for the Government of Canada.

Canada has listed 54 terrorist entities under its *Criminal Code* and 36 terrorist entities under the *Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism.* [23] The majority of these entities are based in foreign countries, mainly in Africa, Asia and the Middle East.[24] Members or supporters/sympathizers of some of these listed entities 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 in foreign countries. 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[25] have also been affected by terrorism-related incidents that have occurred abroad.

Not all 90 listed terrorist entities pose a TF 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 TF 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 TF threat in Canada is lower. On the other hand, some entities pose a very high or high TF threat but a lower terrorist attack threat to Canada.[26]

A number of TF 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.[27] The transfer of suspected terrorist funds to international locations has been conducted through a number of methods including the use of MSBs, banks and non-profit organizations (NPOs) as well as smuggling bulk cash across borders. Based on open source and other available reporting 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, Pakistan, Palestinian Territories, Somalia, Sri Lanka, Syria, Turkey, United Arab Emirates and Yemen.

---

22 Public Safety Canada. *2014 Public Report on the Terrorist Threat to Canada*.

23 As at December 31, 2014.

24 Examples of terrorist entities in these three regions include: 1) Africa—Al Shabaab, Boko Haram, Al Qaida in the Islamic Maghreb; 2) Asia—Taliban, Haqqani Network, Al Qaida, Liberation Tigers of Tamil Eelam; and 3) Middle East—Hizballah, Hamas, Islamic State of Iraq and Syria (formerly Al Qaida in Iraq).

25 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.

26 It should be noted, however, that this assessment only focused on TF threats and not terrorist attack threats.

27 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 themselves conducting acts of violence, such as in the case of lone wolves or foreign fighters.

Discussion of the Terrorist Financing Threat Assessment Results

After a thorough review of publicly available and classified information related to terrorist groups with a Canadian nexus, the TF threat posed by actors associated with 10 terrorist groups and foreign fighters was assessed (see Table 2 below).

Table 2
Terrorist Financing Threat Groups of Actors

Al Qaeda in the Arabian Peninsula	Hizballah
Al Qaeda Core	Islamic State of Iraq and Syria
Al Qaeda in the Islamic Maghreb	Jabhat Al-Nusra
Al Shabaab	Khalistani Extremist Groups
Foreign Fighters/Extremist Travellers	Remnants of the Liberation Tigers of Tamil Eelam
Hamas	

Experts used the following six rating criteria to assess the TF threat posed by the actors associated with these groups and operating in Canada:

1) *Sophistication*: the extent of the threat actors' knowledge, skills and expertise to conduct sustainable, long-term and large-scale TF operations in Canada without being detected by authorities.
2) *Capability*: the extent of the threat actors' network, resources and overall capability to conduct TF 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 TF activities in Canada.
5) *Diversification of Methods*: the diversity and complexity of TF 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.

Using these rating criteria and currently available intelligence, the terrorist groups listed in Table 2 were assessed as posing a low, medium or high TF threat in Canada. Further information on some of these groups and their financing networks in Canada is provided below.

Al Qaeda Core and Affiliated Groups

Most of the global fundraising networks of Al Qaeda Core and affiliated groups such as Al Qaeda in the Arabian Peninsula (AQAP), Al Qaeda in the Islamic Maghreb (AQIM), Islamic State of Iraq and Syria (ISIS) (formerly Al Qaeda in Iraq) and Jabhat Al-Nusra (an AQIM splinter group) mainly operate in the Middle East. For example, ISIS[28] has been reported to use a range of methods to finance its activities that have been conducted in the territory it occupies in the Middle East. Consequently, fundraising activity by Al Qaeda and affiliated groups in Canada is usually conducted by a handful of individuals using legitimate and illegitimate means, and the TF methods are usually simple and limited.

Al Shabaab

Al Shabaab is a Sunni militant Islamist group aiming to create an Islamist state in Somalia, expel all foreign forces, overthrow the federal government of Somalia and purge the country of any practices it considers un-Islamic. The group also subscribes to the ideology of transnational jihad espoused by Al Qaeda. Al Shabaab has a diversified global fundraising network, although most of its funds come from the area it controls. For example, in East Africa and particularly in Somalia, it exhibits a certain level of sophistication and capability to raise funds, and a significant amount of funding comes from leveraging the area that is under its control and influence. In addition, Al Shabaab has some financing networks in Canada, and fundraising techniques observed in the United States and some Scandinavian countries have also been used in Canada.

Foreign Fighters/Extremist Travellers

More attention has been given in recent years by Canada and other countries to individuals referred to as "foreign fighters" or "extremist travellers" who have travelled to other countries to participate in terrorism-related activities. 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. These foreign fighters are frequently self-funded or have raised funds from friends and family, and have participated or currently participate in conflicts such as those in Afghanistan, Iraq, Somalia and Syria. Foreign fighters may deplete and close bank accounts and max out credit cards prior to travelling abroad. A number of those individuals remain abroad, some have returned to Canada and others are presumed dead.[29] Foreign fighters returning to Canada[30] 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.

[28] Various news articles and reports, for example the FATF report *Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)*, published in February 2015, have discussed the breadth of TF methods used to date by ISIL (ISIS).

[29] Public Safety Canada. *2014 Public Report on the Terrorist Threat to Canada*.

[30] The Canadian Government is aware of about 80 individuals who have returned to Canada after travel abroad for a variety of suspected terrorism-related purposes. Source: Public Safety Canada. *2014 Public Report on the Terrorist Threat to Canada*.

Hamas

Hamas, which is an abbreviation of 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.

Globally, Hamas is a complex and highly organized group that is well-funded, utilizing a number of financing strategies. Hamas's global network of support is largely based outside of Canada, but there are small groups of Hamas supporters across Canada.

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. 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.

Khalistani Extremist Groups

Khalistani extremist groups, such as Babbar Khalsa International and the International Sikh Youth Federation, are suspected of raising funds for the Khalistan cause in a number of countries, particularly in countries that have large Sikh diaspora populations. 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 fractured and diffuse.

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 assessment 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 ML/TF vulnerabilities of 27 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 27 rated areas, the overall ML/TF vulnerability was rated "very high" for five sectors and products, "high" for 16 sectors and products, "medium" for five 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.

Corporations (and company services providers), express trusts, lawyers[31] and NPOs, 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 ML/TF 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 ML/TF risks. These include, but are not limited to, cheque cashing businesses, closed-loop pre-paid access,[32] factoring companies,[33] financing and leasing companies, ship-based casinos, unregulated mortgage lenders and white-label automated teller machine providers.

Table 3
Overall Inherent Money Laundering/Terrorist Financing Vulnerability Rating Results

Very High Vulnerability Rating	
Corporations[1]	National Full-Service MSBs[3]
Domestic Banks	Small Independent MSBs
Express Trusts[1]	
High Vulnerability Rating	
Brick and Mortar Casinos	Life Insurance Companies
Company Services Providers	Registered Charities
Credit Unions and Caisses Populaires	Open-Loop Prepaid Access
Dealers in Precious Metals and Stones	Real Estate Agents and Developers
Foreign Bank Branches	Securities Dealers
Foreign Bank Subsidiaries	Smaller Retail MSBs
Internet-Based MSBs	Trust and Loan Companies
Legal Professionals	Virtual Currencies
Medium Vulnerability Rating	
Accountants	Provincial Online Casinos
British Columbia Notaries	Wholesale and Corporate MSBs
Independent Life Insurance Agents and Brokers	
Low Vulnerability Rating	
Life Insurance Intermediary Entities and Agencies[2]	

1 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.

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

3 The definition of each of type of assessed MSB is provided in the glossary.

31 The provisions of the PCMLTFA that apply to the legal profession are effectively inoperative as a result of court decisions and related injunctions. Following a February 13, 2015 Supreme Court of Canada ruling, the Government of Canada is revisiting these provisions and intends to bring forward new provisions for the legal profession that would be constitutionally compliant.

32 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 involving a defined merchant or location (or set of locations). The definition includes gift cards that provide access to a specific retailer, affiliated retailers or a retail chain, or alternatively to a designated locale such as a public transit system.

33 Factoring is a form of asset-based financing whereby credit is extended to a borrowing company on the value of its 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.

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[34] in the world with a land area of 9.9 million square kilometres. Canada has a total of over 200,000 kilometres 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 kilometres, 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 and Financial System

Canada was the 15th largest economy in the world at the end of 2013 (based upon a ranking of real gross domestic product (GDP), with a value of 1,518.4 billion current international dollars).[35] 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.[36]

[34] Financial Action Task Force (FATF). *Third Mutual Evaluation on Anti-Money Laundering and Combating the Financing of Terrorism—Canada* (Paris: FATF/OECD, 2008); and Central Intelligence Agency. *The World Factbook.* Website content on Canada.

[35] International Monetary Fund. *World Economic Outlook: Legacies, Clouds, Uncertainties*. October 2014.

[36] Statistics Canada. Gross domestic product at basic prices, by industry. CANSIM Table 379-0031.

International trade represents more than 60 per cent of Canada's GDP.[37] Canada's economy is closely linked to that of the United States. In 2013, over 74 per cent of Canada's exports went to and through the United States, and over 64 per cent of Canada's imports came from the United States.[38] The two other main export destinations for Canada are China and the United Kingdom.[39] China and Mexico are the two other main sources of Canadian imports behind the United States.[40]

Since 2006, the size of Canada's underground economy (i.e., economic activity that is not reported for tax purposes) expressed as a percentage of GDP is estimated to have dropped to 2.3 per cent[41] from 2.9 per cent in 1992. A recent Organisation 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.[42]

Canada's financial system is mature, sophisticated and well diversified, and plays a key role in the Canadian economy. The financial system, with assets totalling about 500 per cent of GDP,[43] contributes to 6.7 per cent of Canada's GDP.[44] Canada's banks and other financial institutions operate an extensive network of more than 6,200 branches, and about 60,000 automated teller machines (ATMs) of which about 16,900 are bank-owned.[45] In 2012, approximately 842 million transactions were logged at bank-owned ATMs.[46]

The Internet is now the main means of conducting banking transactions for nearly 50 per cent of Canadians, and the use of the Internet as the primary banking choice is increasing among all age groups.[47] Banks also operate through agents or mandataries, mostly in remote areas. Canada also enjoys a relatively high rate of financial inclusion, with 96 per cent of the population having an account with a formal financial institution.[48]

While the banking sector in Canada is diverse and includes many service providers, it is relatively highly concentrated and holds over 60 per cent of the financial system's assets.[49] The banking sector is dominated by six domestic banks that, in the aggregate, hold 93 per cent of bank assets.[50] These six banks are the parents of large conglomerate financial groups and have been designated as D-SIBs by OSFI, Canada's prudential supervisor. Provincially regulated financial institutions, including pension funds, mutual funds and credit unions, amount to almost 30 per cent of the financial system. There are also some large provincially chartered and supervised deposit-taking financial institutions with aggregate financial sector assets equivalent to five per cent of banking sector assets.[51]

---

37 Foreign Affairs, Trade and Development Canada. *Global Markets Action Plan: The Blueprint for Creating Jobs and Opportunities for Canadians Through Trade*. 2014.

38 Statistics Canada. Imports, exports and trade balance of goods on a balance-of-payments basis, by country or country grouping. CANSIM Table 228-0069.

39 Ibid.

40 Ibid.

41 Canada Revenue Agency. *Reducing Participation in the Underground Economy—Canada Revenue Agency 2014–2015 to 2017–2018*. November 2014.

42 György Gyomai and Peter van de Ven. "The Non-Observed Economy in the System of National Accounts." OECD Statistics Brief. June 2014.

43 International Monetary Fund. *Canada: Financial Sector Stability Assessment*. IMF Country Report No. 14/29. February 2014.

44 Statistics Canada. Monthly gross domestic product by industry at basic prices in chained (2007) dollars—Seasonally adjusted. August 2013.

45 Canadian Bankers Association. *Fast Facts About the Canadian Banking System*. Toronto: November 2014.

46 Ibid.

47 Ibid.

48 World Bank. Financial Inclusion Data (Canada). 2011.

49 International Monetary Fund. *Canada: Financial Sector Stability Assessment*. IMF Country Report No.14/29. February 2014.

50 Ibid.

51 Ibid.

There are approximately 31,000 financial institutions and DNFBPs (e.g., 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. Table 4 provides an appreciation of the relative size of the various assessed sectors and products.[52]

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 60 per cent of the financial sector's assets; the six largest domestic banks, the D-SIBs, hold 93 per cent of these assets.
Other Domestic Banks[53]	22	
Foreign Bank Subsidiaries[54]	24	
Foreign Bank Branches[55]	29 (26 full service and 3 lending)	
Life Insurance Companies	73 federal and 18 provincially regulated[56]	Assets held on behalf of Canadian policyholders and annuitants totalled over $646 billion (end of 2013).
Independent Life Insurance Agents and Brokers	154,000 agents and 45,000 brokers (est.)	
Trust and Loan Companies	63 federally regulated trust companies and loan companies and 14 provincially regulated[57]	Trust and loan companies account for four per cent of the financial sector's assets, or over $320 billion (mid-2013). The six largest Canadian banks own 95 per cent of these trust and loan companies.[58]
Securities Dealers	3,487[59]	The D-SIBs own six of the securities dealers, accounting for 75 per cent of the sector's transaction volume. This sector also includes financial advisors and investment counsellors.
Credit Unions and Caisses Populaires (CUCPs)	696 CUCPs,[60] six Cooperative Credit Associations and one Cooperative Retail Association that are federally regulated	CUCPs hold over $320 billion in assets (November 2014).
Money Services Businesses (MSBs)	850 registered MSBs[61]	The MSB sector handles billions of dollars in transactions each year. It is estimated that MSBs registered with FINTRAC handle approximately $39 billion a year.

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

[53] Office of the Superintendent of Financial Institutions. *Who We Regulate*. October 2014.

[54] Ibid.

[55] Ibid.

[56] Ibid and Financial Consumer Agency of Canada. *Federal Oversight Bodies and Other Regulators*. October 2014.

[57] Ibid.

[58] Statistics Canada. Trust and mortgage loan companies excluding bank trust and mortgage subsidiaries: quarterly statement of assets and liabilities, end of period. CANSIM Table 176-0028. 2014.

[59] Based on information obtained from the Canadian Securities Administrators (December 9, 2014) and Ontario Securities Commission (as of October 1, 2014) and compiled by FINTRAC.

[60] Credit Union Central of Canada. *System Results*. November 27, 2014.

[61] FINTRAC. Money Services Businesses. Website content. March 31, 2014. It should be noted that the total number of registered MSBs does not include the number of MSB agents. In the Canadian regime, MSB agents are often covered through the MSB which engages/contracts with the agents (depending on the other activities of the MSB agents).

Sector or Product	Number of Known Entities	Notes
Provincially Regulated Casinos[62]	39 reporting entities with 110 locations[63]	The Canadian casino sector generates over $15 billion in revenue annually.
Real Estate Agents and Developers	20,784[64]	
Dealers in Precious Metals and Stones	642[65]	
British Columbia Notaries	Over 336[66]	
Accountants	3,829[67]	
Legal Professionals	104,938 lawyers, 36,685 paralegals and 3,576 civil law notaries[68]	
Express Trusts[69]	Millions (210,000 trusts filed tax returns in 2011 as a result of being liable for tax payable).[70]	
Corporations	Over 2.6 million for-profit corporations, including almost 4,000 publicly traded companies,[71] and approximately over 180,000 not-for-profit[72] organizations[73]	
Company Services Providers	8[74]	
Registered Charities	86,000 federally registered charities[75]	
Prepaid Access (Open-Loop)	N/A	Global open-loop prepaid card transaction volumes have grown by more than 20 per cent over the past four years and were expected to reach 16.9 billion annually in 2014.
Virtual Currencies	Over 480 convertible virtual currencies worldwide accounting for US$5.5 billion in worldwide market capitalization[76]	

[62] 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 ML threats, in particular under "illegal gambling".

[63] As of November 2014 and provided by FINTRAC.

[64] As of January 2013 and provided by FINTRAC.

[65] As of January 30, 2013 and reported by FINTRAC.

[66] As of October 31, 2014 and provided by FINTRAC.

[67] As of January 2013 and provided by FINTRAC.

[68] Based on Canada's *Response to the FATF Survey ML/TF Vulnerabilities of Legal Professionals—2012*.

[69] Express trusts are offered by trust companies that are subject to the PCMLTFA and therefore are partially covered by AML/ATF measures.

[70] See Table 1 in http://www.cra-arc.gc.ca/gncy/stts/t3/2007-2011/table01-eng.pdf

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

[72] This statistic includes not-for-profit organizations that are not incorporated.

[73] As of December 2014 and provided by the Canada Revenue Agency—Charities Directorate.

[74] Based on internal research.

[75] As of December 2014 and provided by the Canada Revenue Agency—Charities Directorate.

[76] As of November 9, 2014. Retrieved from http://coinmarketcap.com/currencies/views/all/.

Demographics

Approximately 86 per cent of Canada's 35.5 million people (July 2014 estimate) live in the country's four largest provinces: Ontario (38 per cent), Quebec (23 per cent), British Columbia (13 per cent) and Alberta (12 per cent).[77] The three largest Canadian cities, in terms of population, are Toronto, Montreal and Vancouver. Data from the 2011 National Household Survey (NHS) conducted by Statistics Canada indicates that Canada, that year, was home to about 6.8 million foreign-born individuals who represented 20.6 per cent of the total population. More than 200 ethnic origins were reported by respondents to the 2011 NHS.

Canada is a multiethnic and multicultural country. This results in a very rich and diversified Canadian society. However, this can also become a vulnerability in certain circumstances or situations that criminals can exploit. Certain diaspora have been 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 media) 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 overseas to become 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, the domestic banks were rated the most vulnerable (very high), primarily driven by the size of the six designated D-SIBs. The D-SIBs are 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 opportunities to use third parties and gatekeepers (e.g., lawyers and accountants) to undertake banking transactions.

The vulnerability of credit unions and caisses populaires (CUCPs), foreign bank branches and subsidiaries, and trust and loan companies were rated high. These institutions are 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 their business focused on corporate clients (given the $150,000 minimum deposit threshold). All of these institutions offer a range of vulnerable products and services and undertake a mix of transactional, ongoing and third-party business. These vulnerable products and services are available to a client base 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 (PEPs) and clients with connections to high-risk jurisdictions. CUCPs operate in more remote Canadian locations that, in

[77] Statistics Canada. Population by year, by province and territory. July 2014.

some instances,[78] may attract high crime and corruption activities as well as transient workers sending remittances back to their home countries, which may be at high risk of ML/TF. Finally, most of these institutions provide services through face-to-face and non-face-to-face delivery channels, provided online or over the telephone, which lend themselves 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, CUCPs 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): Although the MSB sector is broadly vulnerable, the degree of vulnerability is not uniform largely 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 national full-service MSBs that have the most dominant presence in Canada. These MSBs conduct a large amount of transactional business of products and services (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 PEPs, 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 consists of the small, predominantly family-owned MSBs located across Canada that provide wire transfer services largely through informal networks. These 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, they may be vulnerable to being exploited for illicit purposes.

ML/TF Vulnerabilities of Corporations (Very High) and Company Services Providers (High): Of the types of corporations that were assessed, privately held corporate entities were considered to be of greatest concern. Although these entities are widespread and play an important and legitimate role in Canada's economy, they also exhibit certain characteristics that can be exploited to conduct money laundering and terrorist financing. These entities can be structured to conceal the beneficial owner and can be used to disguise and convert illicit proceeds. Company services providers can make it exceptionally easy to establish corporations expeditiously that can be used as part of an illicit scheme.

[78] 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 Vulnerability of Express Trusts (Very High): The express trust is a widely used legal arrangement in Canada, and the assets held in and the volume of transactions generated from these trusts are believed to be very significant. The critical vulnerability of the express trust is that it can be structured to make it difficult to ascertain the identity of the parties to the trust and it can be difficult to freeze and seize assets held in the trust since the trust separates legal ownership (control) from beneficial ownership. The client profile of express trusts would include high net worth clients (i.e., wealth, estate and tax planning) and clients who may be attracted to the trust vehicle given the anonymity and asset shield that it can provide (e.g., protection from civil litigation, regulatory and criminal action, divorce and bankruptcy proceedings). Express trusts have global reach; Canadians can establish Canadian trusts in Canada or abroad using domestic or foreign-based trustees, and non-residents can do the same in Canada. Settlors, trustees and beneficiaries may be located in different countries, potentially exposing these trusts to high-risk jurisdictions. Canadian express trusts are predominantly established through 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. Although trusts can be established expeditiously through these professionals, there do not appear to be Canadian-based online trust service providers offering to establish trusts in Canada or abroad for a fee, as is seen for corporate entities.

TF Vulnerabilities of Registered Charities (High):[79] The registered charities of greatest concern are those engaged in "service" activities that operate in close proximity to an active terrorist threat. This encompasses registered charities 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. The assessment indicates that these service-oriented organizations offer a number of vulnerable products and services, including funds, gifts-in-kind, and educational and social services. They may be involved in transactional and indirect relationships. A large number of the financial transactions conducted by registered charities may be performed via delivery channels involving a high degree of anonymity and involving some level of complexity, such as when multiple intermediaries are involved. Individuals may make anonymous donations to registered charities. While the transfer of funds from one organization to another is not likely to be anonymous, the significant use of cash 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 Brick and Mortar Casinos (High): Brick and mortar 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 is undertaken with these products and services is viewed as important. The casino's business relationship with clientele is mostly transactional but there are some ongoing relationships. The casino's clientele would include PEPs and 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. Despite this monitoring, there is no customer identification or verification of the source of funds.

ML/TF Vulnerabilities of Provincially Regulated Online Casinos (Medium): British Columbia, Quebec, Manitoba and the Atlantic provinces operate online casinos. Although the (legitimate) online casino sector is small, it is poised for growth in other provinces. Online casinos provide a limited number of vulnerable products and services, which constitute the majority of the sector's business operations. Online casinos would have transactional and ongoing client relationships. The client profile of online casinos may include clients in vulnerable occupations and businesses.

[79] The vulnerabilities assessment for NPOs for terrorist financing is presented here while the assessment for ML is included as part of the section on corporations.

The geographic reach of these online casinos is very limited, 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 (Medium) Sectors: The legal and accounting sectors both have a large number of practitioners across Canada who 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 real estate and securities-related transactions, while in accounting this expertise predominantly encompasses financial and tax advice and company and trust formation. Both professions offer vulnerable services to a range of individuals and businesses and frequently act as third parties in transactions. The client profile of the legal sector is believed 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 they are 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 counsel is protected by solicitor-client privilege, which can make the business relationship more opaque to competent authorities.

ML/TF Vulnerabilities of the Life Insurance Sector (Low to High): The life insurance sector in Canada is very large and 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 have operations in foreign countries 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 conducted 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, usually through wire transfers from bank accounts. The securities sector offers a range of products and services that are vulnerable, including brokerage accounts, a variety of investment products and wire transfers, constituting a significant portion of the sector's operations. Clients include individuals, corporate entities, pension funds and institutional accounts, both domestic and foreign. 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. Operations are not restricted to domestic transactions; the sector has international reach and involves business with high-risk jurisdictions on an ongoing basis. Most of the securities transactions involve face-to-face interactions; however, online brokerages, whose presence has been growing, are providing the 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.

ML/TF Vulnerabilities of the Real Estate Sector (High): The real estate sector is very significant in terms of its size and scope and generates a large number of high-value financial transactions on an ongoing basis. The real estate sector is integrated with a range of other sectors, and the purchase and sale of real estate involves a variety of facilitators, including real estate agents, lawyers, accountants, mortgage providers and appraisers. The sector provides products and services that are vulnerable to money laundering and terrorist financing, including the development of land, the construction of new buildings and their subsequent sale. The real estate business consists of a combination of transactional as well as ongoing client relationships and is exposed to high-risk clients, including PEPs, foreign investors (including from locations of concern) and individuals in vulnerable occupations and businesses. Although real estate transactions are typically done face-to-face, third parties can be used to conduct the transactions and there is opportunity to put in place complex ownership structures to obscure the beneficial owner and the source of funds used for the purchase.

ML/TF Vulnerabilities of Dealers in Precious Metals and Stones (DPMS) (High): There are a large number of DPMS located across Canada, from very large to very small dealers, that are highly accessible to domestic clients and, in some cases, international clients (e.g., through online sales). DPMS conduct a large volume of business in high-value commodities that are vulnerable to money laundering and terrorist financing. 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 includes high-risk clients, notably those in vulnerable businesses or professions. The DPMS is a highly accessible sector where there are high-risk clients who can purchase high-value commodities for cash relatively anonymously.

ML/TF Vulnerabilities of Virtual Currencies (High): The virtual currency sector is significant in terms of assets and volume of transactions and it employs a variety of complex business/delivery models, involving a range of participants, some of which are evolving rapidly. The sector provides one type of vulnerable product—virtual currency—but it provides a number of different forms of virtual currency, each of which exhibit varying degrees of vulnerability. Convertible virtual currencies, which constitute an important part of the sector, are the most vulnerable, largely because of the increased anonymity that they can provide as well as their ease of access and high degree of transferability. Virtual currency providers appear to have largely transactional relationships with their clients in addition to some more ongoing relationships. Given some recent cases, criminal elements would appear to be attracted to the level of anonymity provided by convertible virtual currencies. Virtual currencies, notably convertible decentralized virtual currencies, can provide a high degree of anonymity and complexity. They can be traded on the internet and some virtual currencies may permit anonymous funding (funding using cash, prepaid cards, or third-party funding 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 ownership of the virtual currency involved in criminal activities.

ML/TF Vulnerabilities of Open-Loop Prepaid Access (High): The use of prepaid access is prevalent in Canada but it represents a small portion of the payment methods used domestically. Open-loop products, which are offered across Canada, 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 and have higher loading limits require proof of identification. In some cases, however, the verification may be done online, in a non-face-to-face setting.

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

All assessed economic sectors[80] and financial products were found to be potentially exposed to inherent ML risks while a more limited number were found to be exposed to inherent TF risks. This chapter presents the results of the assessment of inherent ML/TF risks by sector and by product, which are represented in a number of charts to allow for comparisons between the level (i.e., very high, high, medium or low rating) of inherent ML or TF risks for each of them. Examples of inherent ML/TF risk scenarios[81] are provided to further demonstrate how threat actors have exploited or could exploit particular sectors and products.

Inherent Money Laundering Risks

By matching the ML threats with the vulnerable sectors or products, the assessment revealed that 14 sectors and products[82] are exposed to very high inherent ML risks involving threat actors (e.g., OCGs and third-party money launderers) laundering illicit proceeds generated from 10 main types[83] of profit-oriented crime.

As stated earlier in this report, transnational OCGs operating in Canada pose the greatest ML threat and, therefore, the greatest ML 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. This is because these launderers are generally not involved in the actual predicate offences and have the expertise to develop schemes that make use of multiple ML methods and techniques that often involve varied sectors, products and services.

Bulk cash smuggling or the use of cash couriers, within Canada and across the Canadian border, is a ML method that is frequently used, including by professional money launderers, as the first step in the ML process and does not involve any sector, product or service. Trade-based money laundering[84] 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.

Charts 3 to 9 provide a graphic representation of all inherent ML risk scenarios involving the exploitation by ML 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 9 on the horizontal axis of Charts 3 to 9 should be cross-referenced with Table 5.

---

[80] It should be noted that the vulnerability and risk to money laundering in regards to NPOs was taken into account as part of the assessment of the ML vulnerability and risk for corporations, while a separate and more specific TF vulnerability assessment of the NPO sector was conducted.

[81] ML or TF risk scenarios presented in this chapter are based on ML/TF expert knowledge and sometimes draw from actual cases or are a composite of multiple cases.

[82] These sectors and products (from highly to very highly vulnerable) are: Brick and Mortar Casinos, Credit Unions and Caisses Populaires, Trust and Loan Companies, Internet-Based MSBs, Virtual Currencies, Legal Professionals, Foreign Bank Subsidiaries, Smaller Retail MSBs, Securities Dealers, Corporations (including NPOs), Domestic Banks, National Full-Service MSBs, Small Independent MSBs and Express Trusts.

[83] The 10 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.

[84] 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.

Table 5
Types of ML Threats (from Low to Very High) Used in Charts 3 to 9

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

The overall inherent ML risk rating for each sector or product was assigned a normalized numerical value of 0 to 1 and is represented on the vertical axis of Charts 3 to 9. The results in the charts are based on the following colour code and numerical values.[85]

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

It should be noted that some areas have the same ML risk rating value and therefore share the same series of points in the charts (e.g., foreign bank subsidiaries and securities dealers in Chart 3 below) and are therefore combined in the legend.[86]

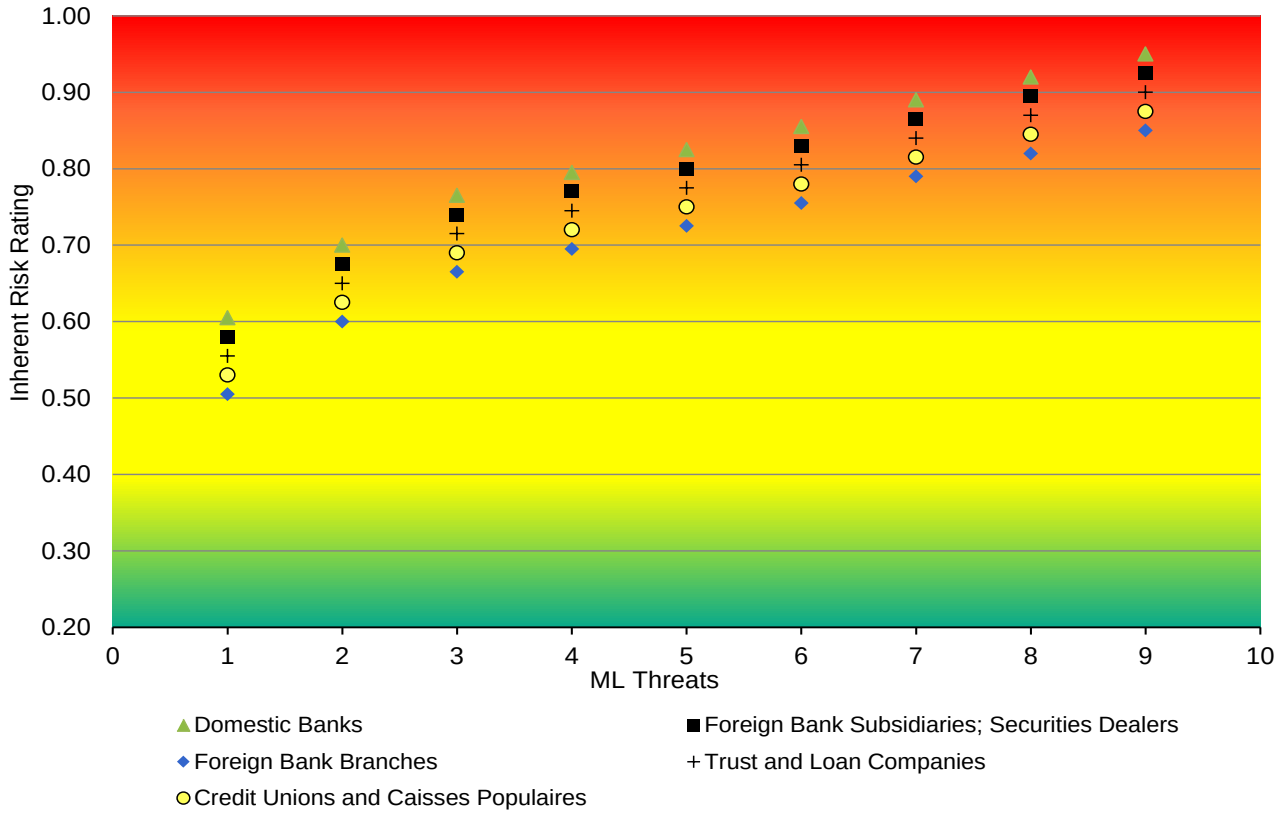
Deposit-Taking Financial Institutions

As illustrated in Chart 3, the majority of ML risk scenarios involving the banking sector, securities dealers, trust and loan companies as well as credit unions and caisses populaires are rated high with a few in the medium or very high range.

[85] The same applies to the TF risk charts provided later in this chapter.
[86] The same applies to the TF risk charts provided later in this chapter.

Chart 3

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



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 travellers). The main ML 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;
- 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 for Canadian currency and vice versa;
- Refining (i.e., converting large cash amounts from smaller to larger bills); and
- Non-face-to-face deposits (i.e., 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 ML activities with the assistance of 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 ML 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 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 ML 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 are exchanged directly between entities rather than through an organized stock exchange such as the Toronto Stock Exchange;
- 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; 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

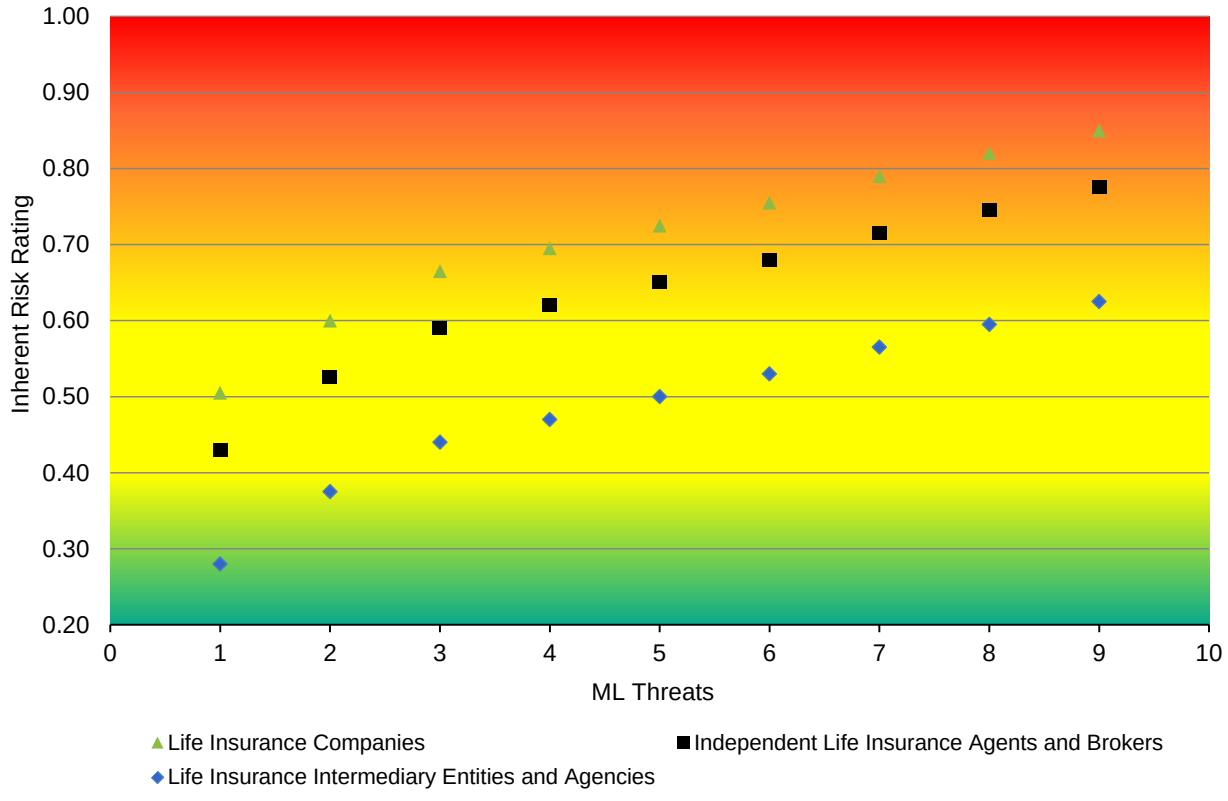
A subject of an investigation purchased over one million shares in a company traded over the counter in an off-market transaction for less than a third of the market price. An investment company sold the shares through an integrated firm (i.e., a major financial institution) on behalf of the investigative 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.

Life Insurance

As illustrated on Chart 4, ML 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 and allow commission pooling opportunities and 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.

Chart 4

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



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

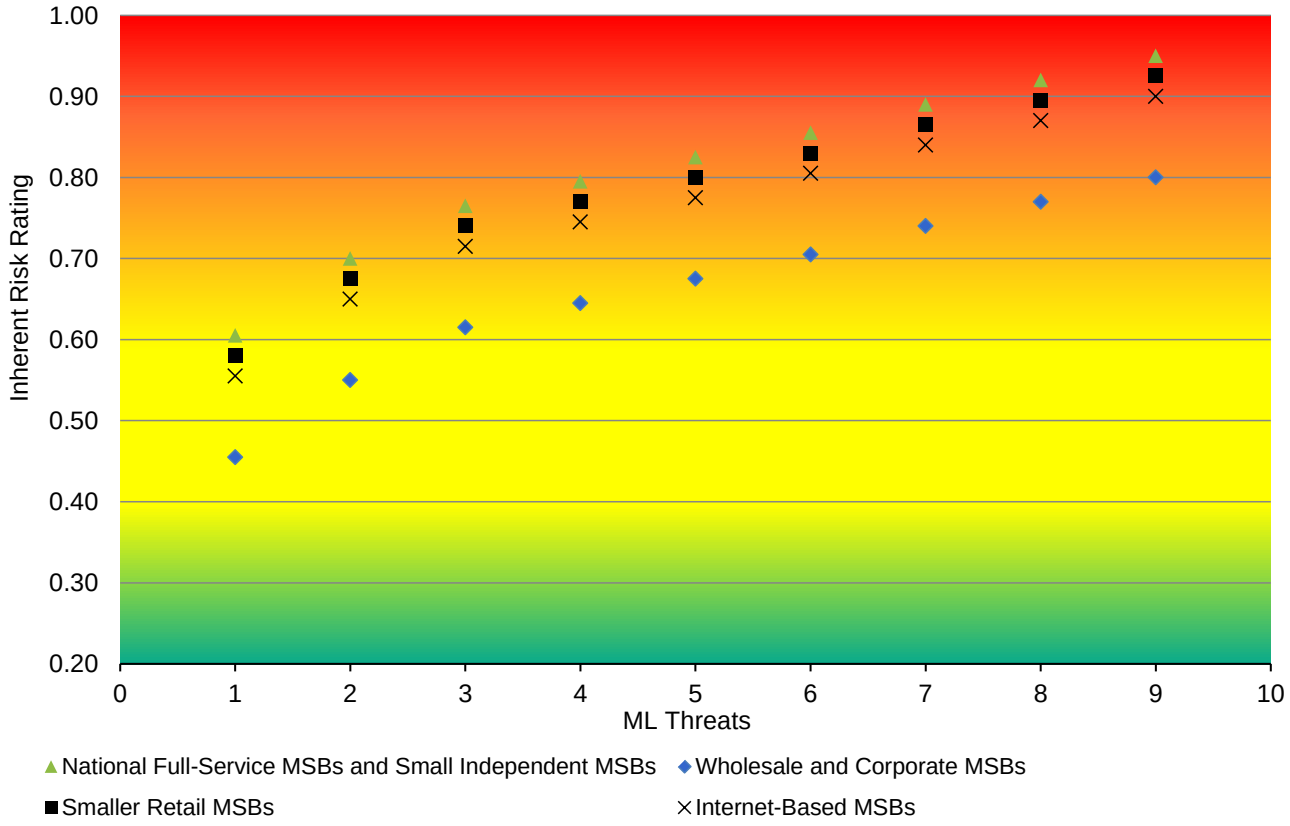
- Early redemption/surrendering of life insurance products with single premium payments and/or high cash values;
- Premium payments made by third parties;
- Use of offshore policies and professional advisors;
- Direct co-option of life insurance industry representatives by criminal elements (e.g., through 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 the ML layering stage once proceeds have been placed in other sectors, with the exception of life insurance fraud proceeds that may be directly placed in this sector.

Money Services Businesses

The majority of ML risk scenarios illustrated in Chart 5 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).

Chart 5

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



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). Cash transactions in this sector are very common and can therefore be used in the ML placement stage. Other products and services such as EFTs, money orders and travellers cheques can also be used in the layering stage of money laundering. Five main ML methods/techniques have been identified for the MSB sector and are further described in the following ML 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;
- Exploiting negotiable instruments; and
- Refining.

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.

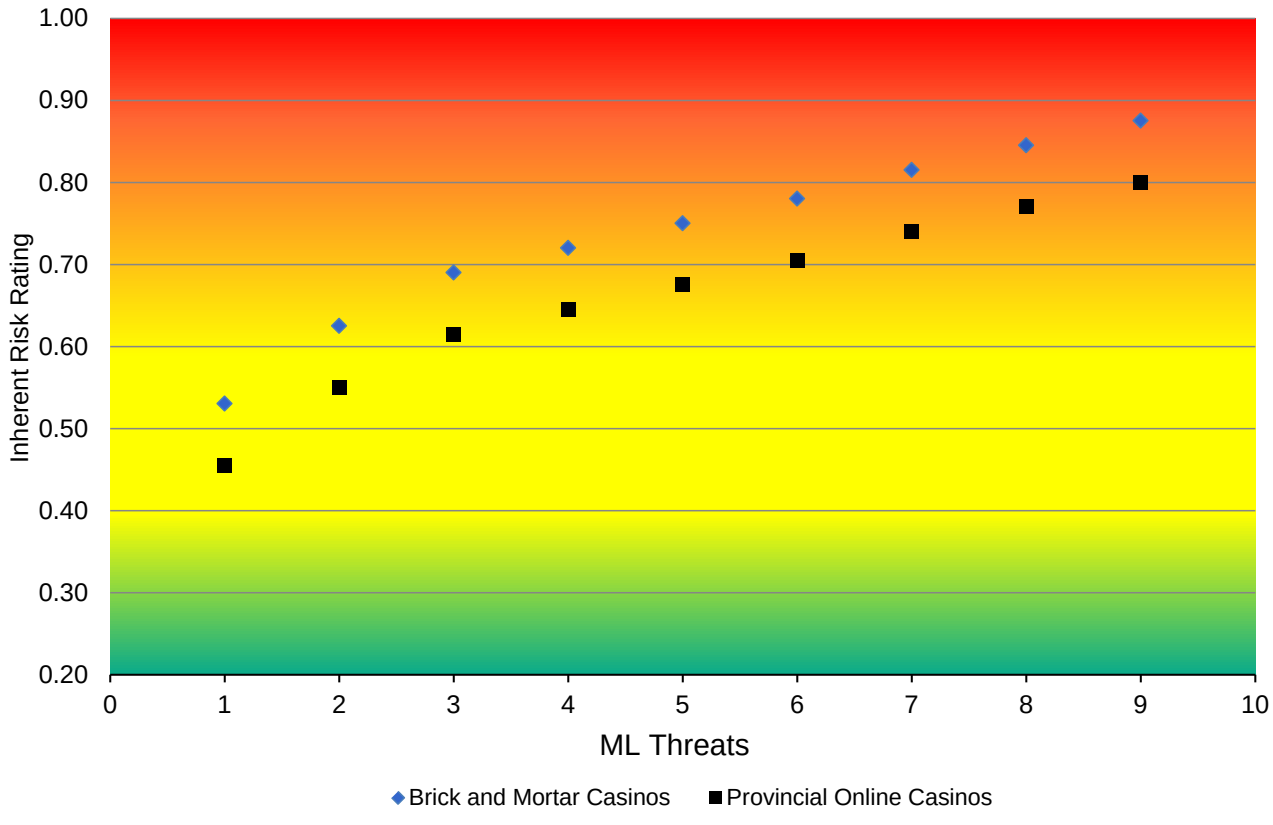
Inherent ML Risk Scenario Involving Monetary Instruments and an Attempt to Circumvent Client Identification Requirements

In one case, an individual purchased dozens of money orders valued in the tens of thousands, in less than a year. Each transaction was structured below record-keeping thresholds, 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.

Casinos

Chart 6 illustrates the different level of ML risk scenarios involving brick and mortar 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 ML risk scenarios than provincially regulated online casinos.

Chart 6
Inherent ML Risks Related to Casinos by Type of ML Threats



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 ML methods and techniques have been used in brick and mortar casinos:

- Use of casino chips;
- Refining (i.e., exchange of small denomination for larger denomination bills);
- Currency exchange;
- Structuring;
- Use of front money account; and
- Use of credit cards.

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 ML activities which include the following:

- Exchanges of small denomination bills for larger denomination bills at the cashier window in amounts under the reporting threshold;
- 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 of a large amount of foreign currency (most often US dollars) 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;
- Passing of cash, casino chips or other casino value instrument between related OCG members prior to entering the casino, either 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 of 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.

Provincially Regulated Online Casinos

Provincially regulated online casinos can be mainly used in the layering stage of money laundering and can involve ML methods and techniques described in the following ML risk scenarios:

Inherent ML Risk Scenario Involving Funding of Account Through Prepaid Credit Card and Minimal Gaming Activity

Criminals, or nominees acting on their behalf, use online casinos to launder illicit proceeds and regularly use credit cards (for which accounts are later paid with illicit funds) or prepaid open-loop cards to fund multiple casino online accounts, after having loaded the prepaid open-loop card with illicit proceeds. When setting up the online accounts, they select the option for having the winnings under a certain threshold and other payouts paid by cheque or deposited directly to their bank accounts. Payouts of funds drawn on a credit card, if under a certain threshold, are refunded to the credit card.

The same individuals are also depositing illicit cash into bank accounts, using those funds to load their online gaming account, and requesting a payout following minimal gaming activity using any of the aforementioned methods, or following cancellation or termination of the account. In other instances, they make multiple transfers of funds, each time going over the online casino operator's account limit, to get casino cheques mailed to them.

Inherent ML Risk Scenario Involving Third-Party Funding

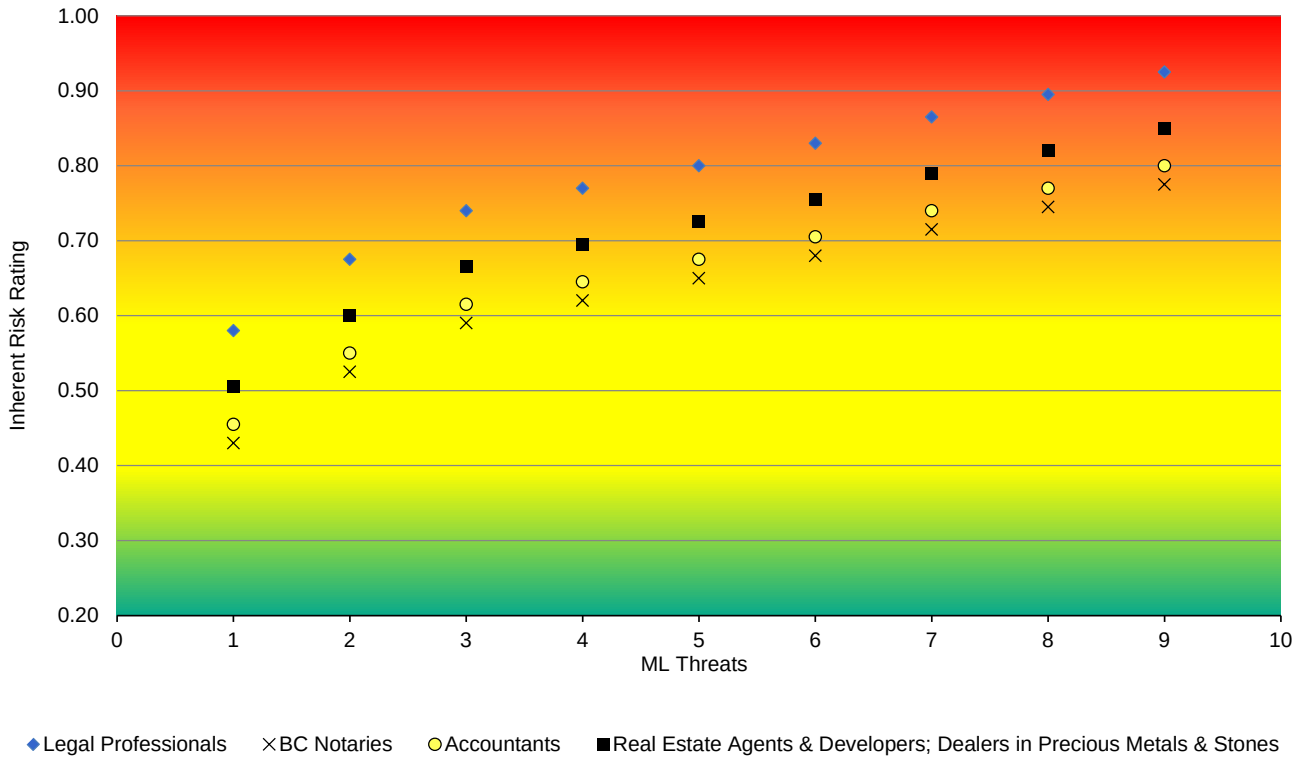
Similarly, the option of wire transfers directly from bank accounts can also be used to facilitate third-party funding of one online casino account. Criminal associates or smurfs hired by a professional money launderer can use the web banking "bill payment" option and select the appropriate online casino operator as a payee. These associates or smurfs may then deposit illicit cash into a bank account and, consequently, transfer funds to the money launderer's online gaming account. The money launderer can then request the payout of funds by way of casino cheque, or could allow the funds deposited to put the account over its limit, generating an automatic payment as described in the first scenario.

Non-Financial Businesses and Professions

The majority of the non-financial businesses and professions represented in Chart 7 are exposed to high ML risk scenarios, although a few fall into the medium or very high category.

Chart 7

Inherent ML Risks Related to Non-Financial Businesses and Professions by Type of ML Threats



Legal Professionals and BC Notaries

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

Legal professionals and BC 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, 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.

Real Estate Sector

The products and services offered by real estate agents and developers provide opportunities to criminals and money launderers. The following four basic ML methods and associated techniques are commonly employed by criminal entities to launder the proceeds of crime through real estate transactions:

- Purchase or sale of property;
- Accessing financial institutions through gatekeepers (e.g., lawyers, mortgage brokers);
- Assisting the purchase or sale of property; and
- Mortgage and loan schemes.

The associated ML techniques most often observed are as follows:

- Hiding or obscuring the funds' source or the buyer's identity;
- Buying or selling using a nominee, corporation or trust;
- Involving a realtor or a non-financial professional as the means for accessing the financial system; and
- Two main ML-specific schemes can involve value tampering and/or purchase-renege-refund.[87]

Real estate transactions can include entities outside of the real estate sector (i.e., third parties relative to a real estate reporting entity and its client). For example, mortgage transactions are conducted within the financial sector; real estate investment trusts operate within the securities dealer sector. In other words, the end-to-end process of applying funds to real estate transactions can involve multiple sectors. Real estate transactions usually involve lawyers and their trust accounts. These lawyers can knowingly or unknowingly provide legitimacy and/or obscure the source of illegally sourced funds. In addition, mortgage brokers, realtors and real estate appraisers can be complicit in laundering proceeds of crime through the purchase of real estate or mortgage fraud. Consequently, mortgage and loan schemes to conduct money laundering usually involve multiple sectors.

Other ML 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. Finally, illicit foreign funds can also be used to purchase Canadian real estate properties.[88]

[87] This refers to the activity involving individuals who commit to purchase a property, make a payment towards it, but then ultimately receive their funds back for not following through on the purchase.

[88] If these funds are sent through an 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 or terrorist financing were suspected.

Dealers in Precious Metals and Stones

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. 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 and jewels 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 ML methods identified are as follows:

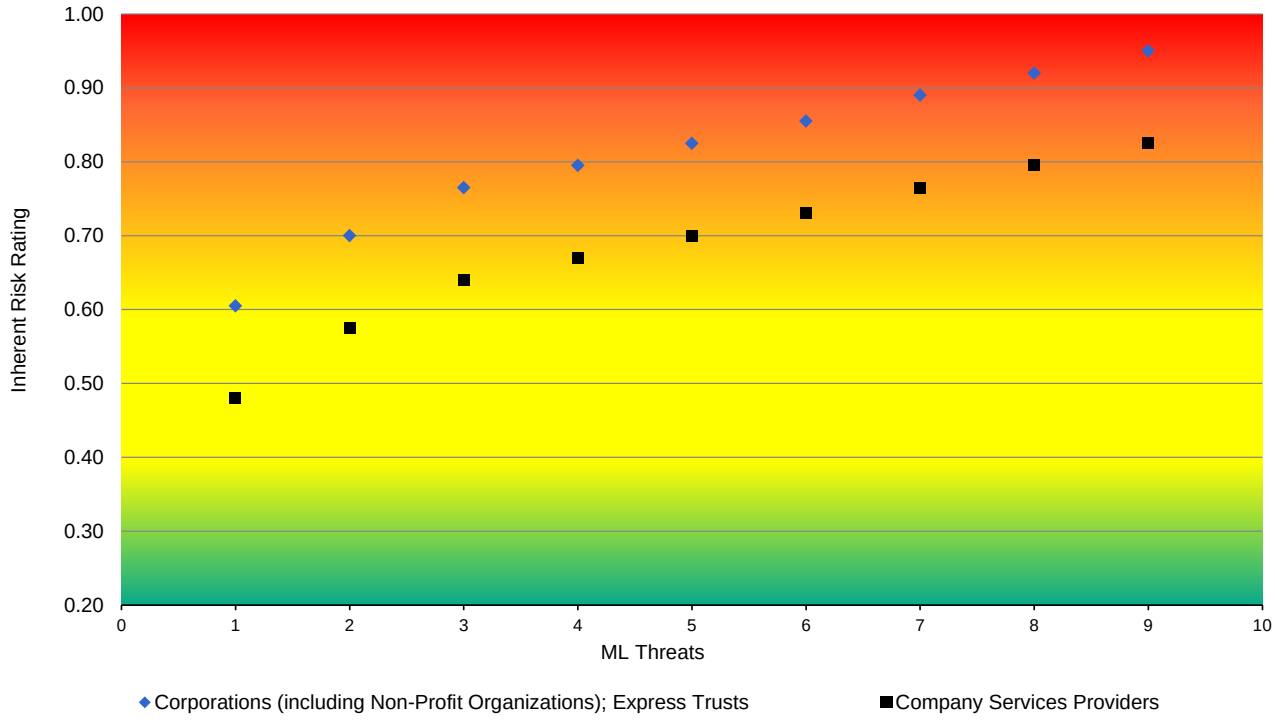
- Purchase of precious metals and jewellery with the proceeds of crime and subsequent sale;
- Use of DPMS sector businesses as fronts to launder proceeds of crime;
- Use of accounts held with precious metal dealers for laundering the proceeds of crime;
- Assisting the purchase or anonymizing the purchase 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; and
- Use of precious metals to purchase illicit goods (e.g., drugs).

Corporations, Express Trusts and Company Services Providers

As illustrated in Chart 8, the majority of ML risk scenarios involving corporations and express trusts are rated high to very high since they are often used to hide the beneficial owners of illicitly generated funds through very complex structures that often involve multiple jurisdictions and intermediaries. Private corporations pose the higher inherent ML risk and over 60 per cent of ML cases disclosed to law enforcement by FINTRAC during a five-year period have involved at least one business.[89] Moreover, the commingling of legitimate business revenue with criminal proceeds is a common ML method observed, in particular in drug-related cases. Corporations can also be used as fronts where numerous business bank accounts are used to conduct various transfers of funds between them.

Chart 8

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



[89] This refers to businesses incorporated in both Canada and internationally.

The most commonly documented ML technique is the use of shell companies. A shell company is a legal entity that possesses no significant assets and does not perform any significant operations. To launder money, the shell company can purport to perform some service that would reasonably require its customers to often pay with cash and then create fake invoices to account for the cash. The company can then deposit the cash, make withdrawals, and thus "integrate" the proceeds of crime into the legitimate economy.

Legal entities (i.e., corporations and trusts), chains of ownership of legal entities, and nominees, in conjunction with other tools and methods (e.g., use of offshore services), can then be used to conceal the true owner of the corporation or the trust. Legal entities are therefore used to effectively conceal or at least deter authorities from uncovering the identity of their beneficial owners.

As indicated above, setting up an offshore corporation through gatekeepers such as a law firm can also be an effective method to conceal a corporation's true beneficial ownership. Offshore corporations can be quickly established and managed by a local company services provider (CSP). Moreover, because it may be difficult to differentiate between legitimate and illegitimate financial activity, offshore corporations can be effective tools in the layering or integration stages of money laundering.

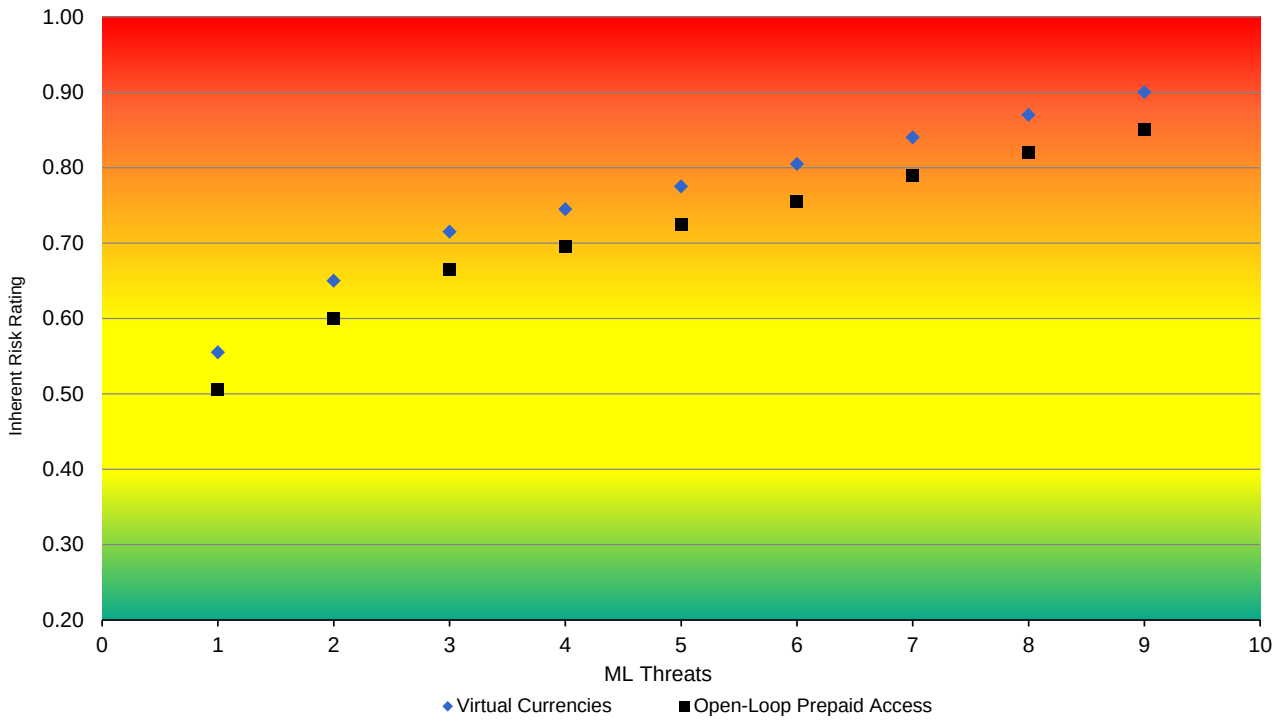
There are only a few CSPs in Canada but they are also exposed to high inherent ML risks, in particular when they are involved in managing corporations for their clients. The limited number of CSPs in Canada is likely due to the fact that provincial or federal incorporation can be done online through provincial/federal service websites, is straightforward and inexpensive, can be done very quickly and does not necessarily require the services of a professional (e.g., a lawyer or a notary). However, legal professionals may be sought to assist in establishing more complex corporate structures.

Canadian criminals can use domestic and offshore corporations and trusts in their ML scheme, but foreign criminals can also use Canadian corporations and trusts to conduct money laundering.

Selected Products Holding Monetary Value

Chart 9 illustrates the level of ML 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 ML 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.

Chart 9
Inherent ML Risks Related to Selected Products Holding Monetary Value by Type of ML Threats



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 digital currency and doing several subsequent layering activities:

- Purchasing goods and services directly with the virtual currency;
- Exchanging the currency again for real money, obtaining a wire transfer from the exchange company; and
- Exchanging one virtual currency for another several times using different exchange companies, before converting it back to real money.

Some virtual currencies, although not criminally controlled, can be adopted by a criminal network as the form of payment. For example, Bitcoin became the exclusive currency of Silk Road, a website used for many crimes including money laundering, after the Liberty Reserve virtual currency was shut down. In another scenario, a criminal could place illicit cash in the Bitcoin automated machine to purchase Bitcoins and then sell them to another buyer. That way, the illicit funds would be placed and layered.

Prepaid Access Products

Because they can be reloaded 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. There have been specific incidents where prepaid access products, mainly open-loop ones, were suspected of being used in ML schemes in Canada:

- In 2009, 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.
- 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 U.S. 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.

Inherent Terrorist Financing Risks

Depending on the nature and extent of TF activities in Canada conducted by individuals associated with the different assessed terrorist groups (see Table 6 below and the discussion in Chapter 4), the breadth of TF collection/acquisition (i.e., fundraising) and aggregation/transmission methods vary and can involve a limited or extended number of sectors and products/services.

Table 6
Terrorist Financing Threat Groups of Actors

Al Qaeda in the Arabian Peninsula	Hizballah
Al Qaeda Core	Islamic State of Iraq and Syria
Al Qaeda in the Islamic Maghreb	Jabhat Al-Nusra
Al Shabaab	Khalistani Extremist Groups
Foreign Fighters/Extremist Travellers	Remnants of the Liberation Tigers of Tamil Eelam
Hamas	

The assessment of TF risks resulted in the identification of five very high TF risk scenarios that involve five different sectors (i.e., corporations, domestic banks, national full-service MSBs, small and predominantly family-owned MSBs and express trusts) that have been assessed to be very highly vulnerable to terrorist financing, combined with one high TF threat group of actors.

On the other hand, a total of 93 high TF risk scenarios were identified that involve, to varying degrees, all 19 sectors and products represented in Charts 10 to 13, and that were assessed to have a medium to very high vulnerability to terrorist financing. Seven different groups of TF 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 TF risk scenarios included in Charts 10 to 13 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.

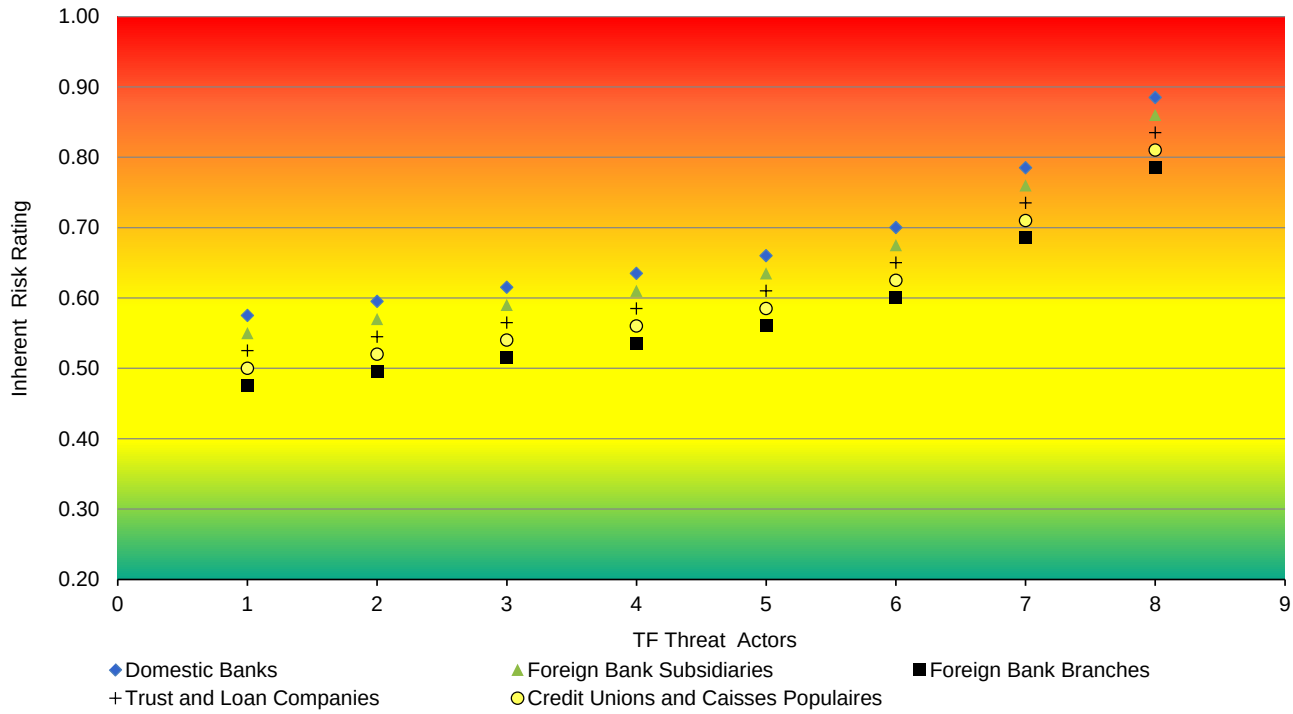
Each number (i.e., 1-8) on the horizontal axis of Charts 10 to 13 represents one group of TF threat actors associated with the different assessed terrorist groups.

Deposit-Taking Financial Institutions

Deposit-taking financial institutions included in Chart 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, the majority of which are active in foreign countries. As for money laundering, but to support different goals, TF risk scenarios described below and rated medium to very high, generally involve the use of domestic wire transfers, international EFTs, monetary instruments such as bank drafts, money orders and cheques (e.g., personal, travellers), personal and business accounts, currency exchanges, trust accounts as well as loan/mortgage and credit card services.

Chart 10

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



Inherent TF Risk Scenarios Involving Deposit-Taking Financial Institutions

The majority of TF actors associated with the assessed terrorist groups are suspected of using international EFTs as one TF transmission method to send funds overseas,[90] often in high-risk jurisdictions. Individuals associated with some of those groups may also use domestic wire transfers to move funds within Canada and/or aggregate collected funds (e.g., cash or web-based[91] 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 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 TF methods involve the use of monetary instruments and commingling of illicit funds[92] with legitimate business revenue in Canada.

Other inherent TF 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[93] and card skimming, have been used by some TF 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 TF 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.

Money Services Businesses

As for 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 TF risk scenarios (rated medium to very high) involving the majority of TF actors associated with the assessed terrorist groups. Although all types of MSBs illustrated in Chart 11 can be exploited for TF 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 EFT services are typically agents of national full-service MSBs. Operators of small independent MSBs may have ethno-cultural or familial links to some foreign jurisdictions and possibly links to informal money value transfer operators (e.g., hawalas). 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.

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

---

[90] The other main method used by many TF actors to move funds overseas is the use of cash couriers travelling overseas; they sometimes travel overseas themselves.

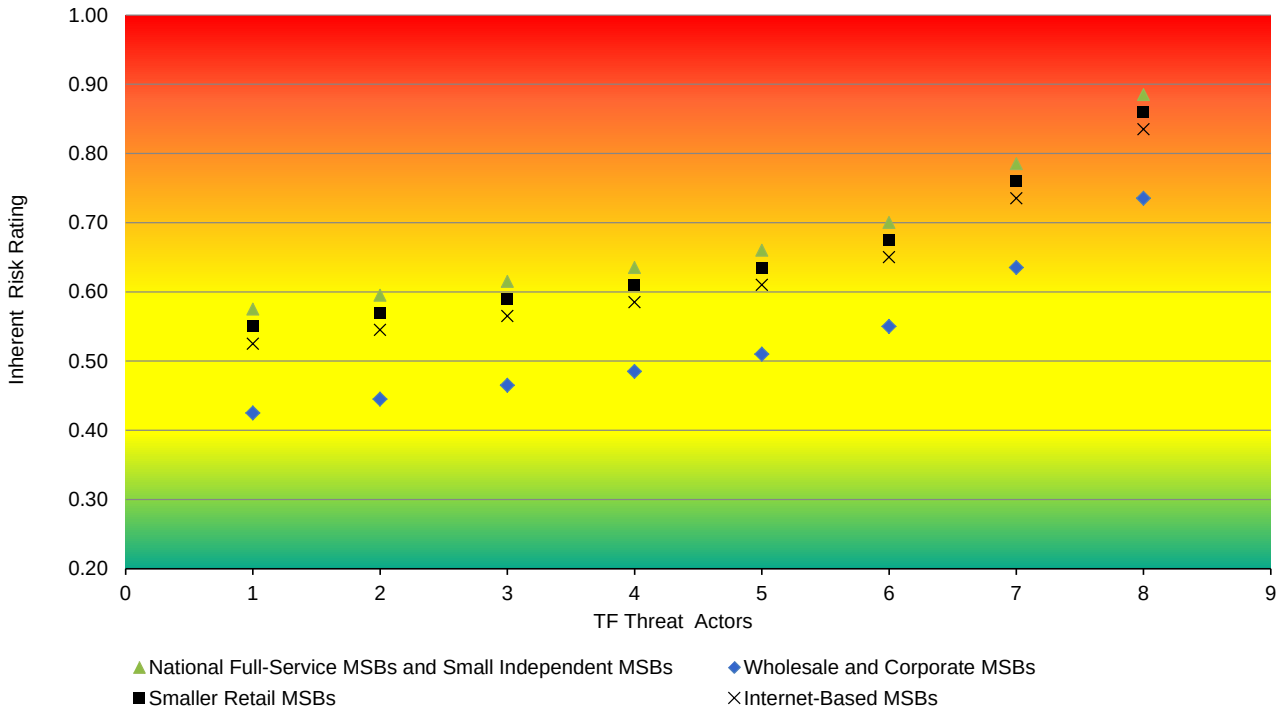
[91] Some TF actors are suspected of having used or are still using websites or social media tools (e.g., Facebook, Twitter) to raise funds, and such activity sometimes involves crowd funding (i.e., multiple donors contributing funds for the same cause or the same individual). Mobile payment systems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

[92] Some TF actors are 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.

[93] 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 variation of this scheme is often the use of stolen or fake identity to obtain credit in the first place.

Chart 11

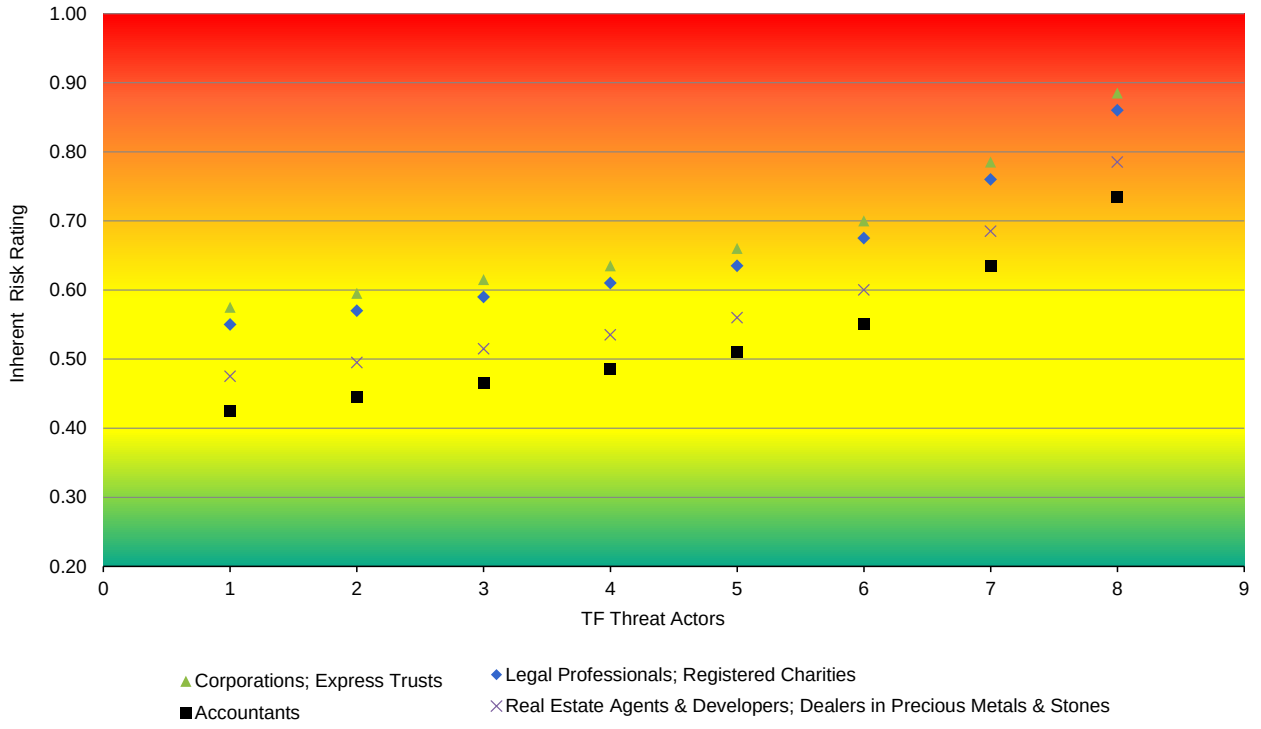
Inherent TF Risks in the Money Services Businesses Sector by TF Threat Actors



Express Trusts and Non-Financial Businesses and Professions

As illustrated in Chart 12, the majority of TF scenarios involving corporations, express trusts, legal professionals and NPOs were rated medium to very high. TF risk scenarios involving accountants, real estate agents and developers, as well as dealers in precious metals and stones were rated medium to high.

Chart 12
Inherent TF Risks Related to Express Trusts and Non-Financial Businesses and Professions by TF Threat Actors



Corporations

Corporations, particularly private ones, are used in TF 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. Generally, corporations involved in TF schemes have been from the food, import/export, shipping/freight, automobile, general contracting/labour, real estate, travel, telecommunications, textile and trading industries. In addition, in the broader context of terrorist resourcing, the procurement of goods is also considered a form of terrorist financing and could involve various types of corporations. Most TF actors associated with the assessed terrorist groups use businesses in some TF schemes.

Legal Professionals and Accountants

Trust accounts, in particular those that are set up by legal professionals, are known to have been used in TF risk scenarios. There have also been some instances where accountants facilitated fraudulent schemes generating funds to support suspected terrorist activities.

Registered Charities

In the context of terrorism and terrorist financing in Canada, the registered charities at higher TF risk are the ones operating in close proximity to an active terrorist threat. Those operating overseas are most vulnerable, as funds or goods may be abused at the point of distribution by the charity or partner organizations. Registered charities that operate domestically, within a population that is actively targeted by a terrorist movement for support and cover, are also exposed to TF risks, as resources generated in Canada may be transferred internationally to support terrorism if the organization does not exercise direction and control over the end-use of its resources. The majority of the TF actors associated with the assessed terrorist groups have used registered charities.

Inherent TF Risk Scenarios Involving Charities

The TF methods used in the majority of TF risk scenarios involving Canadian and foreign charities (referred to as organizations below) can be summarized as follows:

- Diversion of funds—an organization, or an individual acting on behalf of an organization, diverts funds to a known or suspected terrorist entity;
- Affiliation with terrorist entity—an organization, or an individual acting on behalf of an organization, maintains operational affiliation with a terrorist organization or supporter of terrorism, putting it 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 TF 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 centres, 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 redirected to a terrorist entity.

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 with the organization as third parties, such as fundraisers and foreign partners.

Dealers in Precious Metals and Stones

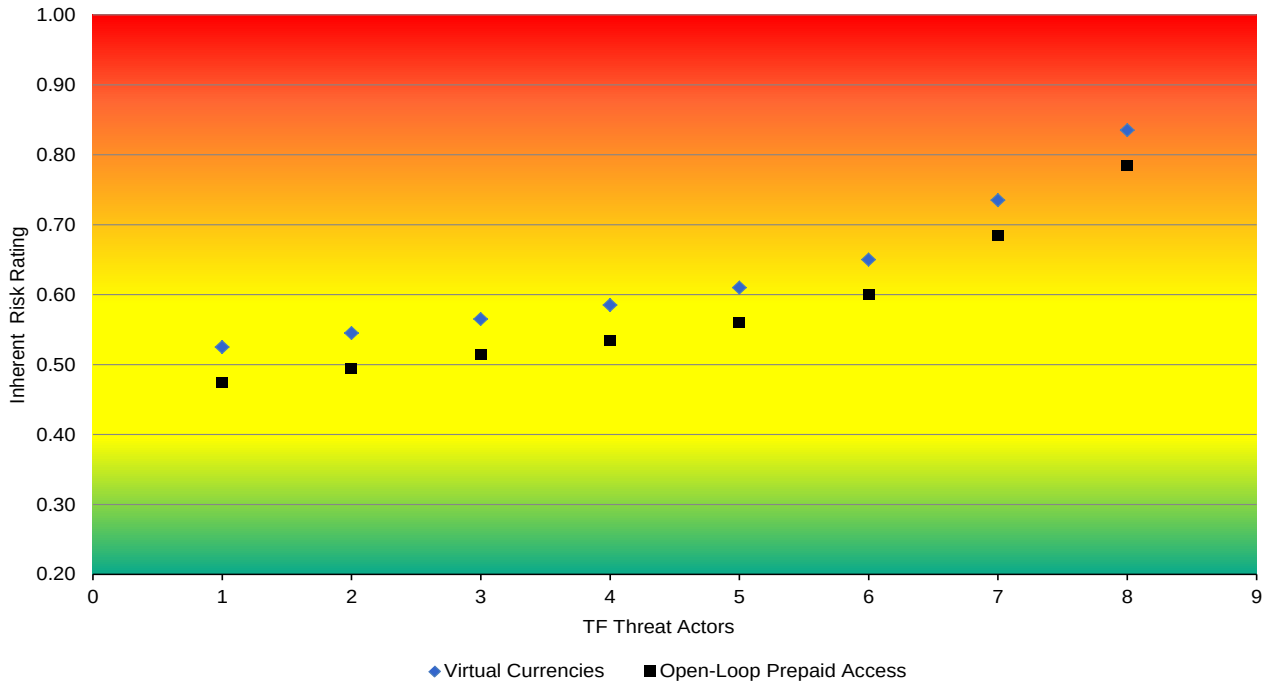
TF actors have purchased precious metals and stones to transfer value without being detected by authorities. Another method to avoid detection is to use precious metals and stones entities as front companies to move funds between different jurisdictions.

Virtual Currencies and Open-Loop Pre-Paid Access

TF risk scenarios involving virtual currencies and prepaid access products have been rated medium to high, as shown in Chart 13. Some TF actors have been reported to use Bitcoins as part of their TF activities and may use other virtual currencies. Although only a few TF cases in Canada have involved the use of open-loop prepaid access products, other jurisdictions have also reported such use.

Chart 13

Inherent TF Risks Related to Products Holding Monetary Value by TF Threat Actors



Next Steps

This risk assessment is an analysis of Canada's current situation and represents a key step forward in providing the basis for the AML/ATF regime to promote a greater shared understanding of inherent ML/TF 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 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 ML/TF risks. FINTRAC and OSFI will include relevant information related to inherent risks in their respective 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 ML/TF risks. Members of the oversight of the regime will also use the results of the risk assessment to inform policy and operations as part of the ongoing efforts to combat money laundering and terrorist financing.

Annex: Key Consequences of Money Laundering and Terrorist Financing

Social Consequences

- Increased criminal activity writ large
- 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 ML/TF activities ("safe haven")
- Loss of credibility and influence internationally
- Lower government revenues
- Negative public perception in the government's ability to deal with ML/TF activity (weak on crime)

Glossary

beneficial owner: the natural person who ultimately owns or controls a customer 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 involving a defined merchant or location (or set of locations). The definition includes gift cards that provide access to a specific retailer, affiliated retailers or a retail chain, or alternatively to a designated locale such as a public transit system.

consequences of ML/TF: the negative impact that money laundering and terrorist financing has on a society, economy and government.

criminalized professionals (or white collar criminals): individuals who hold or purport to hold a professional designation and title in an area dealing with financial matters and who use their professional knowledge and expertise to commit or wittingly facilitate a profit-oriented criminal activity. Criminal professionals would include lawyers, accountants, notaries, investment and financial advisors, stock brokers and mortgage brokers.

designated non-financial businesses and professions: casinos, real estate agents, dealers in precious metals, dealers in precious stones, lawyers, notaries, other independent legal professionals and accountants and trust and company services providers.

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

express trusts (legal arrangements): legal 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, where the assets of the trust are distributed during the settlor's lifetime. In the context of ML/TF, 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 its 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.

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 intermediary entities and agencies to access insurance products.

inherent ML/TF risk: the ML/TF risk that is present in the absence of any controls to mitigate that risk.

inherent ML/TF 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 assessed categories of MSBs, but they are a growing segment of the MSB business.

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.

ML/TF threat: a person or group of people that have the intention, or may be used as witting or unwitting facilitators, to launder proceeds of crime or to fund terrorism.

money mules: individuals who facilitate fraud and money schemes, often unknowingly (e.g., moving money through international EFTs 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 fairly basic and can be used to launder smaller amounts of proceeds of crime.

organized crime 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.

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

smaller retail MSBs: these MSBs are focused on retail transactions, and have 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 is often found in border towns (e.g., duty-free shops), while 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.

structuring and smurfing: 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.

wholesale and corporate MSBs: these MSBs provide money services and related products, predominantly electronic funds transfers and bank drafts, primarily to corporations, on a wholesale basis.

List of Key Acronyms and Abbreviations

AML/ATF	anti-money laundering and anti-terrorist financing
CSP	company services provider
CUCP	credit union and caisses populaires
DNFBP	designated non-financial businesses and profession
DPMS	dealers in precious metals and stones
D-SIB	domestic systemically important bank
EFT	electronic funds transfer
FATF	Financial Action Task Force
GDP	gross domestic product
ML/TF	money laundering and terrorist financing
MMF	mass marketing fraud
MSB	money services business
NPO	non-profit organization
OCG	organized crime group
PCMLTFA	*Proceeds of Crime (Money Laundering) and Terrorist Financing Act*
PEP	politically exposed person

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
ISIS	Islamic State in Iraq and Syria
LTTE	Liberation Tigers of Tamil Eelam
JN	Jabhat Al-Nusra