Department of Finance Canada
Ministère des Finances Canada

Consultation on Strengthening Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime

June 6, 2023

Canada

Process

The Government of Canada has launched this public consultation to examine ways to improve Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime. We invite you to submit comments or feedback in response to specific questions and issues identified in the consultation paper, as well as any further comments or feedback relevant to the scope of this consultation.

Submissions to this consultation will close on **August 1, 2023**.

Contact Us

Email us your comments and feedback at fcs-scf@fin.gc.ca with "Consultation Submission" as the subject line.

Comments and feedback may also be sent by mail to:

Director General
Financial Crimes and Security Division
Financial Sector Policy Branch
Department of Finance Canada
90 Elgin Street
Ottawa ON K1A 0G5

Confidentiality

In order to respect privacy and confidentiality, please advise when providing your comments whether you:

- consent to the public disclosure of your comments in whole or in part;
- request that your identity and any personal identifiers be removed prior to publication; or
- wish that any portions of your comments not be publicly disclosed (if so, clearly identify the portions in question).

Information received through this comment process is subject to the *Access to Information Act* and the *Privacy Act*. Should you indicate that your comments, or any portions thereof, be considered confidential, all reasonable efforts will be made to protect this information.

Table of Contents

Executive Summary

Money laundering and terrorist financing support, reward, and perpetuate criminal activities that threaten the safety and security of Canadians and the integrity of our economy. Canada faces continually evolving risks and threats from money laundering and terrorist financing as criminals adopt new strategies to exploit economic sectors and emerging financial technologies. A strong legislative and regulatory framework and consistent and effective enforcement are required to detect, disrupt, and deter these financial crimes.

In an increasingly interconnected world, Canada is also exposed to transnational criminal elements and corrupt actors seeking to use Canada's economy and financial system as a vehicle for money laundering and terrorist financing. Maintaining international best practices and ensuring a robust sanctions framework assist Canada in fulfilling our international obligations and commitments to combat transnational crime and international security concerns and protect Canadians.

The Government of Canada is committed to a strong Anti-Money Laundering and Anti-Terrorist Financing (AML/ATF) Regime to combat financial crime, while respecting citizens' rights, including privacy rights. Canada's AML/ATF Regime is established under several statutes, including the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA), its associated Regulations, and the *Criminal Code*.

This year, a Committee of Parliament will conduct a Parliamentary Review of the PCMLTFA, as required every five years under section 72(1) of the Act. This requirement provides the opportunity to keep the AML/ATF Regime current in response to market developments, as well as new and evolving risks. The Parliamentary Committee will release a report of its review that will inform future policy measures to strengthen Canada's AML/ATF Regime. To support the 2023 Parliamentary Review of the PCMLTFA, the government has released this consultation paper to review Canada's AML/ATF statutory framework and seek feedback to support the development of policy measures to strengthen the AML/ATF Regime.

Since the last Parliamentary Review in 2018, the government has made important enhancements to the AML/ATF Regime, including strengthening and modernizing laws and regulations, and investing in operational partners. The Department of Finance has published Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime Strategy 2023-2026 outlining its national strategic vision and federal priorities for combatting money laundering and terrorist financing, as well as a Report on Performance Measurement Framework detailing the results achieved by Canada's Regime. This paper aligns with the Regime Strategy and is informed by the findings of the Report on Performance Measurement Framework.

As the money laundering and terrorist financing environment has continued to evolve, the Department of Finance has released an Updated Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada to help policy makers and the public understand the main inherent money laundering and terrorist financing risks faced by key sectors and products in Canada. Notably, the COVID-19 pandemic changed the way people interact with the financial sector and accelerated the trend towards financial sector digitization, which can pose new money laundering and terrorist financing risks.

The government has also responded to new money laundering and terrorist financing risks posed by virtual asset service providers, foreign money services businesses (MSBs), crowdfunding platforms, payment service providers, mortgage lending entities, and armoured car companies. In the two decades since the PCMLTFA was enacted, the global threat landscape has changed in ways that may compromise Canada's national and economic security. Additionally, the government continues to adapt to international security concerns posed by Russia's illegal invasion of Ukraine, including by implementing sanctions against Russian individuals and entities. These raise questions over whether and how the AML/ATF Regime should respond and adapt to these threats.

Despite continued improvements to the legislative and regulatory AML/ATF framework, achieving operational effectiveness remains a persistent challenge. This can cause negative perceptions of Canada as a jurisdiction that is not hostile to money laundering or other financial and profit-motivated crime despite the significant efforts that have been made to crack down on these crimes. Over the years, domestic and international expert reports have highlighted challenges in the ability of Canada's AML/ATF Regime to use financial intelligence, ensure transparency of legal persons and arrangements, successfully investigate and prosecute money laundering, and deprive criminals of the proceeds of crime.

For instance, in its 2016 Mutual Evaluation of Canada, the Financial Action Task Force (FATF), an intergovernmental AML/ATF standard-setting body, found that Canada generally has strong AML/ATF legislation and regulations. However, it pointed to a need for increased efforts to detect, investigate, and prosecute cases across a broader range of the high-risk areas consistent with Canada's risk profile, including various forms of money laundering, pursuing asset recovery more consistently, and use of financial intelligence. The FATF also noted certain gaps in meeting technical standards, many of which were addressed in Canada's 2021 follow-up report. Canada's next Mutual Evaluation by the FATF is scheduled to occur in 2025 for publication in 2026.

Domestically, the provincial government of British Columbia launched the Commission of Inquiry into Money Laundering in British Columbia (also known as the Cullen Commission). The Cullen Commission's final report, issued in June 2022, was critical of the federal AML/ATF Regime and raised questions about its effectiveness. The final report contained findings and recommendations specific to British Columbia, some of which are relevant to the federal AML/ATF Regime. The Government of Canada welcomed the Commission's final report and has committed to responding to all recommendations within its jurisdiction.

Objectives and Structure of This Paper

The overall objectives of this paper are to support the 2023 Parliamentary Review of the PCMLTFA and consult on potential policy measures, some of which may be considered for future legislative and regulatory amendments, including to the PCMLTFA and the *Criminal Code*. Feedback provided to this consultation will be valuable to policy makers within the AML/ATF Regime, such as the Departments of Finance and Justice, and the Parliamentary Committee conducting the review. Using feedback from this paper and the findings of the upcoming Parliamentary Review, the government will take further actions to:

- Improve the operational results of the AML/ATF Regime regarding the detection and disruption of money laundering and terrorist financing activities;
- Strengthen the overall Regime, in alignment with the AML/ATF Regime Strategy and Performance Measurement Framework Report;
- Address risks and vulnerabilities, including those of higher risk identified in the updated risk assessment and those related to national and economic security;
- Position Canada for its next FATF evaluation and uphold international commitments; and
- Respond to findings from the Cullen Commission.

This paper is organized into four main parts. Part I (Chapters 1-3) provides an overview of Canada's AML/ATF Regime and government efforts to combat money laundering and terrorist financing. Part I provides background information and context on Canada's AML/ATF Regime and contributions to international efforts. It also outlines key developments since the 2018 Parliamentary Review, such as legislative and regulatory changes, investments in operations, and efforts to combat new risks stemming from trade-based money laundering. Part 1 also explores priorities for greater federal, provincial, and territorial collaboration and engagement, including advancing a pan-Canadian beneficial ownership registry, exploring risks in the legal profession, and depriving criminals of their property, including reviewing civil forfeiture powers and the potential need for new tools, such as unexplained wealth orders.

Part II of this paper (Chapters 4-6) explores ways to enhance the operational effectiveness of the AML/ATF Regime to investigate and prosecute money laundering and terrorist financing and deprive criminals of the proceeds of crime. Chapter 4 explores areas for possible criminal law reforms under the *Criminal Code* for which the Department of Justice seeks input, including the seizure and forfeiture of proceeds of crime and digital assets, and on the offence and sentencing of money laundering. Chapter 5 considers the creation of a new Canada Financial Crimes Agency that would become the lead enforcement agency against financial crimes. Chapter 6 explores enhancing information sharing to better facilitate the detection and disruption of money laundering and terrorist financing, while protecting privacy rights. Chapter 6 also considers a framework for private sector organizations to share information among themselves for AML/ATF purposes, as well as enhancing information sharing between the private sector and federal AML/ATF entities, and among government departments and agencies.

Part III of this paper (Chapters 7 and 8) considers the legislative and regulatory framework of the PCMLTFA. Chapter 7 explores the scope and obligations of the PCMLTFA to help ensure that current obligations effectively target risks, and whether it should expand to cover new sectors, such as luxury goods, white label automated teller machines, horse racing betting, title and mortgage insurers, real estate sales by owner or auction, crypto and digital assets technology, as well as financial crown corporations. Chapter 7 also explores whether regulatory requirements can be streamlined in keeping with a risk-based approach. Chapter 8 reviews the regulatory compliance framework to ensure that the Financial Reports and Analysis Centre of Canada (FINTRAC), Canada's AML/ATF regulator and financial intelligence unit, can effectively supervise persons and entities subject to the PCMLTFA. This includes exploring new compliance and oversight tools for FINTRAC, such as allowing FINTRAC to record compliance examinations, provide exemptive relief for testing new technologies, and requiring all regulated persons and entities under the PCMLTFA to register with FINTRAC. It also considers additional measures to target and mitigate risks on a sectoral and geographic basis and strengthen existing requirements around verifying the source of funds used in transactions to ensure they are legitimate.

Part IV of this paper (Chapter 8) discusses national and economic security. The global threat landscape has changed considerably since the PCMLTFA was first introduced and may require an update to consider broader threats to the security of Canada. Holding Russia accountable for its illegal invasion of Ukraine has made economic sanctions an important foreign policy tool. This makes sanctions evasion an even more pressing and concerning economic threat, as it undermines the efforts of Canada and international allies to isolate Russia economically. Budget 2023 announced the government's intent to review the mandate of FINTRAC to determine whether it should be expanded to counter sanctions evasion and the financing of threats to national and economic security. Chapter 8 considers these issues in greater detail.

The paper also contains an annex of further technical proposals to modernize and enhance the AML/ATF legislative and regulatory framework.

Other policy measures and issues for consideration that are not explored in this paper may be raised or proposed in the future, potentially stemming from findings from the Parliamentary Review.

This paper was developed by the Department of Finance in collaboration with the federal government departments and agencies that form Canada's AML/ATF Regime (see next section for a list of organizations), and with input from private sector members of the Advisory Committee on Money Laundering and Terrorist Financing. As part of this consultation process, submissions will be shared with the appropriate federal department or agency.

Through this consultation, the government has taken a broad and comprehensive look at Canada's AML/ATF Regime and considered many potential measures for its improvement. As noted above, this includes improving operational effectiveness and enforcement outcomes, facilitating greater information sharing, modernizing legislative and regulatory obligations while balancing burden on the private sector, and responding to national and economic security risks. The government invites feedback and views on ways to improve Canada's AML/ATF Regime, including on the main policy themes, as well as on the specific questions and issues raised in this consultation. Submissions can choose to cover any and all of the topics raised in this consultation.

Part I – Overview and Government Efforts to Combat Money Laundering and Terrorist Financing

Chapter 1 – Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime

Combatting Money Laundering and Terrorist Financing

Money laundering is the process used to convert or conceal the origin of criminal proceeds to make them appear as if they originated from legitimate sources. Money laundering benefits domestic and international criminals and organized crime groups. Terrorist financing 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.

Most Canadians have no direct exposure to money laundering or terrorist financing activities; however, these crimes affect our society by supporting, rewarding, and perpetuating broader criminal and terrorist activities. Money laundering is not a victimless crime. The proceeds of crime being laundered in Canada are often generated at the direct expense of and harm to innocent Canadians, through crimes such as fraud, theft, drug trafficking, human trafficking for sexual exploitation, and online child sexual exploitation. As long as criminals can continue laundering the proceeds from their crimes, they have a strong incentive to continue the criminal activities and enterprises that harm Canadians and our society.

Measures to counter money laundering and terrorist financing have long been recognized as powerful means to combat crime and protect the safety and security of Canadians, as well as the integrity of our economy and financial system.

Internationally, Canada is recognized as a multicultural and multiethnic country with a stable and open economy, accessible financial system, well-developed international trading system, and strong democratic institutions. Although these features are among Canada's strengths, some can be subject to criminal exploitation. Transnational criminals, organized crime groups, and terrorist financiers may seek to use Canada's stable economy and financial system as a vector for money laundering and terrorist financing, exploiting Canadians, including diaspora communities, in the process. Measures taken by the government to mitigate risks related to money laundering and terrorist financing should be considered within this context. Many Canadians have ties to communities around the world which they maintain, and while there are international risks, these relationships are not, in and of themselves, a vector for money laundering, terrorist financing or other criminality.

Overview of the Anti-Money Laundering and Anti-Terrorist Financing Regime

Several federal statutes and regulations establish Canada's Anti-Money Laundering and Anti-Terrorist Financing (AML/ATF) Regime and set out the roles and responsibilities of the 13 federal partners that contribute to and share responsibility for the Regime's outcomes. Principal among these laws are the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA) and its associated Regulations, and the *Criminal Code*.

The following 13 federal partners contribute to Canada's AML/ATF regime:

- Canada Border Services Agency (CBSA)
- Canada Revenue Agency (CRA)
- Canadian Security Intelligence Service (CSIS)
- Department of Finance Canada
- Department of Justice Canada
- Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)
- Global Affairs Canada
- Innovation, Science and Economic Development Canada
- Office of the Superintendent of Financial Institutions (OSFI)
- Public Prosecution Service of Canada
- Public Safety Canada
- Public Services and Procurement Canada
- Royal Canadian Mounted Police (RCMP)

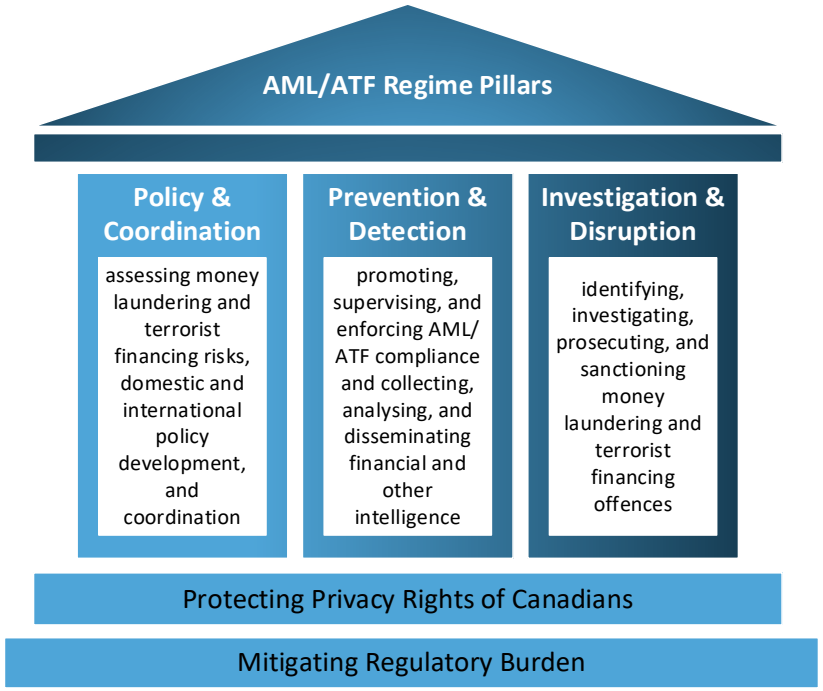
Provincial and municipal law enforcement bodies, provincial Crown Attorneys' offices or prosecution services, and provincial regulators (including those with a role in the oversight of the financial sector) also play important roles in combating money laundering and terrorist financing and may work in partnership with federal Regime partners.

The PCMLTFA stipulates the persons and entities subject to its legislative framework, such as financial institutions and designated non-financial businesses and professions. These persons and businesses, known as reporting entities, must fulfill reporting, record-keeping, and client due diligence obligations under the PCMLTFA. There are over 24,000 reporting entities that play a critical, frontline role in efforts to prevent and detect money laundering and terrorist financing.

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

1. **policy and coordination** – assessing money laundering and terrorist financing risks, domestic and international policy development, and coordination;
2. **prevention and detection** – promoting, supervising, and enforcing AML/ATF compliance and collecting, analyzing, and disseminating financial and other intelligence; and
3. **investigation and disruption** – identifying, investigating, prosecuting, and sanctioning money laundering and terrorist financing offences.

Figure 1
AML/ATF Regime Pilars



Protecting Privacy and Charter Rights

The potential policy measures in this paper seek to combat money laundering and terrorist financing while respecting the Constitutional division of powers, the *Canadian Charter of Rights and Freedoms* (*Charter*) and the privacy rights of Canadians.

Section 8 of the *Charter* enshrines privacy rights as an implicit extension of the individual's right to protection from unreasonable search or seizure by the state. Privacy rights are further established in Canada's two federal privacy laws: the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act*. Privacy rights and protections are detailed further in Chapter 6 on Information Sharing.

The PCMLTFA requires reporting entities to disclose designated financial information to FINTRAC and allows FINTRAC to disclose certain designated information to law enforcement and intelligence agencies for investigation once certain legislative thresholds are met. FINTRAC is independent and arm's length from law enforcement agencies and does not conduct criminal investigations. The PCMLTFA has safeguards in place to ensure that privacy rights are protected in the course of FINTRAC's activities. First, the PCMLTFA prescribes the specific information that FINTRAC can receive and disclose, in addition to the law enforcement and intelligence agencies to which FINTRAC may disclose. The PCMLTFA also limits the circumstances in which FINTRAC can disclose information to these agencies. To disclose information, FINTRAC must have reasonable grounds to suspect that the information would be relevant to the investigation or prosecution of a money laundering or a terrorist financing offence, or relevant to the investigation of threats to the security of Canada.

Further, the PCMLTFA requires the Privacy Commissioner of Canada to conduct reviews of the measures taken by FINTRAC to protect information it receives or collects under the PCMLTFA. This is to ensure that FINTRAC protects the information it receives as part of its operations. The Privacy Commissioner reports the findings of each review to Parliament.

Canada's Contribution to International Efforts

In an interconnected global financial system, the fight against money laundering and terrorist financing requires international efforts and cooperation. Canada's AML/ATF Regime protects the integrity and stability not only of our own financial system, but also contributes to protecting the global financial system. Maintaining a strong AML/ATF Regime helps ensure Canada's financial system and economy remain secure and trustworthy in the eyes of our international allies and trading partners and allows Canada to meet its international commitments.

The Financial Action Task Force (FATF) is an inter-governmental body that sets standards for combating money laundering and terrorist financing and ensures that all members' AML/ATF regimes are held to the same standards. The FATF monitors the implementation of these standards among its own 39 members and the more than 200 countries and jurisdictions in the global network of FATF-style regional bodies through peer reviews and public reporting. Canada is a founding member of the FATF and continues to be an active contributor to the FATF global network.

Canada will have the opportunity to exercise global leadership and influence in combatting money laundering and terrorist financing. Canada has been chosen to serve for two years, effective July 2023, as Vice President of the FATF. Additionally, from July 2022 to July 2024, Canada serves as the Co-Chair of the Asia-Pacific Group on Money Laundering (APG), one of the FATF-style regional bodies. During its time as APG Co-Chair, Canada will advance key priorities in the Asia-Pacific region related to beneficial ownership transparency, combatting grand corruption, countering terrorist financing and digital transformation.

Canada also works with international partners through fora such as the United Nations, the G7/G20, and the Counter-ISIL Finance Group. Canada implements all relevant United Nations Security Council Resolutions to freeze and seize the assets of persons and entities engaged in terrorism.

Canada's Mutual Evaluation Report by the FATF

In September 2016, the FATF released its peer reviewed Mutual Evaluation Report of Canada's AML/ATF Regime. The report found that Canada has a good understanding of its money laundering and terrorist financing risks and that AML/ATF cooperation and coordination are generally good at the policy and operational levels. In addition, Canada was found to have strong AML/ATF legislation and regulations.

The FATF did highlight areas for improvement. With respect to Canada's framework, the limited availability of accurate beneficial ownership information for use by competent authorities, and the fact that the legal profession is not covered by the PCMLTFA, were identified as weaknesses. Regarding operational results, the FATF found that financial intelligence could be used to a greater extent by investigators, money laundering investigation and prosecution results were not commensurate with Canada's risk profile, and that asset recovery was low.

In October 2021, the FATF released its follow-up report, in which Canada was upgraded on several technical compliance standards. The FATF found that Canada had made progress in addressing technical compliance deficiencies related to politically exposed persons, wire transfers, reliance on third parties, reporting of suspicious transactions, and designated non-financial businesses and professions. However, Canada was also downgraded from compliant to partially compliant on the recommendation regarding non-profit organizations, which was revised after Canada's 2016 evaluation.

Canada's next mutual evaluation by the FATF will be adopted in June 2026 and will focus to a greater extent on Canada's ability to demonstrate the effectiveness of its AML/ATF Regime, including Canada's ability to investigate and prosecute financial crime and deprive criminals of offence-related property and the proceeds of crime.

Several of the potential policy measures discussed in this paper are aimed at strengthening Canada's AML/ATF Regime, which would help position Canada for its next FATF assessment.

Chapter 2 – Key Developments Since the 2018 Parliamentary Review

The 2018 Parliamentary Review: Report and Recommendations

The 2018 Parliamentary Review of the PCMLTFA was undertaken by the House of Commons Standing Committee on Finance. The Committee's report, Confronting Money Laundering and Terrorist Financing: Moving Canada Forward, released in November 2018, contained 32 recommendations aimed at improving Canada's AML/ATF Regime.

The government published a response to the Committee' report. The government substantively agreed with most of the Committee's recommendations, which were aligned with the government's direction on AML/ATF.

Since 2018, the government has taken significant actions to strengthen the AML/ATF Regime and address the Committee's recommendations. Many of the recommendations have been addressed, while some are subject to further policy analysis, such as enabling the private sector to share AML/ATF-related information, covering luxury goods and white-label automated teller machines under the PCMLTFA, and creating a framework for geographic and sectoral targeting orders. These proposals are considered in this consultation paper.

Cullen Commission of Inquiry into Money Laundering in British Columbia

On May 15, 2019, the province of British Columbia announced the establishment of the Commission of Inquiry into Money Laundering in British Columbia, also referred to as the Cullen Commission. Broadly speaking, the Cullen Commission had a mandate to inquire into and report on money laundering in British Columbia, and to make recommendations relevant to its findings.

On June 15, 2022, the Cullen Commission released its final report. The Cullen Commission did not make recommendations directly to the federal government, as the inquiry was circumscribed to provincial affairs only. Nevertheless, the findings of the Cullen Commission are valuable for exploring ways to improve Canada's AML/ATF Regime, and some of the report's recommendations have implications for the federal Regime.

The government welcomed the Cullen Commission's final report and has committed to respond to all recommendations within its jurisdiction. Many of the proposals in this consultation paper respond to findings of the Cullen Commission.

Enhancing the Legislative and Regulatory Framework

The government has continued to strengthen and modernize the AML/ATF legislative and regulatory framework to keep pace with new risks, market developments, and international standards.

Based on assessments of risk, additional businesses have been added to the AML/ATF Regime, such as virtual asset service providers, foreign money services businesses (MSBs), crowdfunding platforms, payment service providers, mortgage lending entities, and armoured car companies.

In every Budget since 2019, the government has announced measures to combat money laundering and terrorist financing, including legislative amendments to strengthen the AML/ATF Regime. These changes include amendments to the *Criminal Code* to add the fault element of recklessness to the money laundering offence, as well as amendments to the PCMLTFA to enhance FINTRAC's ability to share financial intelligence with federal partners, increase criminal penalties, and strengthen MSB registration requirements.

Most recently, in Budget 2023, the government announced its intent to introduce legislative amendments to the *Criminal Code* and the PCMLTFA to strengthen the investigative, enforcement, and information sharing tools of Canada's AML/ATF Regime.

These legislative changes would:

- Give law enforcement the ability, based on prior judicial authorization, to seize digital assets that may be confiscated as the proceeds of crime;
- Enhance the ability of Attorneys General to obtain, with prior judicial authorization, tax information for the purposes of investigating offences that give rise to proceeds of crime, by expanding the number of serious offences for which this measure would be available;
- Improve financial intelligence information sharing between law enforcement and FINTRAC;
- Introduce a new offence for structuring financial transactions to avoid FINTRAC reporting;
- Strengthen the registration framework for MSBs to prevent their abuse and criminalize the operation of unregistered MSBs;
- Establish powers for FINTRAC to disseminate strategic analysis related to the financing of threats to the safety of Canada;
- Provide whistleblowing protections for employees who report information to FINTRAC;
- Broaden the use of non-compliance reports by FINTRAC in criminal investigations; and
- Set up obligations for the financial sector to report sanctions-related information to FINTRAC.

Budget 2023 also announced the government's intent to make legislative changes to ensure it has the tools to protect the integrity and security of the Canadian financial sector in response to evolving threats, such as foreign interference. This includes changes to the PCMLTFA that would:

- Provide new powers under the PCMLTFA to allow the Minister of Finance to impose enhanced due diligence requirements to protect Canada's financial system from the financing of national security threats, and allow the Director of FINTRAC to share intelligence analysis with the Minister of Finance to help assess national security or financial integrity risks posed by financial entities;
- Improve the sharing of compliance information between FINTRAC, OSFI, and the Minister of Finance; and
- Designate OSFI as a recipient of FINTRAC disclosures pertaining to threats to the security of Canada, where relevant to OSFI's responsibilities.

The government has also modernized and strengthened Regulations made under the PCMLTFA on a regular basis. In 2020 and 2021, significant regulatory amendments came into force that re-organized the main Regulations under the PCMLTFA and updated and modernized many obligations. This included requirements related to performing client due diligence, verifying beneficial ownership, and identifying politically exposed persons.

Consultations on the latest round of proposed regulatory changes recently concluded on March 20, 2023. The draft regulations, once in force, would:

- Impose AML/ATF obligations on mortgage lending entities and the armoured car sector;
- Enhance the MSB registration framework;
- Improve due diligence and ongoing monitoring with regards to correspondent banking relationships;
- Increase cross-border currency reporting penalties;
- Streamline requirements for sending documents related to Administrative Monetary Penalties to reporting entities, and
- Prescribe a formula for FINTRAC to assess the expenses it incurs in the administration of the PCMLTFA against reporting entities.

Investments in Operations

Since 2019, the government has made investments of $319.9 million, with $48.8 million ongoing, to strengthen data resources, financial intelligence, information sharing and investigative capacity to support money laundering investigations in Canada.

Significant funding has gone to FINTRAC, including $89.9 million over five years and $8.8 million ongoing as part of Budget 2022. This investment will enable FINTRAC to implement new AML/ATF requirements for crowdfunding platforms and payment service providers; support the supervision of federally regulated financial institutions; continue to build expertise related to virtual currency; modernize its compliance functions; and update its financial management, human resources, intelligence, and disaster recovery systems.

As Canada's financial intelligence unit and AML/ATF regulator, FINTRAC plays a key role in helping to combat money laundering and terrorist financing in Canada and internationally. In 2021-22, FINTRAC provided 2,292 unique disclosures of actionable financial intelligence to law enforcement and national security agencies in support of money laundering and terrorist financing investigations across Canada and around the world. This included 757 financial intelligence disclosures related to Canada's public-private partnerships created to combat money laundering in British Columbia, human trafficking for sexual exploitation, online child sexual exploitation, the trafficking of illicit fentanyl, and romance fraud. FINTRAC intelligence disclosures can contain information from hundreds or thousands of reports received from reporting entities. In 2021-22, FINTRAC contributed to 335 major, resource-intensive investigations in Canada, and many hundreds of other investigations at municipal, provincial and federal levels, as well as internationally. Significantly, 97 per cent of the feedback that FINTRAC received from law enforcement and national security agencies in 2021-22 indicated that its financial intelligence was both valuable and actionable.

Project Collector: Dismantling a money laundering organization

In November 2022, FINTRAC's financial intelligence was recognized by the Alberta Law Enforcement Response Team (ALERT) in relation to Project Collector, a three-year investigation that resulted in the dismantling of a third-party money laundering organization that was working in support of some of Canada's largest crime groups. Seventy-one charges were laid against 7 suspects, including participation in a criminal organization and laundering proceeds of crime. Charges were also laid under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*. In announcing the charges, police said that they "relied heavily on intelligence from FINTRAC."

In 2020, the government announced $19.8 million over five years for the RCMP to create new Integrated Money Laundering Investigative Teams (IMLITs) in British Columbia, Alberta, Ontario, and Quebec. As the IMLITs began to ramp up in 2021, the teams integrated specialized investigative resources from partners across Canada's AML/ATF Regime to undertake money laundering investigations and reduce the capacity of, and increase the costs to, organized criminals and crime groups through the removal of their assets.

The RCMP also leads Integrated Market Enforcement Teams (IMETs). These special units detect, investigate, and deter capital markets fraud, which is a form of financial crime that can be associated with money laundering. The IMETs promote compliance with the law in the corporate community and assure investors that Canada's markets are safe and secure. The IMET Initiative is a partnership with the Public Prosecution Service of Canada, provincial and municipal police forces, securities commissions, and market regulators. IMETs are composed of police officers, lawyers, and other investigative experts. They are deployed in the major markets of Toronto, Vancouver, Montreal, and Calgary to respond swiftly to major capital markets fraud.

Combatting Trade Fraud and Trade-Based Money Laundering

Until recently, customs-based commercial trade fraud was mostly understood as a series of techniques used to evade duties and taxes at the border. However, in recent years, it has become increasingly evident that trade fraud techniques can be used to manipulate global trade to conceal and move proceeds of crime across borders. This is known as trade-based money laundering.

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

The CBSA is best positioned to identify most trade-based money laundering attempts using its customs authorities and its knowledge and expertise of international trade. AML/ATF Regime partners are exploring how best to leverage the CBSA's position as Canada's trade "gatekeeper" and enable it to proactively share intelligence with law enforcement for criminal investigations, while respecting privacy laws and *Charter* rights.

Advanced data analytics tools to improve the CBSA's ability to detect trade non-compliance will play an important role in combatting trade-based money laundering in the future. Embracing analytics by onboarding modern tools and technology would vastly expand the CBSA's ability to proactively identify trade non-compliance and reduce dependency on external tips and leads. The CBSA has been collaborating with enforcement partners internationally to identify best practices for identifying complex trade fraud and trade-based money laundering schemes in Canada. This includes exploring the viability of establishing a "Trade Transparency Unit" in Canada (see box below). The final report of the Cullen Commission highlighted trade transparency units as a promising way to better address trade-based money laundering.

Trade Transparency Units

The United States Department of Homeland Security established the concept of trade transparency in 2004 as a tool to identify complex trade fraud and trade-based money laundering schemes through bilateral collaboration between customs services. Trade transparency is achieved through an exchange of corresponding import and export data between the United States and the trading partner's trade transparency unit. Anomalies can be detected when import declarations do not match the equivalent export declarations from the trading partner, and vice versa. These anomalies serve as investigative leads for both countries to confirm through investigative collaboration. Since 2004, the United States has signed 18 bilateral trade transparency unit agreements.

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

In March 2023, the government published the Updated Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada, which updates the first version from 2015.

The 2023 risk assessment assessed the money laundering threat posed by 22 profit-oriented crimes, as well as the threat posed by third-party money launderers (i.e., third parties who launder money as a service to criminals). The assessment found that transnational organized crime groups and third-party money launderers remain the key money laundering threat actors in the Canadian context. Canada's largest money laundering risks come from illicit drug trafficking, various types of fraud, especially mass-marketing fraud, and third-party money laundering. Illegal gambling, corruption, collusion, and bribery are also significant concerns. AML/ATF Regime partners are also carefully monitoring the financing risks linked to ideologically motivated violent extremist (IMVE) threat actors, including white-supremacist groups recently listed as terrorist organizations in Canada.

Understanding money laundering and terrorist financing risks contributes to the government's ability to effectively combat these illicit activities. It supports the policy-making process to identify and address vulnerabilities and potential gaps in the AML/ATF Regime. It informs operational decisions about priority setting and resource allocation, helping to focus on those threats with the greatest economic, social, and political consequences. It also helps the private sector, especially reporting entities, apply risk-based approaches and mitigate their risks.

Regime Strategy and Performance Measurement Framework

In March 2023, the Department of Finance published Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime Strategy 2023-2026, which sets out the government's plan to combat money laundering and terrorist financing over the medium term, including actions to improve performance and outcomes. This consultation paper aligns with the priorities of the Regime Strategy.

The government also published the Report on Performance Measurement Framework for Canada's AML/ATF Regime. Findings from this report have helped to inform priority areas of focus for this consultation paper to improve the results of the AML/ATF Regime.

The report found that, as of 2019-20, the AML/ATF policy framework continues to be improved on a regular basis but identified gaps in corporate beneficial ownership transparency and the mitigation of money laundering risks in the legal profession. The report noted the AML/ATF Regime's increased efforts to promote preventive measures among reporting entities, which has led to FINTRAC receiving more transaction reporting, particularly suspicious transaction reporting. This provided FINTRAC with more information that could be turned into actionable tactical and strategic intelligence, although available resources and the quality of the reporting can affect intelligence output.

The report also noted that results for investigations, prosecutions and forfeitures declined over the past decade. Law enforcement laid few money laundering charges; most money laundering court cases ended with charges being stayed or withdrawn; and the number of convictions and guilty pleas declined. Further, there were very few forfeiture orders in connection with money laundering charges.

Chapter 3 – Federal, Provincial, and Territorial Collaboration

Combating financial and profit-motivated crimes is a shared responsibility between federal, provincial, and territorial governments. Coordinated actions across all levels of government help prevent criminals from exploiting gaps and vulnerabilities across jurisdictions.

Notably, the federal government continues to engage on advancing a pan-Canadian approach to corporate beneficial ownership transparency and has tabled Bill C-42 to finalize its commitment to establish a federal publicly accessible beneficial ownership registry.

To ensure Canada does not become a haven for financial criminals, all levels of government must intensify efforts to deter, investigate, and prosecute money laundering and terrorist financing, as well as efforts to recover proceeds of crime using criminal and civil processes. The federal government wishes to explore how differing levels of governments can better use existing tools to seize and forfeit the proceeds of crime, and the potential need for new measures, such as unexplained wealth orders, while respecting the *Charter* and the constitutional division of powers. Operational partnerships, joint enforcement efforts, and information sharing also play important roles.

Certain economic sectors and businesses vulnerable to money laundering, including money services businesses, provincial financial entities, the legal profession, real estate, casinos, and car dealers and other high-value goods vendors, are subject to different levels and types of

provincial and territorial oversight, including self-regulation according to standards set out in provincial legislation or direct regulation by a provincial government authority. Holistic regulatory efforts across levels of government can help ensure that these sectors and businesses effectively understand and mitigate money laundering risks.

The federal government seeks to collaborate more closely with provinces and territories on cross-governmental issues related to money laundering and terrorist financing, including on the priority areas below.

3.1 – Beneficial Ownership Transparency

The use of anonymous Canadian shell companies can conceal the true ownership of property, businesses, and other valuable assets. With authorities unable to ascertain their true ownership, these shell companies can become tools of those seeking to launder money, avoid taxes, or evade sanctions.

To address this, the federal government committed in Budget 2022 to implementing a public, searchable beneficial ownership registry of federal corporations by the end of 2023. This registry will cover corporations governed under the *Canada Business Corporations Act*, and will be scalable to allow access to the beneficial ownership data held by provinces and territories that agree to participate in a pan-Canadian registry.

Building on previous amendments, in March 2023, the government tabled Bill C-42 to amend the *Canada Business Corporations Act* and other laws, including the PCMLTFA and the *Income Tax Act*, to implement a publicly accessible beneficial ownership registry.

Recognizing the shared responsibility of federal, provincial, and territorial governments for incorporation law, a federal-provincial-territorial working group has collaborated since 2016 on measures to increase beneficial ownership transparency. As a result of this work, most provinces and territories have amended their legislation to require corporations to maintain records about their beneficial owners. The working group continues to meet regularly to advance beneficial ownership transparency objectives, notably the means and mechanisms through which provinces and territories who choose to participate in a pan-Canadian registry could do so.

The federal government will continue calling upon provincial and territorial governments to advance a pan-Canadian approach to beneficial ownership transparency. The government remains committed to a collaborative, harmonized approach to the collection and reporting of beneficial ownership information, while respecting our provincial and territorial responsibilities for corporations.

The Cullen Commission's final report states that governments should not focus their efforts solely on improving the transparency of corporations and notes the largely unmitigated money laundering risks associated with trusts and limited partnerships. Unlike corporations, the responsibility for partnerships falls exclusively under provincial and territorial legislation. Quebec's public beneficial ownership registry, launched, on March 31, 2023, covers not only corporations incorporated in Quebec but also all other legal entities registered to do business there, including partnerships. As progress is made on the transparency of corporations in Canada, criminals may shift their activities towards entities such as partnerships. The federal government will therefore consult with provinces and territories on approaches to access beneficial ownership information for partnerships.

The government passed Bill C-32, which received Royal Assent on December 15, 2022, to require trusts to file additional beneficial ownership information as part of their annual income tax return. Starting in taxation years ending after December 30, 2023, trusts will have to report the identity of all trustees, beneficiaries, and settlors of the trust, along with each person who has the ability (through the trust terms or a related agreement) to exert control or override trustee decisions over the appointment of income or capital of the trust (e.g., a protector). This change improves the collection of beneficial ownership information with respect to trusts and helps the CRA assess the tax liability for trusts and its beneficiaries.

Given the money laundering risks associated with real estate, the lack of access by authorities to beneficial ownership information in this sector is a potential gap in the AML/ATF Regime. Canada does not have a pan-Canadian land registration system. Registration of private residential property ownership falls under provincial and territorial jurisdiction, and land registration systems generally do not contain beneficial ownership information. However, British Columbia launched its Land Owner Transparency Registry on November 30, 2020. It requires all corporations, trustees and partners who purchase land in British Columbia to disclose their interest holders by registering a transparency report with the searchable registry. In Budget 2022, the federal government announced its intention to work with provincial and territorial partners to advance a pan-Canadian approach to a beneficial ownership registry of real property.

3.2 – The Legal Profession

The potential money laundering risks within the legal profession have been well-documented in Canada, including in Dirty Money – Part 2 by Peter German and Associates, the Cullen Commission's final report, and the Updated Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada. These findings are consistent with results from other countries and international reports, such as the FATF's report titled Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals.

In 2015, the Supreme Court of Canada rendered a decision stating that the regulatory requirements of the AML/ATF framework, as they applied to the legal profession, violated the *Charter*. The Court acknowledged the important public purpose of Canada's AML/ATF Regime, and that Parliament could impose obligations on the legal profession that are within constitutional boundaries.

The lack of inclusion of the legal profession in Canada's AML/ATF framework was considered a major deficiency in the FATF's 2016 evaluation of Canada.

Provincial and territorial law societies regulate the legal profession in the public interest, including for AML/ATF purposes. Since June 2019, the government has worked closely with the Federation of Law Societies of Canada (the Federation) to explore issues related to money laundering and terrorist financing in the legal profession and strengthen information sharing between law societies and the Government of Canada. The government will continue working with the Federation on this collaborative approach.

As the legal profession and law societies fall under provincial and territorial jurisdiction, the federal government will also consult with the governments of provinces and territories on AML/ATF issues in the legal profession. Additionally, the Departments of Finance and Justice will monitor the ongoing efforts of the province of British Columbia to modernize their framework for legal service providers and consult with the province and stakeholders if necessary for any matters related to the AML/ATF regulation of British Columbia notaries under the PCMLTFA.

3.3 – Civil Asset Forfeiture

The FATF calls for countries to adopt measures that allow authorities to seize or restrain laundered property, proceeds of crime, and funds used or intended for terrorist activities. The FATF also calls for measures authorizing forfeiture absent a criminal conviction to the extent that this approach to forfeiture is consistent with fundamental principles of domestic law, such as human rights or other constitutional obligations.

While the federal government is responsible for criminal forfeiture, provincial and territorial governments have jurisdiction over civil forfeiture in most cases. Both criminal and civil forfeiture regimes can act as powerful means to disrupt and deter crime. They can also serve to compensate crime victims and fund anti-crime initiatives.

Although Canada has criminal and civil forfeiture laws in place, the AML/ATF Regime has been criticized for giving insufficient priority to the forfeiture of proceeds of crime and offence-related property and failing to demonstrate results in this area. The federal government seeks to explore how governments can better use existing tools to seize and forfeit the proceeds of crime, and the potential need for new measures, such as unexplained wealth orders, while respecting the *Charter* and the constitutional division of powers.

Unexplained Wealth Orders

Unexplained wealth orders are court orders that compel a person to provide information about their interest in specific property, such as the nature and extent of their interest and the provenance of the property, where a designated government authority has established a suspicion that the property is associated with unlawful activity. If the person does not respond or does not account for the provenance of the property, this failure to account for the property could support an application for a civil forfeiture proceeding. It could establish a presumption that the property is associated with unlawful activity and eligible for forfeiture, which could be rebutted by the owner or a person with an interest in the property. Such measures have been adopted in the context of civil recovery schemes in other jurisdictions, including the United Kingdom and Australia.

The Cullen Commission's final report recommended the Government of British Columbia develop and integrate unexplained wealth order powers into its provincial civil forfeiture regime. The Government of British Columbia has passed legislative amendments to introduce an unexplained wealth order regime. Manitoba is currently the only other province in Canada whose civil forfeiture regime provides for a form of unexplained wealth order.

The federal government will hold further exchanges with provinces and territories on establishing unexplained wealth orders as part of their civil forfeiture regimes, and how to make better use of existing tools with the objective of increasing the forfeiture of proceeds of crime and other unlawful activity. The government also welcomes views on whether and how unexplained wealth order measures could be incorporated into the federal legislative framework, taking into consideration constitutional considerations.

Chapter 3 Discussion Questions

The government is seeking views on:

- How can different orders of government work together better to address money laundering and terrorist financing?
- How can different orders of government better collaborate and prioritize AML/ATF issues related to beneficial ownership, the legal profession, and civil forfeiture?
- Are there examples of successes in other jurisdictions that Canada should consider? Are there examples of approaches in other jurisdictions that Canada should avoid?
- Are there other areas or issues related to money laundering and terrorist financing that could benefit from greater federal, provincial, and territorial engagement?
- The government is seeking views on whether unexplained wealth order measures could be incorporated into the federal legislative framework. What could be the options? What would be the benefits? What would be the drawbacks?

Part II – Operational Effectiveness

The hallmark of an effective AML/ATF Regime is one that mitigates risks to which the country is exposed and delivers results commensurate to the risk level. A strong, comprehensive legislative and regulatory framework is foundational to this effort, but it must also be backed up by effective operational actions that target areas of greatest risk.

By certain metrics, Canada's AML/ATF Regime struggles to be effective. For instance, federal money laundering and terrorist financing charges, convictions, and forfeiture of proceeds of crime have all decreased over the past decade, which is not in line with Canada's risk profile. Both the FATF and the Cullen Commission criticized the AML/ATF Regime for its lack of operational effectiveness in these areas.

This section explores potential policy measures and changes to legislation to better support operational actions, including facilitating investigations and prosecutions into money laundering, terrorist financing, and associated criminal activity. Chapter 4 considers areas for possible criminal law reforms under the *Criminal Code* for which the Department of Justice seeks input including the seizure and forfeiture of proceeds of crime and digital assets and on the offence and sentencing for money laundering. Chapter 5 outlines considerations for a new Canada Financial Crimes Agency that would be Canada's lead enforcement agency in financial crimes. Chapters 6 considers enhancing information sharing to better facilitate the detection and disruption of money laundering and terrorist financing, while protecting privacy rights.

Chapter 4 – Criminal Justice Measures to Combat Money Laundering and Terrorist Financing

In addition to the issues highlighted elsewhere in this report where the Department of Justice is seeking input in coordination with other federal regime partners, the Department of Justice is seeking views on possible reforms to the *Criminal Code*, the *Canada Evidence Act*, and related measures that fall under the mandate of the Minister of Justice in this chapter.

4.1 – Investigation and Prosecution of the Offence of Laundering Proceeds of Crime

The offence of laundering proceeds of crime is set out at section 462.31 of the *Criminal Code*, which makes it an offence to deal with property or proceeds of property with the intent to convert or conceal the property, and knowing, believing or being reckless to the fact that the property was obtained through the commission of a designated offence in Canada or an act or omission outside of Canada, that if it had occurred in Canada, would have constituted a designated offence. A designated offence is any offence that may be prosecuted as an indictable offence and includes hybrid offences, with the exception of a small number of offences from eight federal statutes which have forfeiture provisions tailored to the subject matter of the statutes.

"Third party money laundering" (or launderer) (TPML) is the term used to describe the laundering of proceeds of crime as a service and for a fee, and where the launderer is generally not involved in the commission of the predicate offence. The TPML provides expertise to convert money or other form of property, or to conceal the nature, source, location, ownership, or control of property. They can rely on techniques including complex webs of transactions through various corporate vehicles and financial instruments, involvement in money service businesses (MSBs) or trade-based money laundering, engaging 'money mules' to structure financial transactions, or moving money through various cryptocurrencies and related applications. TPMLs may draw on the skills or influence of professionals, who may be unwittingly involved or complicit, or may belong themselves to a regulated sector or profession, or specialized area of business.

The FATF has found that many countries are not investigating and prosecuting third party or complex laundering of proceeds to the extent that it considers necessary in light of the ability of TPML to move large amounts of proceeds of crime through the international financial system, and the risks that this entails. However, while TPMLs may not be involved in the commission of the predicate offence, they are generally aware that the property that they move is not legitimate. Hence, prosecutions have demonstrated that the TPML was willfully blind to the fact that the property was proceeds of a specific predicate offence or had knowledge that the property was obtained from a type of predicate offence based on their clients' activities.

Investigations into laundering of proceeds of crime, particularly by TPMLs, can be complex and require specialized expertise. These factors can strain resources and budgets. Prosecutions also frequently require specialized skills and experience. In recent years, the Government of Canada has taken multiple actions to mitigate the risks of TPML. These include: new regulations targeting foreign MSBs and virtual asset service providers under the PCMLTFA; amendments to the *Criminal Code* to include a lower mental element of recklessness for the money laundering offence; the establishment of Integrated Money Laundering Investigative Teams under the RCMP; and the establishment of a Trade Fraud and Trade-Based Money Laundering Centre of Expertise at the CBSA. Budget 2023 also announced proposed legislative amendments to establish new offences in the PCMLTFA for structuring financial transactions to avoid triggering FINTRAC reporting and operating an unregistered MSB.

The Cullen Commission observed that the 2019 amendment to the laundering of proceeds offence in the *Criminal Code*, and the clarification by courts that the mental element of "belief" does not require establishing that the property was in fact derived from the commission of a designated offence[1] will be useful in prosecutions of TPMLs. The Cullen Commission also pointed to resourcing and prioritization challenges with law enforcement and prosecutors as the main challenge underlying the low rate of investigations and prosecutions of money laundering and made recommendations in this regard.

Nevertheless, some have called for additional reforms to address TPML, such as altering the requirement to establish a nexus between the predicate offence and the laundering or focusing only on particular typologies of money laundering.

The government is seeking views on approaches to the offence of laundering proceeds of crime:

- Should the offence of laundering proceeds of crime be amended to better address third-party money laundering, such as by altering the nexus required between the predicate offence and the laundering activity?
- What would such a reform look like from your perspective?
- What would be the benefits to such reforms?
- What would be the drawbacks to such reforms?
- Could operational approaches enhance outcomes? What would such approaches entail?
- Are efforts needed to enhance education, awareness, and reporting to authorities among at-risk groups and sectors to better address third-party money laundering?
- Is enhanced capacity building for criminal justice system participants needed to better address third-party money laundering? What could this look like?

[1] See, for example, R. v. Tejani, 1999 CanLII 3765 (ON CA).

4.2 – Offences for other Economically-Motivated Crime

Frauds of varying kinds have become a concern for Canadians, particularly in recent years. When perpetrators of fraudulent schemes are located in Canada, law enforcement may be able to pursue criminal charges. In other instances, perpetrators are difficult to trace or located outside Canada, often in jurisdictions where effective legal cooperation is difficult or impossible. In some instances, funds may be recovered and returned to victims; in others, the courts may order restitution or forfeiture following a conviction. However, losses are not always recoverable.

The *Criminal Code* contains a number of offences that can address fraudulent conduct. For example, section 342 applies to credit card theft, including possession, use or trafficking in credit card data. Section 342.1 applies to unauthorized uses of a computer, including use of a computer with intent to commit an offence, and criminalizes activities associated with computer "hacking", as does the criminal offence under section 430 (1.1). Section 345 applies to stopping a mail conveyance, which may be relevant to schemes relying on mail. There are also the offences of false pretence or false statement (section 362), obtaining execution of valuable security by fraud (section 363), as well as forgery and false information offences. There is the general fraud offence (section 380) which applies to a broad range of circumstances where an actor has perpetrated a dishonesty and a loss, or a risk of loss, and fraud affecting a public market (section 380(2)). Canada also criminalizes identity theft (section 402.2) and identity fraud (section 403).

The government has also put in place a number of targeted responses to activities that can be associated with telephone and online frauds. The Canadian Radio-Television and Telecommunications Commission (CRTC) regulates unsolicited telecommunications pursuant to section 41 of the *Telecommunications Act*. It has established Unsolicited Telecommunications Rules, including rules relating to "spoofing" caller identification by displaying inaccurate, false, or misleading information in an attempt to induce individuals to answer such calls. The CRTC can conduct compliance and enforcement actions and can issue administrative monetary penalties for violations of the Rules.

Separately, Canada's Anti-Spam Legislation (CASL)[2] contains prohibitions in relation to unsolicited commercial electronic messages (spam), computer programs installed without consent (e.g., unwanted software and malware) and unsolicited redirections (e.g., malicious interception of internet traffic). These elements of the CASL are also enforced by the CRTC through compliance and enforcement actions including administrative monetary penalties. Canada's Anti-Spam legislation also provided for the Office of the Privacy Commissioner to play a role in investigating email harvesting and spyware that collects personal information.[3]

While activities associated with activities such as "phishing" and "spoofing" are illegal in Canada under existing law, some have questioned whether there might be a benefit from enacting additional criminal offences relating to these activities. The scenario of concern is where fraudsters aim to obtain personal information from individuals through telephone, text, or online means to defraud their victims.

The government is seeking views on approaches to combating fraud:

- Would additional offences in the *Criminal Code* effectively contribute to combating fraud, notably through "phishing" or "spoofing"?
- What would be the benefits?
- What would be the shortcomings?

[2] *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act (S.C. 2010, c. 23)*

[3] More information on these efforts is available here: https://ised-isde.canada.ca/site/canada-anti-spam-legislation/en/understand-canadas-anti-spam-legislation/understand-canadas-anti-spam-legislation-sub/understanding-canadas-anti-spam-legislation

4.3 – Sentencing for Laundering Proceeds of Crime

The penalty for laundering proceeds of crime is a maximum of 10 years' imprisonment when prosecuted on indictment, and up to two years' imprisonment on summary conviction. Some have called for reforms to sentencing for money laundering, suggesting that there is little deterrence and little perceived incentive to investigate and prosecute money laundering. This is due to sentencing decisions that frequently impose short incarceration periods to be served concurrently with the sentence for other offences and is particularly the case when an offender is convicted of both a predicate offence and the laundering of proceeds.

However, others point to the totality principle of sentencing, which requires that a sentence not be excessive or exceed the overall culpability of the offender, and express concern that reliance on consecutive sentencing could result in lower sentences for individual offences to respect the totality principle. In addition, research shows that the likelihood of being caught and facing prosecution may be more effective deterrents of crime than longer sentences.

An option could be to add aggravating factors to the offence of laundering proceeds of crime, for instance where the value of the proceeds is particularly high, where the offender failed to comply with professional standards, or in other circumstances. Some have called for amendments to the *Criminal Code* to add laundering of proceeds of crime as an aggravating factor in sentencing in cases where the accused is successfully prosecuted for another designated offence but where laundering of proceeds of crime charges were not pressed or had to be dropped.

The government is seeking views on approaches to sentencing relating to the laundering of proceeds of crime:

- Should the government consider sentencing reforms for the offence of laundering proceeds of crime?
- What could this look like?
- What would be the benefits to such reforms?
- What would be the drawbacks to such reforms?

4.4 – Access to Subscriber Information under the *Criminal Code*

The 2014 decision of the Supreme Court of Canada in *R. v. Spencer*[4] significantly exacerbated the problems for police in obtaining access to information about subscribers such as name, address, phone number, and related account identifiers, such as an IP address. What constitutes "subscriber information" varies.

A tool similar to the targeted production orders in the *Criminal Code* that are available for transmission data, financial data, tracking data (associated with an object but not a person) and tracing information, all of which can be obtained when there are reasonable grounds to suspect, would be useful to investigators seeking subscriber information. As there is currently no tool to seek subscriber information, police must default to the general production order, at reasonable grounds to believe, which can be a challenging standard to meet at an early stage of an investigation. A related issue is that law enforcement has reported concern with the length of time provided in these orders for third parties to respond. The response time is usually set at 30 days to align with the timeframe provided in subsection 487.0193(2) for notice of an application for review of an order. In some circumstances, a 30-day wait time for a response to a narrow request, such as a request for subscriber information, can severely compromise the usefulness of the information. This delay can be compounded where several requests are submitted as an investigation proceeds and 30-day timelines multiply. Law enforcement have indicated the 30-day timeframe is common, even where consultation with the relevant entity has indicated an ability to respond in a relatively short timeline.

[4] R. *v.* SPENCER, 2014 SCC 43, [2014] 2 S.C.R. 212

Although the current Canadian legal landscape is closely similar to European Union countries, Canada's practices for access to subscriber information are somewhat out of step with those of many other allied countries, such as the United States, the United Kingdom, and Australia, which permit access to subscriber information without prior judicial approval and in short time frames.[5]

Previous governments have engaged in public consultations on this issue on several occasions. Prior to the Supreme Court decision in *R. v. Spencer*, successive governments brought forward, in multiple legislative proposals,[6] schemes for administrative oversight frameworks for access to subscriber information consistent with how such access is authorized in many other jurisdictions. These prior legislative proposals for access to subscriber information were criticized due to privacy concerns. Many commented their concerns arose from the administrative nature of the schemes and criticized the proposals for the lack of judicial oversight. These proposals were not ultimately enacted.

The government is seeking views on:

- Should the *Criminal Code* be amended to include an order for subscriber information?
- What should be the extent of information available through such an order?
- Should legislative solutions be explored to address the issues raised by law enforcement regarding turnaround times?
- What would be the benefits?
- What would be the challenges?

4.5 – Electronic Devices

Electronic devices such as mobile phones can present particular challenges in the investigation of serious offences. Issues arise from the reliance on authorities such as search warrants under section 487 of the *Criminal Code* for searches of mobile devices, as these provisions were not developed for the digital age or for the context of modern investigative search requirements. One area that gives rise to many issues is that mobile devices may contain a significant volume of information that is useful to law enforcement, including key evidence related to the criminal activity under investigation, making effective and timely access to the content of such devices a key tool for investigators to respond to criminal activity in a timely manner. At the same time, the extent of information contained in a mobile device raises important legal considerations, including privacy rights under section 8 of the *Charter*. Individuals frequently carry such a device on their person, which raises distinct questions in the execution of a search. For example, in *R. v. Vu*, the Supreme Court of Canada indicated that a warrant that specifically anticipates that the device will be examined for its data is needed to provide the necessary authority to examine the device for data.

[5] Member states of the European Union are bound by the decision of the European Court of Human Rights in *Benedik vs. Slovenia* (2014) regarding dynamic IP addresses. It is of note that the *Benedik* decision discusses Canada's R. v. Spencer in key details (paras. 68-72). Source: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-154288%22]}

[6] Bill C-74, the *Modernization of Investigative Techniques Act*, completed first reading on Nov.15, 2005 (38th Parliament, 1st Session) but died on the order paper. Bill C-47, *Technical Assistance for Law Enforcement in the 21st Century Act*, completed second reading on Oct.29, 2009 (40th Parliament, 2nd Session) and died on the order paper. Bill C-52, *Investigating and Preventing Criminal Electronic Communications Act*, completed first reading on Nov.1, 2010 (40th Parliament, 3rd Session) and died on the Order Paper. Bill C-30, *Protecting Children from Internet Predators Act*, completed first reading on Feb.14, 2012 (41st Parliament, 1st Session) and died on the Order Paper.

Subsection 11(5) of the *Controlled Drugs and Substances Act* (CDSA) authorizes a peace officer who executes a warrant issued under section 11(1) of that Act and who has reasonable grounds to believe that any person found in the place set out in the warrant has on their person a controlled substance, property or thing set out in the warrant, to search the person for the item without placing the person under arrest. Similar authority is found in s. 87(5) of the *Cannabis Act*. This power only provides for the search and seizure of the item named in the warrant and would not authorize a search of a device. A separate search warrant would be required to search the device.

The clarity provided by this provision does not exist in the context of a search conducted pursuant to a warrant under section 487 of the *Criminal Code*, which, as noted above, has become challenging in some respects as a tool for modern investigations. A new authority along the lines of the search authority in the CDSA and the *Cannabis Act* could aim to address this one area where some questions have been raised as to whether a search warrant under section 487 provides sufficient authority for police to seize a phone where the warrant authorized police to be in that place for the purpose of searching for and seizing that phone, if the phone is in the person's hand or pocket.

Solicitor-Client Privilege and Electronic Devices

In the *Lavallee* decision,[7] the Supreme Court of Canada concluded that section 488.1 of the *Criminal Code*, which sets out a procedure for determining a claim of solicitor-client privilege in relation to documents seized from a law office under a warrant, constituted an unreasonable search and seizure under section 8 of the *Charter*. The Supreme Court of Canada concluded that the section could not be saved under section 1 as it results in more than a minimal impairment of solicitor-client privilege. The Supreme Court of Canada provided a set of ten principles to guide Parliament in legislating searches of law offices in order to adequately protect solicitor-client privilege, and the courts have developed similar principles relating to investigatory techniques such as wiretaps where communications protected by solicitor-client privilege may be involved (*Doiron v. R.*, 2007 NBCA 41, *R. c. Robillard*, 2000 CanLII 6756 (QC CA)). The *Lavallee* principles have not been codified by Parliament, but they have been used in practice since the 2002 Supreme Court of Canada decision.

Some have expressed concerns that the current framework, using a referee to review and manage any material on electronic devices that is protected by solicitor-client privilege, is unwieldy and time-consuming. There are concerns that charges may be stayed for delay as a result. There are also concerns that such processes are similarly time-consuming and challenging where an extensive amount of documents are involved but that do not involve electronic devices.

[7] *Lavallee, Rackel & Heintz v. Canada (Attorney General)*; *White, Ottenheimer & Baker v. Canada (Attorney General)*; *R. v. Fink*, 2002 SCC 61 (CanLII), [2002] 3 SCR 209.

The government is seeking views on:

- Should the Criminal Code be amended to provide explicitly for the inclusion of a power to search a person for a thing or property set out in a warrant under section 487 or under section 462.32 where the peace officer has reasonable grounds to believe that the person has the thing on their person?
  - What would be the benefits?
  - What would be the drawbacks?
- What are options to facilitate searches of electronic devices where there is a concern that such a device may contain material protected by solicitor-client privilege, that would meet the constitutional protections afforded to such material?
- Is there a need to consider options for searches involving other forms of materials that may be protected by solicitor-client privilege?
  - What would be the benefits?
  - What would be the drawbacks?

4.6 – Digital Assets and Related Challenges

Cryptocurrency and other digital assets can be attractive to perpetrators of crime for their pseudonymity and easy and rapid movement, including through service providers that operate outside the sphere of regulatory obligations. Questions outlined within this chapter regarding the rapid seizure and restraint of property that may be forfeited as proceeds of crime are particularly important for dealing with digital assets.

While attention has been given to the importance of seizing cryptocurrency for eventual forfeiture as proceeds of crime, it may be important to consider whether amendments to the *Criminal Code* are required to respond to other challenges relating to digital assets. Examples may include establishing that an accused was in control of a digital asset for asset tracing purposes or to establish liability for a financial crime, or to preserve emerging forms of digital assets whose value may primarily be evidentiary, such as non-fungible tokens.

Blockchain records

Blockchains have been described as databases or ledgers shared among a computer network's nodes, known for maintaining a secure, unalterable, and decentralized record of transactions undertaken on a particular blockchain. However, they have broader uses, and can maintain logs of information or transactions involving other digital assets. Given their generally immutable nature, there is interest in their evidentiary role in proving transactions between parties and the timing of particular events, for example.[8]

The *Canada Evidence Act* establishes certain rules of evidence in court proceedings relating to federal law and codifies common law rules in many respects. It includes a number of provisions that may be relevant to blockchain records, including in relation to books and documents and admissibility.

[8] Bitcoin, Not Blockchain for Governments Everywhere, Pulat Yunusov, Selected Slaw columns from 2016-2019 2021 CanLIIDocs 352

Production of information related to digital assets

Many cryptocurrency users rely on centralized exchanges to maintain and manage their cryptocurrency holdings, transactions, and private key information. Such exchanges share some characteristics with conventional financial institutions that provide banking services in that they maintain cryptocurrency accounts for clients, which clients can use for holding and transacting in cryptocurrencies. It may be necessary in the course of an investigation to obtain information from a centralized exchange that is similar to the information that can be obtained through *Criminal Code* production orders (e.g., section 487.018), relating to an account holder or an account. Some have indicated that centralized exchanges for cryptocurrency are willing to engage with law enforcement and are responsive to court orders for information. Others question whether existing production order provisions, e.g., section 487.018, can apply to data[9] held by centralized exchanges based on its current wording.

Decentralized services

Decentralized financial services typically consist of financial products and services that operate on decentralized platforms using blockchains to record and share data. They generally operate through automated protocols and as such, they can present special challenges in the investigation of crime. These include the fact it can be difficult to locate a central entity upon which judicial authorizations to disclose information or restrain property may be served. This is a challenge facing law enforcement in multiple jurisdictions. However, law enforcement in some jurisdictions are finding that a number of decentralized services may in fact rely on centralized entities or persons on whom court orders may be served.

The government is seeking views on amendments to the *Criminal Code* in relation to challenges posed by digital assets, including as follows:

- Should the *Criminal Code* be amended to better enable the seizure and restraint of digital assets including cryptocurrency for evidentiary purposes or as offence-related property?
- Are other measures needed?
- Is there a need to amend the *Canada Evidence Act* to provide for the admissibility of blockchain data as evidence? Is blockchain data already covered by existing rules?
- Should the *Canada Evidence Act* be amended so that the authenticity of records created using blockchain technology may be presumed? In what circumstances could this be presumed? Are existing rules adequate for this purpose?
- Can information be obtained from centralized exchanges through existing production order provisions? Should amendments be considered?
- What would be the benefits of the above reforms?
- What would be the drawbacks?

[9] Account number of a person named in the order or name of the person for an account number included in the order; type or status of an account, or date on when an account was opened or closed.

4.7 – Pre-Trial Seizure and Restraint of Property Associated with Crime

The confiscation of proceeds of crime is considered an important means to disrupt and discourage organized crime and the commission of economically-motivated crimes. The FATF is highlighting the importance of early seizure and restraint powers in achieving better outcomes for the recovery of proceeds of crime, while the Cullen Commission recommended that agencies involved in the investigation of profit-oriented crime be given the skills and knowledge to identify assets for seizure and/or restraint and forfeiture. Currently, the provisions for seizure and restraint of property that may be forfeited as proceeds of crime, at sections 462.32 and 462.33, respectively, of the *Criminal Code,* require an application to a judge by the Attorney General of Canada or the Attorney General of the province in which the proceedings are taken. This step ensures that due consideration is given to the likelihood that an order of forfeiture may be made in respect of property seized or restrained. However, it can also lead to delays in obtaining a warrant or order, resulting in property being moved beyond the reach of law enforcement.

The risk of dissipation of property believed to be proceeds of crime is a challenge across many types of property, but the risk is particularly acute in the case of digital assets, such as cryptocurrency, which can be moved extremely quickly. This makes the need to be able to seize or restrain these assets in a timely manner, in appropriate circumstances, an important consideration in recovering proceeds of crime.

Measures available in a faster manner to restrain or seize property believed to be proceeds of crime may contribute to strengthening Canada's ability to investigate money laundering and proceeds of crime and to confiscate criminals' ill-gotten gains. An option could be to enable a peace officer to apply directly to a justice of the peace or judge for an interim seizure or restraint order, in a manner that would complement existing measures and processes, including the role of the Attorney General in seeking a special warrant or restraint order. Appropriate safeguards to protect the interests of affected persons and ensure consistency with the *Charter* must be considered.

In addition to concerns regarding delay, the special search and seizure and restraint provisions for proceeds of crime require an undertaking by the Attorney General in relation to damage caused by the execution of the warrant or order. Some provincial Attorneys General are reluctant to apply for seizure or restraint of proceeds of crime as a result of this undertaking or maintain operational procedures which may restrict the use of these tools and limit the recovery of proceeds of crime for possible forfeiture.

The government is seeking views on approaches to enhance the pre-trial preservation of proceeds of crime for possible forfeiture under the *Criminal Code*.

- Should the *Criminal Code* be amended to enable a peace officer to apply directly to a justice of the peace or judge for an interim seizure or restraint order?
- Are there are other measures that could facilitate preservation of proceeds of crime under the *Criminal Code*?
- What would be the benefits to such reforms?
- What would be the drawbacks?

4.8 – Criminal Forfeiture

Criminal forfeiture occurs when a convicted offender is permanently deprived of property that was involved in the commission of an offence (offence-related property) or obtained or derived from the commission of an offence (proceeds of crime), following their conviction and at the same time as sentencing.

Criminal forfeiture is an important aspect of the government's efforts against money laundering and organized crime, as it seeks to ensure that "crime doesn't pay" and to disrupt and deter organized and serious crime. Forfeiture of property associated with crime more broadly is also a priority area of work internationally, as pronounced in the April 2022 Declaration of the Ministers of the FATF, which was endorsed by Canada.

After reviewing the criminal forfeiture regime in Canada, the Cullen Commission observed that Canada has "powerful but underutilized tools that have the potential to disrupt and deter organized crime groups and others involved in serious criminal activity," and that it can provide efficiencies and the opportunity for forfeiture of property beyond the scope of a civil forfeiture action. It recommended that more attention be paid to criminal forfeiture in the context of criminal investigations and prosecutions.

One of the tools considered by the Commission was "rebuttable presumption" forfeiture scheme at section 462.37(2.01-2.07) of the *Criminal Code*. This scheme was adopted by Parliament in 2005. This scheme may only be applied where an offender is convicted of criminal organization offences punishable by five or more years' imprisonment, or certain drug offences under the *Controlled Drugs and Substances Act* or the *Cannabis Act*. Under this scheme, a forfeiture order may be made in relation to any property identified in an application by the relevant Attorney General, where the court is satisfied on a balance of probabilities that the offender has engaged in a pattern of criminal activity for the purpose of providing the offender with material benefit, or that income of the offender unrelated to crime cannot reasonably account for the offender's wealth. However, the court shall not make a forfeiture order if the offender demonstrates, also on a balance of probabilities, that the property identified by the Attorney General is not proceeds of crime. If the offender does not rebut the presumption, the property is forfeited. A court may set a limit on the total amount of property forfeited as may be required by the interests of justice.

The scheme includes multiple safeguards to protect the interests of the offender. These include the limited scope of application of the provision to criminal lifestyle and organized crime offences, where a strong connection can be made between the conviction for the underlying offence and the presumption that the assets of the offender are proceeds of crime, the evidentiary burden on the prosecution to establish a pattern of criminal activity or property that exceeds the value of lawfully earned income and the property sought for forfeiture, and the offender's ability to rebut the presumption that the property is proceeds of crime and the court's discretion to limit the property forfeited. This provision has not been frequently used and has not been subject to a *Charter* challenge. Any consideration of expansion to additional offences would need to carefully consider the *Charter* implications.

The government is seeking views on the following:

- Should the scope of the rebuttable presumption provision in the *Criminal Code* be expanded to include a number of additional profit-oriented offences, such as laundering proceeds of crime and major fraud or extortion on the basis that these offences are increasingly associated with a criminal lifestyle, and to recognize the serious societal harms they represent in their own right? Should other offences be contemplated?
- Should minimum thresholds apply, such as a dollar value, the minimum number of victims, or similar, or is the Crown's obligation to establish a pattern of criminal activity or income that exceeds lawful sources in the rebuttable presumption provisions sufficient?
- What other measures could be considered to enhance the criminal forfeiture of proceeds of crime?
- What would be the benefits to such reforms?
- What would be the drawbacks?

4.9 – Intelligence and Evidence

Financial crime cases are complex. These proceedings often produce large quantities of documentary evidence, which must be appropriately handled and disclosed in accordance with fair trial rights as protected by the *Charter* and decisions of the Supreme Court of Canada.

There are also important considerations around protecting intelligence and sensitive information from public disclosure when it is used to inform criminal investigations and prosecutions. The *Canada Evidence Act* sets out a framework for protecting sensitive information from disclosure in court proceedings when doing so would be contrary to the public interest or injurious to international relations, national defence, or national security. Under this framework, the Federal Court ultimately determines, based on public interest, whether the information should be disclosed or protected from disclosure in proceedings. However, protecting sensitive information from disclosure means it may not be able to be relied upon in a particular case to support or defend a decision taken by the government or as evidence in a civil or criminal proceeding. In criminal cases, the non-disclosure of information could lead to a stay of criminal charges, and in civil or administrative cases it could lead to adverse outcomes for the government in the form of an inability to defend a particular decision or the settling of claims against the Crown.

The issue of intelligence and evidence impacts upon a range of national security issues, The government is currently working to explore solutions to facilitate the use of evidence in national security-related cases. Intelligence, particularly financial intelligence, may also be relevant to money laundering or terrorist financing proceedings. AML/ATF Regime partners will participate in any future initiatives related to intelligence and evidence legislative reform, recognizing that challenges in this area have broad impacts upon national security, beyond those relating to money laundering and terrorist financing.

The government is seeking views on the following:

- How could the legislative framework governing the protection and use of sensitive intelligence and information during court proceedings in relation to money laundering and terrorist financing be improved?
- What would be the benefits to such reforms?
- What would be the drawbacks?

4.10 – Criminal Jurisdiction

The general rule regarding inter-provincial jurisdiction is that a Canadian court does not have jurisdiction to try an offence committed entirely in another province (subsection 478(1) of the *Criminal Code*). There are provisions in the *Criminal Code* to address the situation where an offence may be deemed to have occurred in more than one province.

With respect to extraterritorial jurisdiction, the term refers to the competence of a state to make (prescriptive jurisdiction), apply (adjudicative jurisdiction) and enforce (enforcement jurisdiction) laws in respect of persons, property, or events beyond its territory. General principles of international law govern the exercise of extraterritorial jurisdiction in any of the three categories. Central among these is the principle of territoriality, whereby the territorial state has the strongest claim for exercising jurisdiction, as well as the principles of sovereign equality, independence, and non-interference. Further, of these three categories, extraterritorial enforcement jurisdiction (any investigative action with a coercive or intrusive aspect, such as a search or seizure) is associated with the strongest constraints.

The principle of territoriality is codified at section 6 of the *Criminal Code* and is grounded in international comity and principles of international law. Canada's policy has been to assert extraterritorial prescriptive and adjudicative jurisdiction only when there are treaty obligations to do so. Such treaties generally include obligations for international cooperation relating to evidence and other matters required for investigation and prosecution. Consistent with Canada's treaty obligations, section 7 of the *Criminal Code* establishes extraterritorial jurisdiction over offences including money laundering, corruption and foreign bribery, organized crime, human trafficking, and similar conduct. However, Canada does not currently have treaty obligations that provide for the assertion of extraterritorial jurisdiction in relation to cybercrimes, particularly cybercrimes associated with proceeds of crime, such as cyber fraud or ransomware attacks. Nonetheless, Canada may assert jurisdiction based on the common law *Libman* test where an offence is committed in multiple states. The *Libman* test for establishing when a Canadian court may validly exercise territorial jurisdiction over a criminal offence consists of two parts: (1) there must be a "real and substantial link" between Canada and the offence (that is, a significant portion of the activities constituting the offence needs to have occurred in Canada); and (2) it is necessary to consider whether or not anything in those facts would offend against international comity.

Canada's offence of laundering proceeds of crime enables Canada to investigate and prosecute the laundering of proceeds of crime where the property laundered was obtained or derived, directly or indirectly, from the commission of an offence outside Canada that would be a designated offence if it occurred in Canada. This approach enables Canada to investigate and prosecute money laundering in Canada, even where the predicate offence giving rise to the proceeds of crime was committed outside Canada. This provision implements Canada's international obligations under several anti-crime conventions.

The government is seeking views on the following:

- Are reforms to jurisdiction elements of the laundering of proceeds of crime offence needed?
- Should the law be amended so that the issuance by judges of production orders in Canada - where such orders may apply to entities that operate in the digital realm both within and outside of Canada and over whom Canada may seek to exercise jurisdiction in the context of such orders even where these entities are known to be primarily headquartered outside of Canada - be explicitly set out in statute notwithstanding inherent limitations of such orders?
- What would be the benefits to such reforms?
- What would be the drawbacks?

4.11 – Keep Open Accounts Under Investigation

Personal financial account information held by financial institutions can provide valuable intelligence to law enforcement investigations when obtained in an appropriate and lawful manner, such as a production order or warrant. Financial institutions may close an account when becoming aware the account holder is the subject of an investigation. However, this may inadvertently disrupt an investigation by prematurely ending a potential ongoing source of information or result in the subject of the investigation being alerted to the interest of law enforcement.

The Cullen Commission's final report recommended implementing a formal "keep open" regime for financial institutions in which they can, at the request of law enforcement, keep an account suspected of involvement in money laundering open to further a law enforcement investigation.

There are many considerations over how a "keep open" regime would operate, including under what circumstances law enforcement would make a "keep open" request, the discretion of financial institutions to accept or deny the request, whether legal and reputational protections are required for financial institutions that comply with the request, and ensuring privacy protections are maintained between clients of the financial institution and the law enforcement agency making the "keep open" request.

One option could be to include a keep open regime power in the *Criminal Code*, available to law enforcement on prior judicial authorization. The issuance of a keep open order by the courts could reduce legal and reputational risks for financial institutions.

The government is seeking views on implementing a formal "keep open" regime, noting the considerations listed above.

- Should a legislated "keep-open" regime be implemented?
- How should such a regime operate vis-à-vis circumstances under which law enforcement would make a "keep open" request, the discretion of financial institutions to accept or deny the request, whether legal and reputational protections are required for financial institutions that comply with the request, and ensuring privacy rights are protected?
- What would be the benefits to such reforms?
- What would be the drawbacks?

Chapter 5 – Canada Financial Crimes Agency

Against the backdrop of low and declining rates of money laundering investigations and prosecutions, and low recovery of the proceeds of crime, the government recognizes that legislative changes alone will not improve the operational effectiveness of Canada's AML/ATF Regime. Indeed, Canada already possesses a strong and comprehensive legislative framework that, for the most part, provides law enforcement and operational partners with tools to disrupt financial crimes. To improve AML/ATF results, Canada must prioritize and provide dedicated resources and expertise towards pursuing complex money laundering investigations, prosecutions, and asset recovery, including cases of third-party money laundering.

One step in this direction is the government's commitment to create a new, dedicated lead enforcement agency: the Canada Financial Crimes Agency (CFCA). In his 2021 Mandate Letter, the Minister of Public Safety, supported by the Minister of Justice and Attorney General of Canada and the Deputy Prime Minister and Minister of Finance, was tasked by the Prime Minister to bring forward a proposal for the establishment of a CFCA whose sole purpose will be to investigate major financial crimes. Shortly thereafter, Budget 2022 reiterated the commitment and clarified that the CFCA would be Canada's lead enforcement agency in financial crimes. Budget 2022 also provided $2 million to Public Safety Canada to undertake initial work to develop and design the new agency.

Ongoing development and design work will ensure that the CFCA becomes an effective lead enforcement agency for Canada in financial crime, while enhancing operational effectiveness and protecting Canada's economic integrity in the process. Budget 2023 announced the CFCA would in part "bring together expertise necessary to increase money laundering charges, prosecutions and convictions, and asset forfeiture results in Canada", and that further details on the structure and mandate of the CFCA will be provided by the 2023 fall economic and fiscal update.

International Comparisons

Examples of countries with dedicated financial crime units with enforcement and/or coordination functions:

- **United Kingdom – National Economic Crime Centre**, housed within the National Crime Agency. Coordinates national response to economic crime by bringing together law enforcement and justice agencies, government departments, regulatory bodies, and the private sector. Membership includes the Joint Money Laundering Intelligence Taskforce, a public-private partnership between law enforcement and the financial sector.
- **United Kingdom – Serious Fraud Office**. Specialist government department that investigates and prosecutes serious and complex fraud, bribery, and corruption.
- **United States** – **El Dorado Task Force.** This Task Force consists of officials from over 30 law enforcement agencies in New York and New Jersey. It targets a range of complex financial crimes, including securities and investment scams, cyber and cryptocurrency schemes, corruption, and frauds against the United States financial system.
- **Italy – Guardia di Finanzia**. A police force reporting to the Ministry of Economy and Finance with strategic focus on financial crimes such as money laundering, tax evasion, public expenditure offences.
- **The Netherlands – Serious Crime Task Force**. Public-private partnership that seeks to target the financial facilitators that enable organized crime networks' ability to finance their operations.
- **Australia – Serious Financial Crime Taskforce**. Australian Tax Office-led joint taskforce working to identify and tackle serious and complex financial crime, with focus on offshore tax evasion, cybercrime affecting tax system, and illegal phoenix activity (trade through successive insolvent companies).
- **Australia – Taskforce Avarus**. This taskforce brings together officials from the Australian Federal Police, the Australian Transaction Reports and Analysis Centre, the Australian Criminal Intelligence Commission, and the Australian Border Force to investigate complex money laundering cases.
- **Germany – Federal Authority for Fighting Financial Crime.** Initiative to create a new anti-money laundering authority in Germany that will also be responsible for enforcing international sanctions. Germany's existing anti-money laundering agency will be integrated into the new authority.

5.1 – The Mandate and Structure of the Canada Financial Crimes Agency

A core consideration of the development of the CFCA is the scope of its mandate, and in particular, the crimes or threats it will focus on. There are a wide range of crimes and threats that could be considered financial crimes. For example, a number of offences commonly known as white-collar crimes are financial in nature. They can include various types of fraud, market-related offences such as securities and investment crimes, public corruption and bribery, and competition offences. There are also fiscal crimes, which relate to seeking to evade taxes and duties, such as tax evasion and customs offences, as well as regulatory offences that address financial misconduct.

In addition, many profit-motivated crimes, such as human trafficking, drug trafficking, tobacco smuggling and trafficking, and environment and wildlife offences, generate proceeds of crime for criminal groups, which they may seek to keep for themselves or leverage for further criminal activity. To facilitate these actions, criminals must often engage in money laundering to disguise the origin of the proceeds and integrate them into the legal economy, thus evading detection. In fact, some of the top offences that generate proceeds (i.e., predicate offences) for money laundering are crimes such as fraud, tax evasion, and customs offences. The need for criminals to launder their proceeds of crime has led to the development of more sophisticated typologies. These include third-party money laundering and trade-based money laundering.

There are also important linkages to national security. For example, there are economic-based threats to national security whereby potentially hostile foreign actors gain access to sensitive technology, critical infrastructure, and the sensitive personal data of Canadians by exploiting pathways into the Canadian economy via the financial sector, trade, and investment or research partnerships with academics. Such threats can also finance the acquisition of technology necessary for the creation of Weapons of Mass Destruction or other threats to Canada and its allies, also known as proliferation financing. There has also been a recent heightened awareness of sanctions evasion, given the global sanctions imposed on Russia in response to its invasion of Ukraine. The government also continues to remain vigilant against threats posed by terrorism and terrorist financing.

A second core consideration for the CFCA is its structure. There are numerous examples internationally of specialized financial crime enforcement agencies that comprise various structures. Such models could include:

- **Sub-Agency** models, whereby a specialized section or office is created within an existing organization. An example of this is the National Economic Crime Centre in the United Kingdom. Such structures can allow the sub-agency to leverage the supports, resources, and expertise of the hosting organization, but may also contribute to potential competing priorities with other areas in the hosting organization.
- **Dedicated Agency** models, whereby a separate, specialized agency or department is created to achieve the desired outcome and have the component resources and authorities to do so. An example of this model is the Guardia di Finanza in Italy. These structures can allow the entity to better focus its resources in achieving its mandate but can be more complex to establish.
- **Inter-Agency** models, which seek to incorporate resources and expertise from a variety of implicated organizations. An example of this approach is the Serious Financial Crime Task Force in Australia. These structures can leverage synergies and allow for a more holistic approach to tackling complex issues but can face challenges in coordination and prioritization.

While not an exhaustive list of all possible offences and possible structures, the above examples illustrate the range of criminal activities and organizational models that could be taken into consideration for the CFCA.

The government is seeking views on the mandate of the CFCA, specifically:

- Should the mandate of the CFCA include combatting fraud?
- Should the mandate of the CFCA include combatting sanctions evasion?
- Should the mandate of the CFCA include combatting fiscal crimes (e.g., tax evasion)?
- Are there other crimes that should be included in the CFCA's mandate? For example, corruption, markets-based offences, terrorist financing, etc.

The government is seeking input on how a CFCA should be structured to enable more effective investigation, prosecution, and recovery of proceeds of crime.

5.2 – Core Elements of Effective Financial Crime Enforcement

In addition to its mandate and structure, it is essential that the CFCA have the appropriate tools, authorities, and resources to conduct effective enforcement to counter financial crime. There are four key aspects to financial crime enforcement: intelligence, investigation, prosecution, and recovery of the proceeds of crime.

Intelligence is the starting point for many enforcement actions. In the financial crime space this can include financial intelligence such as disclosures from FINTRAC, criminal intelligence from police and other law enforcement bodies, human intelligence from sources such as undercover operations and whistleblowers, and foreign intelligence from Canada's partners and allies abroad. An effective financial crime enforcement agency needs to be able to receive intelligence from multiple sources, analyze it efficiently, leverage it to inform further actions, and disclose to partners where necessary.

Investigation involves pursuing leads, often generated by intelligence, to determine which, if any, criminal offences have occurred. Financial crime investigations can often be complex and time-consuming, requiring timely information access and subject matter expertise. In addition, while investigation of *Criminal Code* offences is generally conducted by federal, provincial, and municipal police, there are other bodies in the financial crime space such as the Canada Revenue Agency, Competition Bureau, and Canada Border Services Agency that investigate offences specific to their mandates. Effective investigation thus requires the right legal authorities to access and share information, and to coordinate with other law enforcement bodies. Information sharing in this context needs to be done in a manner that complies with privacy legislation and the *Charter*.

If an investigation reveals sufficient evidence of a crime, charges may be laid, and prosecution authorities can pursue these charges in court. These measures are crucial to ensure that criminals are punished, the law is upheld, and other potential criminal activities are deterred. Since many financial crime investigations can be complex, it is important that investigators have ready access to advice from prosecution authorities. Financial crime prosecutions can be lengthy and require significant evidence disclosure management in a timely fashion to ensure not only that the accused receives the disclosure to which they are entitled, but also that criminal trials take place within a reasonable time, as protected by the *Charter*.

Finally, following conviction, criminal forfeiture is important to ensure that the profits are being taken out of financial crime. As financial crimes are generally both profit-motivated and feature the use of financial assets and techniques, they frequently generate significant proceeds of crime. Therefore, it is imperative that any effective enforcement strategy ensure that property obtained by crime, whether directly or indirectly – such as cash, cars, houses, and luxury goods – is identified and the subject of an application for forfeiture before the court. This acts as a deterrent and helps prevent such property from financing further criminality. However, much like investigations and prosecutions, effectively identifying, tracing, and proving that property is the proceeds of crime can be complex and lengthy. Criminals may be particularly adept at leveraging their skills to disguise the source and their ownership of property obtained from the commission of a crime.

As financial crime becomes an increasing global threat, the development of a CFCA marks a significant step forward in increasing Canada's ability to respond to this development and protect Canadians. The government is committed to taking into account the views of public and private stakeholders, businesses, and Canadians on how best to design and structure the agency so it can fulfill its important mission.

The government is seeking views on the core activities and functions of the CFCA, including:

- What tools or programs (e.g., legal authorities, organizational policies, technological solutions, whistleblower programs) should be provided to the CFCA to ensure it obtains the information required to conduct effective financial crime enforcement?
- How can the CFCA best attract, develop, and/or retain the expertise required to conduct financial crime investigations, enable prosecutions, and enhance criminal forfeiture?
- Should the CFCA hire or house officials from other AML/ATF Regime partners, such as FINTRAC, RCMP, CSIS, and potentially others?
- What types of public outreach (e.g., research, awareness campaigns, public-private partnerships) should the CFCA engage in to help keep Canadians safe from financial crime threats?

Chapter 6 – Information Sharing

While protecting the privacy rights of Canadians is necessary, secure and timely information sharing between public and private sector entities can facilitate more targeted detection and disruption of illicit activities related to money laundering and terrorist financing, ultimately enhancing the effectiveness of the AML/ATF Regime. There is a need for safeguards against the unrestricted flow of information to protect Canadians' rights and privacy, while maintaining the ability to share the information necessary to protect the financial security of Canadians and Canada's financial system.

Technology continues to enable more information to be shared, and faster. While the use of technology is not without risk, it can also offer solutions to help enhance data protection, while enabling the information important to combatting financial crimes to be shared.

Section 8 of the *Charter* enshrines privacy rights as protection from unreasonable search or seizure by the state, and protects reasonable expectations of privacy. To be consistent with section 8, laws authorizing actions that interfere with reasonable expectations of privacy must reasonably strike a balance between privacy interests and the state interest being pursued. Additionally, Canada has two federal privacy laws:

- the *Privacy Act*, which covers how the federal government handles personal information; and,
- the *Personal Information Protection and Electronic Documents Act* (PIPEDA), which covers how businesses handle personal information.

The *Privacy Act* sets out several core protections relevant to information sharing, namely that the government can only collect personal information that relates directly to one of its operating programs or activities and that the government may only use the personal information for the purposes that it collected it, or for a use consistent with that purpose.

PIPEDA sets the rules for how private-sector organizations collect, use, and disclose personal information in the course of for-profit, commercial activities across Canada. It also applies to the personal information of employees of federally regulated businesses. Similar to information protections under the *Privacy Act*, PIPEDA is concerned with ensuring that use of personal information is done so in an informed and consensual manner.

Types of information sharing may be separated into private-to-private, public-to-private, and public-to-public. This section considers options to enhance each of these types of information sharing for AML/ATF purposes.

6.1 – Private-to-Private Information Sharing

The FATF has observed that with the emergence of fintechs and other new market participants to the banking sector, customers are moving away from traditional financial services and using multiple institutions, instead of banking with a single financial institution with a large market share. This means data about individual customers is becoming increasingly dispersed across a wide array of institutions, making it more difficult to gain AML/ATF insights based on the data available to a single institution.

Criminals can take advantage of a lack of information sharing between reporting entities and may attempt to engage with multiple institutions to facilitate illicit activities, where each institution only has a limited and partial view of transactions. Reporting entities are thus limited in their ability to identify and report potential money laundering or terrorist financing activities. Enhanced private-to-private information sharing can help reporting entities more accurately assess customer risks or identify potential suspicious activity.

Other jurisdictions have implemented changes to their AML/ATF frameworks to promote greater information sharing between reporting entities. The United States provides financial institutions with the ability to share information with one another, under a safe harbour provision in legislation that offers protections from liability, in order to better identify and report activities that may involve money laundering or terrorist activities. Similarly, the United Kingdom allows regulated entities to share information with one another, on a voluntary basis, in relation to a suspicion that a person is engaged in money laundering or terrorist financing Both jurisdictions have implemented regulatory parameters to safeguard personal information.

In Canada, the statutory framework for private-to-private information sharing is more limited. It stems from paragraphs 7(3)(d.1) and (d.2) in PIPEDA, which permits the exchange of personal information by organizations without informed consent for the purposes of a criminal investigation or preventing fraud. These provisions are not prescriptive. Rather, they allow disclosures without consent where it may be appropriate. Reporting entities have generally viewed the statutory framework in Canada as insufficient for promoting information sharing for AML/ATF purposes.

The government is exploring options to enhance private-to-private information sharing as a tool to identify and disrupt money laundering and terrorist financing activities, including building off of the PIPEDA exceptions to consent while expanding the robustness and controls of the information sharing framework under the PCMLTFA, recognizing the potential privacy and data governance implications. The 2018 Parliamentary Review recommended: "That the Government of Canada consider tabling legislation that would allow information that is limited to AML/ATF subject matter to be shared between federally regulated financial institutions such as banks and trust companies, provided that FINTRAC is notified upon each occurrence of such sharing" (Recommendation 18). Under any approach, it will be essential to respect the foundational objectives of privacy protections in Canada.

The government is seeking views on the potential expansion of a framework for private-to-private information sharing for AML/ATF purposes, and is seeking feedback on the following:

- What types of information would be most valuable to share amongst reporting entities to detect, disrupt, and facilitate prosecution of money laundering and terrorist financing offences?
- Are there specific tools, mechanisms, or models from other jurisdictions that could be incorporated into Canadian legislation to support greater information sharing?
- What guardrails would best protect personal information while allowing for additional information to be exchanged between organizations?
- Are there opportunities to leverage technology to enhance information while protecting personal information?

6.2 – Public-to-Private Information Sharing

Canada's AML/ATF Regime enables public-to-private information sharing between federal entities and the private sector by requiring reporting entities to provide prescribed information to FINTRAC. This is critical for combatting financial crime, as information reported to FINTRAC is analyzed and distilled into financial intelligence that, when legislative thresholds are met, can be disclosed to support domestic and international partners in the investigation and prosecution of money laundering and terrorist financing related offences.

Example from the United Kingdom

The United Kingdom's Joint Money Laundering Intelligence Taskforce (JMLIT) is a partnership between law enforcement and over 40 financial institutions to exchange and analyse information relating to money laundering and wider economic threats. Since its inception, JMLIT has supported and developed over 950 law enforcement investigations, which has directly contributed to over 280 arrests and the seizure or restraint of over £86 million.

Through this collaboration, JMLIT private sector members have identified over 7,400 suspect accounts linked to money laundering activity, and commenced over 6,000 of their own internal investigations, while also continuing to develop and enhance their systems and controls for mitigating the threat of financial crime.

Example from Australia

Australia's Fintel Alliance is an Australian Transaction Reports and Analysis Centre initiative established in 2017 to increase the resilience of the financial sector to criminal exploitation and support law enforcement investigations into serious crime and national security matters. Fintel Alliance brings together experts from a range of organizations involved in the fight against money laundering, terrorism financing, and other serious crime. Fintel Alliance partners include major banks, remittance service providers and gambling operators, as well as law enforcement and security agencies from Australia and overseas. Working together, Fintel Alliance develops shared intelligence and delivers innovative solutions to detect, disrupt, and prevent serious crime.

In 2021-22, Fintel Alliance provided 343 intelligence products to law enforcement and intelligence agencies and identified significant fraud involving AUS 850 million in potentially fraudulent payments, among other accomplishments.

Sharing Information Between FINTRAC and Reporting Entities

Increasing two-way communication between FINTRAC and reporting entities could help provide clearer direction and assist reporting entities with their reporting obligations. As reporting entities increasingly make use of technology and rely on automated processes to identify unusual transactions, allowing FINTRAC to provide feedback on the value and utility of reports received is increasingly valuable for the private sector.

The Department of Finance is also interested in reviewing current policy and legislation regarding the ability of FINTRAC to request additional information from reporting entities when and if needed to perform its analysis of suspected money laundering and terrorist financing. This would build off the 2021 legislative amendments to the PCMLTFA that clarified FINTRAC's authority to follow up with a reporting entity regarding information required for analysis and assessment. Further consideration in this area could help support Canada's implementation of international AML/ATF standards, and support FINTRAC's analysis.

The importance of public to private information sharing is recognized internationally. The FATF underscores that a close relationship between the private and public sector is a critical element of a well-functioning AML/ATF regime. FATF guidance recommends that engagement be an ongoing process and not just transactional or driven by particular events, as the private sector should also have an accurate understanding of the constantly changing risk environment to complement the efforts of law enforcement. Information sharing can support more effective decision making by reporting entities in due diligence, transaction monitoring and reporting, as well as the exploration of emerging techniques and technologies that assist in the detection of money laundering and terrorist financing activities.

- How can the government enhance two-way information sharing between FINTRAC and the private sector?
- Should FINTRAC be provided with additional powers to request information from reporting entities? If so, what kinds of information and why?
- What sort of additional information should FINTRAC be able to provide to reporting entities regarding compliance and/or intelligence?
- Are there additional guidance or strategic intelligence products FINTRAC should look to provide to reporting entities and the public?

Public-Private Partnerships in Canada's AML/ATF Regime

FINTRAC has public-private partnerships with financial institutions and law enforcement created to combat:

- Human trafficking for sexual exploitation (Project Protect);
- Online child sexual exploitation (Project Shadow);
- Trafficking of illicit fentanyl (Project Guardian);
- Romance fraud (Project Chameleon);
- Illegal wildlife trade (Project Anton);
- Illicit cannabis (Project Legion); and
- Underground banking (Project Athena).

The Counter Illicit Finance Alliance of British Columbia is an RCMP-led financial information sharing partnership composed of multi-sectoral public and private organizations unified to combat money laundering and financial crime.

Database of Politically Exposed Persons and Heads of International Organizations

Reporting entities may have difficulties verifying whether clients are politically exposed persons (PEPs), heads of international organizations (HIOs), or a family member or close associate of a PEP or HIO, as required under certain circumstances in the PCMLTFA. Some private sector companies and non-profit organizations maintain databases of PEPs and HIOs accessible to reporting entities (often for a fee) to help assist them with their due diligence obligations. There are also online resources provided by international governments. For example, the Central Intelligence Agency of the United States publishes an online directory of World Leaders and Cabinet Members of Foreign Governments that is updated weekly, and the European Union lists members of the European Parliament and members of the European Committee of the Regions.

The Cullen Commission's final report encouraged the federal government to consider the viability of creating and maintaining a database of PEPs (both domestic and foreign), HIOs, and family members of PEPs and HIOs, to assist reporting entities. Regulators and law enforcement may also benefit from access to such a database for identifying and taking enforcement actions against corrupt officials.

There are a number of considerations regarding the creation of a government database of PEPs and HIOs. Such a database would need to be subject to appropriate privacy protections, including considerations regarding how much information to display, who would have access, and potential liability concerns for the government. There may be international sensitivities around the government maintaining an accessible database of foreign PEPs and HIOs. There are also matters of increased cost and burden to government and taxpayers, and whether such costs should be offset by charging an access fee. Finally, a government database would duplicate lists and databases that are already provided by other governments and the private and non-profit sectors.

- Should the government create and maintain a database of politically exposed persons (PEPs), heads of international organizations (HIOs), and their family members and close associates?
- Should the government charge an access fee to help offset costs of such a registry?
- Does this proposal raise any privacy considerations?
- Is there a need for such a database given the existing resources and other databases available?

Modernizing Data Collection Authorities

The PCMLTFA provides FINTRAC authority to collect information that "is publicly available, including in a commercially available database" if FINTRAC considers it relevant to money laundering or terrorist financing. However, the acquisition and analytical use of publicly/commercially available databases (and the information contained therein) relevant to money laundering or terrorist financing is not expressly allowed under the PCMLTFA. As a result, some publicly/commercially available databases, and by extension, datasets, that would be useful to support analysis cannot be included in FINTRAC data holdings and may be limited to a search-by-search basis.

Other administrative data collected by federal or provincial government agencies, which may not be publicly available, can also contribute to the fight against money laundering and terrorist financing. This includes databases not specifically related to law enforcement or national security, such as corporate or landowner registries. While government agencies may already collect such information, the PCMLTFA does not grant FINTRAC authorities to acquire these datasets, which limits FINTRAC's ability to access data on high-risk sectors and activities. For example, accessing data sources on trade, customs, or international investment trends could help FINTRAC gain an understanding of the trends and typologies of trade-based money laundering and assist in analyzing and developing intelligence. Consideration must also be given as to whether the legislation underpinning a government database would permit FINTRAC to access the data.

Clarifying FINTRAC's data collection authorities to include further datasets would help ensure FINTRAC is better positioned to inform its analysis and assessment of money laundering and terrorist financing through analytical methods. This in turn supports operational activities, such as assessing new and emerging trends, developments, and patterns that will enhance regime-wide awareness of the threats and vulnerabilities to which Canada is exposed.

- Should the government amend the PCMLTFA to clarify FINTRAC's data collection authorities to enable the acquisition of publicly available (including commercial) datasets that are relevant to FINTRAC's analysis and assessment of money laundering and terrorist financing?
- Should the government amend the PCMLTFA to clarify FINTRAC's data collection authorities to enable the acquisition of administrative datasets maintained by or on behalf of federal and provincial governments and where such data-sharing is permitted by the enabling legislation?
- Does this proposal raise any privacy considerations?

Non-Profit Sector Outreach

Canada's non-profit sector, comprising of registered charities and other non-profit organizations (NPOs), plays a key role in our society and provides valuable services to Canadians. Some of the features and services of the non-profit sector that are instrumental in providing societal good, such as raising and disbursing funds, and providing aid around the world, including to areas affected by disasters and conflict, can also be exploited by bad actors for illegitimate purposes.

Conducting outreach to the NPO sector – international examples:

The United Kingdom has a Tri-Sector Working Group involving the Home Office, the charity sector, and the financial sector to discuss issues and support initiatives around training, guidance, and sharing best practices.

The United States has an ongoing working group involving the Treasury Department and the NPO sector that regularly discusses anti-terrorist financing policies and issues, as well as solicits feedback from the NPO sector.

New Zealand's Charities Sector Group was started to provide an opportunity for members of the charitable sector to interact directly with Charities Services, the government agency that administers the country's charities legislation. The Charities Sector Group discuss priorities, issues, and perspectives, with the aim of strengthening the collective understanding of the charitable sector and Charities Services' work.

Conducting further outreach and engagement with the non-profit sector is a goal of the Department of Finance and the Canada Revenue Agency (CRA) to ensure this sector understands potential money laundering and terrorist financing risks to which it may be exposed and for relevant government officials to learn and seek feedback from non-profit stakeholders. This could include developing a new forum to bring together representatives from the non-profit sector, the Department of Finance, the CRA and financial institutions to engage on strategic issues relevant to AML/ATF.

- How could the government improve outreach and engagement with the non-profit sector on AML/ATF matters?

Naming Foreign Entities in Strategic Intelligence

Under the PCMLTFA, FINTRAC is authorized to disseminate strategic intelligence research and analysis to the public, stakeholders subject to the PCMLTFA, and relevant authorities to broadly inform on the nature and extent of money laundering and terrorist financing inside and outside Canada, as well as measures taken to detect, prevent, and deter these crimes. Budget 2023 also announced the government's intent to amend the PCMLTFA to authorize FINTRAC to disseminate strategic intelligence on the financing of threats to the security of Canada. In all strategic intelligence products, FINTRAC is not permitted to directly or indirectly identify an individual who provided information to FINTRAC, or a person or entity about whom information was provided.

To provide more valuable context and information to the public and AML/ATF stakeholders and authorities, consideration is being given to allow FINTRAC to identify foreign individuals or foreign entities in its strategic intelligence products related to money laundering, terrorist financing, and the financing of threats to the security of Canada. The ability to identify foreign individuals or entities playing a central role in money laundering or terrorist financing activity would help enhance strategic financial intelligence products, strengthen awareness and knowledge of trends, and provide key contextual information with respect to the international environment, including key enablers of illicit finance and threat finance actors.

- Should the government amend the PCMLTFA to authorize FINTRAC to identify foreign individuals or foreign entities in its strategic intelligence products related to money laundering, terrorist financing, and the financing of threats to the security of Canada?
- Does this proposal raise any privacy considerations?

6.3 – Public-to-Public Information Sharing

Illicit actors take advantage of the lack of information sharing that exists within the private sector to obscure or limit perspective into the nature of the complex transactions and relationships and rely on the limits of information sharing among public sector entities.

Public-to-public information sharing refers to the ability of government entities to share information between themselves. For Canada's AML/ATF Regime to effectively function, the core operational partners (i.e., FINTRAC, the RCMP, CBSA, CSIS, and the CRA) must be able to share information relevant to detecting and disrupting money laundering and terrorist financing, while respecting privacy rights, including the right to be free from unreasonable search and seizure in the *Charter*.

The PCMLTFA allows FINTRAC to disclose designated information it receives to law enforcement and intelligence agencies for investigation when legislative thresholds are met. FINTRAC must have reasonable grounds to suspect that the information would be relevant to the investigation or prosecution of a money laundering or a terrorist financing offence, or relevant to the investigation of threats to the security of Canada.

Budget 2023 announced the government's intention to introduce legislative amendments to strengthen information sharing among AML/ATF Regime partners, and to designate OSFI as a recipient of FINTRAC disclosures pertaining to threats to the security of Canada, where relevant to OSFI's responsibilities.

The AML/ATF Regime is reviewing further ways to enhance public-to-public information sharing as it relates to AML/ATF as outlined below.

Targeted Information Sharing Between Operational Regime Partners and Law Enforcement

Canada's legislative framework allows the AML/ATF Regime's core operational partners (i.e., FINTRAC, the RCMP, CBSA, CSIS, and the CRA) to obtain the information they need to support their individual mandates. However, targeted legislative amendments or policy/operational changes could improve the timeliness of access to that information, and/or the information partners can access (e.g., taxpayer information, customs information, criminal intelligence). Efforts to improve access to targeted information would support the overarching objective of successful and timely enforcement actions across all AML/ATF Regime partners.

- How can the government improve the timely access to targeted information amongst operational partners in Canada's AML/ATF Regime to increase money laundering charges, prosecutions and convictions, and asset forfeiture results in Canada?
- Does this proposal raise any privacy considerations?

Enhancing Financial Intelligence Disclosures

FINTRAC discloses financial intelligence to designated recipients when it has reasonable grounds to suspect the information would be relevant to money laundering or terrorist financing investigations or threats to the security of Canada. These financial intelligence disclosures can contain information from hundreds or thousands of individual reports from reporting entities and contribute to major criminal investigations across Canada.

FINTRAC is continuously looking for ways to improve processes and systems to enable timely disclosure of financial intelligence for the investigation and prosecution of money laundering and terrorist financing. Expanding the list of government departments and agencies authorized to receive FINTRAC disclosures would also improve the accessibility of financial intelligence used to detect, investigate, and disrupt money laundering and terrorist financing.

- How can the government facilitate more timely, accessible, and actionable financial intelligence disclosures from FINTRAC to law enforcement and national security agencies?
- Should the government amend the PCMLTFA to expand the list of disclosure recipients to which FINTRAC discloses designated information when legislative thresholds are met?
- Which organizations/agencies should be added to the list of disclosure recipients?
- Does this proposal raise any privacy considerations?

Sharing Information Between FINTRAC and Canada's Environmental Enforcement Organizations

Environmental crime refers to criminal offenses that harm the environment, including illegal wildlife and natural resource harvesting, extraction, and trading; illegal waste dumping, and other pollution-related crimes. While the full scale of environmental crime is complex and its impacts are constantly evolving, it is estimated to be among the most profitable crimes in the world, generating hundreds of billions of dollars per year. Environmental crime also has far-reaching impacts beyond the financial cost, including for the planet and public health. Globally, environmental crime is linked to crime convergence, which includes tax crimes, smuggling of other illicit goods, corruption, human trafficking, migrant smuggling, as well as terrorist financing.

In Canada, as outlined in the Updated Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada, there is particular concern that organized crime groups have infiltrated the waste management sector and may also be involved in the trafficking of electronic waste and importation of counterfeit products that do not meet Canada's environmental standards. There is also an established illicit market for certain Canadian species, including bears, moose, wolves, reptiles, and narwhals.

Project Anton

It is estimated that 55 African elephants are poached on the African continent every day. In Canada, bears are killed for their bile, paws, and other parts, which are then sold for a large profit domestically and internationally. The illegal wildlife trade threatens endangered species and is a major transnational organized crime, generating approximately 20 billion dollars in criminal proceeds each year. These proceeds are, in turn, used to facilitate other serious crimes across the globe.

Project Anton is a public-private partnership initiative led by Scotiabank and supported by FINTRAC, The Royal Foundation's United for Wildlife, and other domestic and international partners to combat illegal wildlife trade. The project is named after Anton Mzimba, head of security at the Timbavati Private Nature Reserve in South Africa and a Global Conservation Technical Advisor, who was murdered for his brave commitment to protecting and conserving wildlife. In his memory, Project Anton aims to improve the collective understanding of illegal wildlife trade and to improve the detection of the laundering of proceeds from this crime.

Despite the significant criminal proceeds generated from environmental crime, actions to combat laundering the proceeds of environmental crime continues to be a challenge. The FATF's report on Money Laundering from Environmental Crimes highlights the need for AML authorities to build working relationships with non-traditional partners, including environmental crime investigators and environmental protection agencies. Given Canada's rich natural resources, improved efforts to strengthen co-ordination and information sharing between authorities responsible for combatting environmental crimes and those responsible for conducting financial investigations may be warranted.

- Should the government amend the PCMLTFA to expand FINTRAC's disclosure authorities to permit the sharing of financial intelligence with Canada's environmental enforcement organizations to help advance their investigative and enforcement mandates?
- Are there other measures the government should consider to further combat environmental crime and its nexus to money laundering and terrorist financing?
- Does this proposal raise any privacy considerations?

Sharing Information Between FINTRAC and Other Regulators

As part of FINTRAC's risk-based compliance program, FINTRAC conducts examinations of its reporting entities to ensure that businesses are fulfilling their compliance obligations. In certain circumstances, as a means of efficiency, exams have been conducted concurrently with other regulatory bodies. However, FINTRAC cannot use compliance-related findings assessed by other regulators to inform its own compliance assessments and must make non-compliance findings on its own.

Enabling FINTRAC and other regulators to better exchange their respective compliance-related findings, when relevant to the other party, and use those findings in their own examinations could create greater regulatory efficiencies and strengthen their risk and compliance programs. A greater exchange of compliance-related information could help inform FINTRAC's and other regulators' compliance assessments and follow-up actions, as well as improve supervisory strategy, taking into consideration the scope of information that could be shared, and potential legal and privacy limitations.

- Should the government amend the PCMLTFA to provide FINTRAC the ability to leverage findings from other regulators in its compliance examinations and share FINTRAC compliance information with other regulators to inform compliance assessments and help improve supervisory strategy?
- What impact would this have, if any, on reporting entities' relationships with their other regulators, including in terms of openness to share information?
- Does this proposal raise any privacy considerations?

Training

Given the complexity of financial crimes cases, sufficient training should be available to investigators and prosecutors to build capacity and expertise and contribute to successful operational results. The exchange of knowledge and best practices among AML/ATF Regime partners also serves an important, informal training purpose.

The Financial Crime Coordination Centre (FC3) within Public Safety Canada has been working to address learning needs within the AML/ATF Regime. For the past two years FC3 has hosted an annual Spin Cycle Conference, focusing on enhancing domestic cooperation and knowledge sharing among AML/ATF officials at all levels of government. FC3 also provides a "Knowledge Hub Portal" for officials at all levels of government involved in combatting financial crimes with the objective to share relevant AML/ATF resources available online or made accessible by Regime partners, and to facilitate connections among subject matter experts within various fields.

- How can the AML/ATF Regime better train investigators and prosecutors to support and contribute to effective outcomes for the Regime?
- Are there any existing training platforms/curricula that have demonstrated the ability to effectively achieve results across industries with practitioners?

Part III – PCMLTFA Legislative and Regulatory Framework

Canada's main legislative statute establishing the AML/ATF Regime, the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA), stipulates the persons and entities subject to its legislative framework, such as financial institutions, casinos, and designated non-financial businesses and professions. These persons and businesses, known as reporting entities, must fulfill reporting, record-keeping, and client due diligence obligations under the PCMLTFA.

FINTRAC is Canada's AML/ATF regulator and financial intelligence unit, responsible for ensuring the compliance of businesses subject to the PCMLTFA and its associated Regulations. FINTRAC also has a mandate to generate actionable financial intelligence for law enforcement and national security agencies to assist in the investigation of money laundering and terrorist financing offences or threats to the security of Canada.

A robust legislative and regulatory framework is required to combat money laundering and terrorist financing risks in Canada. In complying with the obligations of the PCMLTFA, there are over 24,000 reporting entities that play a critical, frontline role in efforts to prevent and detect money laundering and terrorist financing. Chapter 7 explores the scope and obligations of the PCMLTFA to ensure that money laundering and terrorist financing risks are appropriately targeted by the private sector. Chapter 8 focuses on ensuring FINTRAC has effective regulatory tools and oversight to enforce compliance with the PCMLTFA.

Chapter 7 – Scope and Obligations of AML/ATF Framework

The PCMLTFA applies to businesses in the financial sector, casinos, and designated non-financial businesses and professions. These businesses include banks, credit unions, caisses populaires, trust and loan companies, life insurance companies, and securities dealers, in addition to accountants, British Columbia notaries, dealers in precious metals and stones, and provincially-licensed real estate brokers and sales representatives authorized to help buy, sell, and transfer property, and real estate developers (i.e., a person or entity that sells a number of new real estate property to the public above a certain threshold). The PCMLTFA also applies to money services businesses (MSBs), which includes all persons and businesses that provide one or more of the following services: foreign exchange dealing, remitting or transmitting funds, issuing or redeeming money orders, traveler's cheques or anything similar, dealing in virtual currency, crowdfunding platform services, and, once proposed regulations come into force, the transportation of currency and negotiable instruments. All persons and businesses regulated under the PCMLTFA are collectively referred to as "reporting entities."

The PCMLTFA requires reporting entities to identify their clients, keep records, and establish and administer an internal AML/ATF compliance program. Reporting entities are also mandated to report certain transactions to FINTRAC: suspicious financial transactions, large cash or virtual currency transactions of $10,000 or more, international electronic funds transfers, and other prescribed transactions. The PCMLTFA also creates obligations for reporting entities to identify and assess money laundering and terrorist financing risks and to put in place measures to mitigate those risks, including through ongoing monitoring of transactions and enhanced customer due diligence measures. The AML/ATF Regime takes a risk-based approach in setting obligations on reporting entities, balanced against considerations of regulatory burden.

This chapter explores areas to enhance the AML/ATF policy framework in terms of risk-focused obligations on the private sector and, where appropriate, streamlining obligations to reduce compliance burden. Annex 1 also explores other more technical measures to improve or streamline the policy framework.

7.1 – Review Existing Reporting Entities

Accountants

Accountants and accounting firms are subject to the PCMLTFA and associated Regulations when they engage in or give instructions respecting one or more triggering activities on behalf of a client, such as the receipt, payment or transfer of funds or virtual currency and purchase or sale of securities, real property, or business assets. The Regulations define "accountant" as a "chartered accountant, a certified general accountant, a certified management accountant or, if applicable, a chartered professional accountant." It does not include accountants who are not formally certified under a professional body (i.e., unregulated accountants).

There are potential gaps in this coverage, both in terms of the definition of "accountant" and the scope of triggering activities that are regulated for AML/ATF purposes. Findings from the Cullen Commission highlighted the potential risks of unregulated accountants, who nevertheless may perform triggering activities on behalf of a client. Additionally, AML/ATF obligations do not apply to accountants in respect of preparing for and providing advice about triggering activities. Further, the scope of triggering activities covered under the PCMLTFA excludes certain activities performed by accountants such as company and trust formation and providing financial and tax advice. These gaps can expose accountants to money laundering and terrorist financing risks.

- Should the definition of "accountant" be expanded to include uncertified accountants who perform the triggering activities under the PCMLTFA?
- Should AML/ATF obligations be applied to certified and uncertified accountants when they prepare for and provide advice about triggering activities?
- Should the scope of triggering activities be expanded to include other services provided by accountants, and if so, which ones?

Casinos

The Canadian casino and gaming industry has changed considerably since the last Parliamentary review of the PCMLTFA. The evolution of new forms of legal wagering, such as single-event sports betting and the introduction of provincially regulated digital gaming necessitate reviewing whether the definition of casino activities under the PCMLTFA is keeping pace with the industry.

The PCMLTFA refers to the term "conduct and manage" to identify the entity legally responsible for the gaming activities at a casino. This is in line with the *Criminal Code* terminology. In Canada, all gaming is illegal unless it is a lottery scheme "conducted and managed" by a province or territory under its applicable laws. The provincial and territorial governments then delegate the legal responsibility as to who can conduct and manage gaming activities (lottery scheme) at a casino, which can be a government or a private business. The entity that receives this delegated responsibility is then responsible for meeting the obligations of the PCMLTFA and associated Regulations for that casino. In practice, the entity that "conducts and manages" a casino may not necessarily be the same entity that operates the casino activities on a day-to-day basis, meaning that visibility into areas of risk and information sharing around those risks may be more challenging.

The government is also examining the pari-mutuel betting system, which is used in gambling on horse racing. Under this betting system, all bets of a particular type are placed together in a pool. After taxes and the "house-take" are removed, those holding winning tickets divide the net amount bet in proportion to their wagers. Pari-mutuel betting on horse racing is not currently regulated under the PCMLTFA. Instead, the regulatory role is split between the Canadian Pari-Mutuel Agency (CPMA) and the provinces. The CPMA is a special operating agency with the mandate of maintaining the integrity of pari-mutuel betting in Canada. Provincial governments are responsible for the oversight of horse racing, and its participants.

- Should the PCMLTFA definition of a "casino" be shifted to one that is more activity-based? If so, what should a new definition encompass and what are the implications of such a change?
- Should the PCMLTFA cover a broader range of gaming activities and betting types?
- Should pari-mutuel betting and horse racing be scoped in under the PCMLTFA?
- Are any changes to the PCMLTFA or compliance requirements needed to ensure better visibility into high-risk gaming activities and appropriate reporting to FINTRAC?
- How can information sharing around money laundering risks in the casino sector be improved?

Dealers in Precious Metals and Stones

Precious metals and precious stones (including jewellery) possess characteristics that make them vulnerable to money laundering and terrorist financing risks. They are easily transportable forms of wealth that can be converted into cash anywhere in the world.

Dealers in precious metals and stones are subject to the PCMLTFA and its Regulations once they engage in the purchase or sale of precious metals, precious stones, or jewellery in the amount of $10,000 or more (in cash or another form of currency) in a single transaction. In its supervision of this sector, FINTRAC has noticed that the current coverage and obligations in respect of dealers in precious metals and stones do not adequately mitigate all observed risks.

The $10,000 triggering threshold creates a coverage gap among merchants who may not meet the threshold but nevertheless transact in substantial sums that could facilitate money laundering. Precious metals, stones and jewellery sold at auction are also excluded from coverage. Furthermore, there is a gap in respect of large cash transaction reporting when a transaction of $10,000 or more involves gift cards or cash cards (which are proxies for cash) and/or multiple sources of payment in combination with cash (e.g., covering part of the payment in cash and the rest using a credit card).

In addition, changes to the *Precious Metals Marking Act* (PMMA) and its Regulations could be made to assist law enforcement in pursuing crimes involving jewellery. Such changes could include lengthening the retention period of seized property under the PMMA beyond 90 days to allow sufficient time for assessment and investigation and allowing certain offences under the PMMA to be prosecuted as indictable, while retaining the current option for summary conviction. This latter change would cause indictable offences under the PMMA to qualify as a designated offence for the purpose of laying money laundering charges.

- Should the $10,000 triggering threshold to be considered a dealer in precious metals and stones under the PCMLTFA be lowered or removed to cover a broader set of transactions and entities?
  - If so, how would this affect small businesses in Canada?
- Should the coverage of the AML/ATF framework be expanded to include precious metals, precious stones, and jewellery sold at auction?
- Should new obligations be added for dealers in precious metals and stones to report transactions of $10,000 or more involving gift cards or cash cards, or those involving cash in combination with another form of payment?
- Should the government amend the Precious Metals Marking Act (PMMA) to lengthen the retention period of seized property beyond 90 days and making certain offences liable on indictment?
- Are there other suggestions for enhancements to the PMMA to assist law enforcement in pursuing crimes involving jewellery, including money laundering and terrorist financing?

Payment Service Providers

In April 2022, regulatory amendments were passed to extend AML/ATF Regime obligations to a broader range of businesses providing payment services, recognizing that a large subset of this sector was already subject to the PCMLTFA and its Regulations. This included the removal of exemptions for the payment processing of credit, debit, and prepaid products under the definition of electronic funds transfer to extend regulatory obligations to payment service providers (PSPs) engaged in those activities. In alignment with this policy change, FINTRAC revised its interpretation of existing requirements to include businesses that offer certain payment services as being subject to the PCMLTFA.

PSPs subject to the PCMLTFA must register with FINTRAC as either MSBs or foreign MSBs. These PSPs include a range of businesses providing payment services for goods or services or invoice payment services. Additionally, the term "payment service provider" is defined in the *Retail Payments Activities Act* (RPAA), and the Bank of Canada will supervise the entities and individuals that meet that definition. While many entities that perform payment services are captured by both the PCMLTFA and RPAA, the regimes differ in the definitions used to scope in these entities.

The Department of Finance is currently exploring whether MSBs and PSPs should be differentiated under the PCMLTFA and have separate AML/ATF regulatory requirements that account for the different risks (and degrees of risk) in each sector. The objective is to reduce administrative burden on industry, clarify and streamline obligations, and assess whether PSPs can be situated – and regulated – within Canada's AML/ATF framework in a way that more specifically addresses their risks.

- Should there be a new approach to distinguish payment service providers (PSPs) from money services businesses (MSBs) under the PCMLTFA in a way that provides definitional clarity and takes a risk-based approach to the different services PSPs perform?
- What should this approach look like?

Virtual Currency, Digital Assets, and Technology-Enabled Finance

Canadians are using online services more and more in their daily lives, including in their interactions with the financial sector. Financial technologies, such as virtual currencies as defined in Regulations made under the PCMLTFA, have enabled new and evolving methods for conducting financial transactions. The COVID-19 pandemic accelerated this trend toward online and digitized financial services.

While these developments foster beneficial innovation and improved products and services for Canadians, they may also pose money laundering and terrorist financing risks. Canada is committed to a risk-based approach to combatting money laundering and terrorist financing that includes identifying, assessing, and mitigating new risks as they emerge. As new technologies appear in the Canadian economy, the AML/ATF Regime must determine what, if any, government intervention is appropriate and would be effective to prevent these technologies from being coopted by bad actors to launder funds or finance terrorist activities. The government needs to ensure that the AML/ATF Regime can address these new risks and adapt to mitigate future risks from these technologies.

To stay up to date on new risk areas, the Department of Finance has published two national assessments of inherent money laundering and terrorist financing risks in Canada. FINTRAC routinely publishes and shares more in-depth and current operational alerts, typologies, and other strategic financial intelligence products to support PCMLTFA reporting entities and Canadians to identify and mitigate more specific money laundering and terrorist financing risks.

These risk assessments determined that the inherent risks posed by virtual currencies are high, given their ease of access, anonymity, transferability outside of traditionally regulated sectors, including internationally, and their prevalent use in cybercrime. Open source and protected intelligence also suggest that sanctioned actors such as the Democratic People's Republic of Korea are coopting virtual currencies to evade Canada's sanctions regime. For these reasons, businesses that deal in virtual currencies, including the exchange and transfer of virtual currencies, are covered under the AML/ATF Regime. These businesses must register with FINTRAC as MSBs or foreign MSBs. FINTRAC provides guidance for businesses seeking to determine whether they must register as MSBs. For clarity, central bank digital currencies are not considered "virtual currency" under the PCMLTFA and are not in scope for this consultation.

Further notable examples of new technologies for which money laundering and terrorist financing risks continue to evolve include:

- **Crypto-mixers / Crypto-tumblers –** providers of online services to mix virtual currencies together from a variety of sources before transferring it to the designated receiver(s) to obfuscate the chain of transactions from sender to receiver and enhance anonymity.
- **Decentralized Finance (DeFi) –** DeFi commonly refers to the provision of financial products, services, arrangements, and activities that use distributed ledger technology to disintermediate and decentralize legacy ecosystems by eliminating the need for some traditional financial intermediaries and centralized institutions. Currently, there is no generally accepted definition of "DeFi," or what makes a product, service, arrangement, or activity "decentralized.", but most specialists would include decentralized cryptocurrency exchanges (DEX) and decentralized autonomous organizations (DAO). As this technology grows, more decentralized financial tools are likely to appear.
- **Non-Fungible Tokens (NFTs) –** unique digital assets that are not interchangeable and are generally used as collectibles rather than for payment or investment purposes. They are frequently purchased using virtual currencies.
- **The metaverse –** which generally refers to a virtual reality (which could be entirely virtual or a combination of real-world setting augmented by technology-enabled sensory input) accessed via the internet that allows users to interact digitally, including transact with virtual currencies and digital assets.
- **Fintech –** which refers to financial technology. In general, fintech companies provide technology-enabled financial services, such as depositing cheques, offering credit, transferring money, hosting interest paying savings accounts, and paying bills.
- **Privacy-Enhancing Coins –** a type of virtual asset (e.g., Monero) that seeks to provide its users greater anonymity than other types of virtual assets (e.g., Bitcoin or Ethereum).
- **Tokenized Assets –** digital representations of ownership in real-world assets, such as real estate, art, commodities, stocks, and securities, that are traded on blockchain-based platforms.

Some businesses involved in the new technologies listed above also deal in virtual currencies and should therefore already be subject to AML/ATF obligations. It is incumbent upon these businesses to determine with FINTRAC whether they satisfy the criteria for being required to register as MSBs dealing in virtual currencies. Failure to register as an MSB is a criminal violation under the PCMLTFA. Additionally, Budget 2023 announced the government's intention to criminalize the operation of unregistered MSBs.

AML/ATF Regime partners will continue to monitor emerging technologies to identify and mitigate evolving money laundering and terrorist financing risks in Canada, including providing assessments of these risks to policy makers, operational experts, the private sector, and Canadians in general.

- Are there money laundering and terrorist financing risks posed by new financial technologies that are insufficiently covered or mitigated by the AML/ATF framework?
- What legislative and regulatory remedies could be used to address the risks posed by new FinTech products or services (e.g., Anonymity Enhancing Coins (AEC) / PrivacyCoins, crypto-mixers, DeFi)?
- Should reporting entities be prohibited from transferring (and receiving) virtual currencies to (and from) crypto-mixers/crypto-tumblers that are not registered with FINTRAC?
- What AML/ATF obligations are needed for organizations hosting a Metaverse or having a platform for MSB-like activity conducted through their technology?
- What AML/ATF requirements should be extended to fintechs that are currently not regulated? Which types of fintechs would be implicated?
- How can the government ensure that AML/ATF obligations for this sector are technologically neutral so that new technologies that pose AML/ATF risks are incorporated into the Regime in a timely manner?

7.2 – Expanding AML/ATF Coverage in the Real Estate Sector

The Canadian real estate market has been identified as a sector highly vulnerable to money laundering. To address this risk, entities directly and indirectly involved in real estate transactions (federally regulated lenders, real estate brokers, sales representatives, and developers) have obligations under Canada's AML/ATF legislative and regulatory framework. The latest draft regulations impose AML/ATF obligations on mortgage lending entities.

Real Estate Sales by Owner and Auction

The PCMLTFA and its Regulations currently do not extend to for-sale-by-owner (FSBO) and real estate auction companies.

FSBO companies allow sellers to list their property for a flat fee instead of working with a real estate broker or sales representative. They require a potential seller to register with them. Information required for registration varies slightly between companies but usually include the seller's name, contact information (phone and email), and a password to create an account.

Real estate auction companies sell houses through an online bidding process. The company works with potential sellers to agree to a selling price range and a date for the auction to go live. The company also takes photos of the property and lists it on the Multiple Listing Service. Once the auction goes live, potential buyers, or "bidders", can see what other interested buyers are offering for the property.

There is no data on the percentage of real estate transactions completed by FSBO companies and auctions, but it is likely that their market share is relatively small.

- Should the government expand the coverage of the AML/ATF framework to include for-sale-by-owner (FSBO) companies and real estate auction platforms as reporting entities?
- If so, what AML/ATF obligations should apply?
- Would this proposal help mitigate money laundering risks in the real estate sector?
- What impact would this proposal have on FSBO companies and real estate auction platforms?
- What is the market share of real estate transactions conducted by FSBO companies and by auction?

Unrepresented Parties in a Real Estate Transaction

Currently, real estate representatives are required to take reasonable measures to identify unrepresented parties. When unable to do so, real estate representatives must keep a record of the unsuccessful measures taken to verify the identify of the unrepresented party and the transaction can proceed. There is no requirement for a real estate representative to determine whether a third-party is conducting the transaction on behalf of an unrepresented party (as they are not their client).

Given the money laundering risks in the real estate sector, an obligation for real estate representatives to identify and verify the identity of an unrepresented party (not just to take reasonable measures) and to conduct third-party determination when verifying the identity of an unrepresented party in a real estate transaction could support greater detection and deterrence of money laundering in the real estate sector.

- Should it be obligatory for real estate representatives under the PCMLTFA to identify unrepresented parties and conduct third-party determinations in real estate transactions involving unrepresented parties?
- Would this proposal help mitigate money laundering risks in the real estate sector?
- Would this pose compliance challenges for real estate representatives?

Building Supply and Renovation Companies

The PCMLTFA and its Regulations currently do not extend to building supply or renovation companies. Building supply companies provide material required for large scale construction projects or small home renovations. These companies range in size from large public companies to small family-owned companies. Renovation companies are engaged by homeowners in the renovation of their homes and tend to be small to medium-sized companies.

It was noted by the Cullen Commission that building supply companies could be vulnerable to money laundering risks. The Commission conducted a small-scale case study on the prevalence of large cash transactions ($10,000 or more) in the building supply and renovation industry and found that while there was not a substantial amount of cash transactions, the lack of regulatory coverage and the apparent lack of internal company policies regarding the acceptance of unsourced cash as payment for building supplies does present real risks. Money launderers could exploit the lack of oversight and reporting to move significant amounts of illicit money through building suppliers or renovation companies. Criminals may also use illicit cash to make improvements to real property to convert dirty money into real estate equity.

- Should the government expand the coverage of the AML/ATF framework to include building supply and renovation companies as reporting entities?
- If so, what AML/ATF obligations should apply?
- Should all building supply and renovation companies be included, or should there be a certain threshold for inclusion and what would be an appropriate threshold?
- Would this proposal help mitigate money laundering risks in the real estate sector?
- What impact would this proposal have on building supply and renovation companies?

Title Insurers and Mortgage Insurers

Title insurers and mortgage insurers are indirectly involved in a portion of real estate transactions in Canada but are not currently covered under the AML/ATF framework.

Title insurance is an insurance policy that protects residential or commercial property owners and/or their lenders (depending on the policy) against losses related to the property's title or ownership. Given their role as an insurer for title to a property, title insurers gather a wide variety of information on both the insured individual(s) or entity(ies) and the insured property. The comprehensive set of information title insurers collect could possibly be leveraged to identify transactions presenting indicators associated with suspicions of money laundering and title fraud. Recent cases of title fraud have highlighted the dangers of this type of crime, where fraudsters steal ownership of a home to benefit from its value. However, title insurance is not mandatory in Canada and its usage varies greatly among provinces.

Mortgage insurance is an insurance policy that protects a mortgage lender if the borrower defaults on payments, dies or is otherwise unable to meet the contractual obligations of the mortgage. In Canada, mortgage insurance is offered by the federal government, through the Canada Mortgage and Housing Corporation (CMHC), or by private mortgage insurance companies. Mortgage insurers receive information on the property being insured from the lenders. Due to their sightline into an important share of the mortgage market, mortgage insurers are in a good position to monitor situations where various mortgage applications are made by a single applicant (or where a single individual has mortgages with different institutions), which can sometimes be helpful to identify fraud networks and potential money laundering schemes. However, a significant share of mortgages in Canada are not insured. Mortgage insurance is not mandatory when a down payment of 20 per cent is made. Properties valued above $1 million and non-owner-occupied investment properties are not eligible for mortgage insurance.

Incorporating CMHC into the AML/ATF framework is also being considered in section 7.3 under the proposal for federal financial Crown corporations. Alignment of these two proposals will be considered to ensure consistent AML/ATF requirements for both government-funded and private mortgage insurers.

- Should the government expand the coverage of the AML/ATF framework to include title insurers and mortgage insurers as reporting entities?
- If so, what AML/ATF obligations should apply?
- Would this proposal help mitigate money laundering risks in the real estate sector?
- How can the government ensure consistent AML/ATF requirements for both government-funded and private mortgage insurers?

7.3 – Expanding Regime Scope to Other New Sectors

High-Value Goods

High-value goods such as automobiles, yachts, aircraft, art, and other luxury products can be exploited for money laundering or otherwise purchased or leased using the proceeds of crime. These goods are desirable to criminals both as a store of value for the proceeds of crime and for personal enjoyment. The Cullen Commission's final report reinforced the notion that the luxury goods sector is at high risk for money laundering.

The 2018 Parliamentary Review recommended: "That the Government of Canada require companies selling luxury items to be subject to reporting requirements under the PCMLTFA and report large cash transactions to FINTRAC if those transactions are not already reported through other means" (Recommendation 11).

There are various possible regulatory measures available, including taking a more broad-based approach with universal bulk cash reporting requirements, as discussed in the next proposal.

- Should the government expand the coverage of the AML/ATF framework to include high-value goods dealers as reporting entities, including the financial leasing of these goods?
- Which high-value and/or luxury products are most at risk of facilitating money laundering or terrorist financing?
- If coverage were expanded, what would be an appropriate reporting threshold that balances addressing AML/ATF risks while minimizing administrative burden? For example, would sellers and leasers of cars and artwork worth $100,000 or more, or of boats worth $250,000 or more, meet these objectives?
- Overall, would the standard obligations of the PCMLTFA and its Regulations be appropriate for high-value goods dealers? Is there a need for more tailored obligations to account for the risks and properties of this sector?
    - Would some obligations or concepts not be suitable or effective, such as "business relationship", "ongoing monitoring", and terrorist property reporting?
    - Would additional obligations be appropriate, such as verifying a client's source of funds on all transactions of $100,000 or more?
    - What would be the estimated administrative compliance costs for businesses?

Bulk Cash

While cash remains a popular and legitimate means of purchase in the Canadian economy, it is also widely used in the criminal economy and one of the main forms of the proceeds of crime. Using illicit cash to purchase expensive items is a relatively simple way for criminals to integrate proceeds of crime into the Canadian economy and exchange dirty money for legitimate goods that can be transferred or resold as part of a money laundering operation or kept for personal use.

All reporting entities subject to Canada's AML/ATF framework must report to FINTRAC the receipt of cash of $10,000 or more and conduct some due diligence measures on the client providing the cash. However, this requirement does not apply to businesses outside the coverage of the PCMLTFA, exposing a vulnerability and lack of visibility to potential money laundering activity through large cash purchases.

Considering this vulnerability, the Cullen Commission recommended that the province of British Columbia implement a universal record-keeping and reporting requirement for cash transactions of $10,000 or more for all businesses, with certain exceptions, including for one-time transactions between private individuals, and for financial institutions, financial services businesses, and lawyers.

There are various policy options that could help mitigate the vulnerability of large cash purchases, including broadening reporting requirements, prohibiting cash purchases over a certain threshold, as has been proposed by the Council of the European Union for cash transaction of €10,000 or more, or taking a more targeted approach to include certain high-value goods dealers in the AML/ATF Regime, discussed in the previous proposal.

- Should the government amend legislation to mitigate vulnerabilities of large cash transactions, for instance by:
- Extending large cash reporting requirements to all businesses in Canada over a certain threshold, or
- Prohibiting cash purchases over a certain threshold?
- For each option, what would be an appropriate threshold?

Company Service Providers

Businesses that provide incorporation services to the public ("company service providers") guide individuals in forming a corporation. Nonetheless, these entities are at risk of misuse for money laundering and terrorist financing purposes when used to help individuals set up shell corporations to transfer funds and obscure the ultimate ownership of assets and properties. It is a requirement of the FATF for countries to include company service providers within the scope of AML/ATF measures.

Requiring these businesses to implement AML/ATF measures – such as know-your-client and suspicious transaction reporting requirements – could reduce vulnerabilities in the sector and make it more resilient to misuse, while also complementing other measures the government is taking to improve corporate transparency in Canada.

- Should the government expand the coverage of the AML/ATF framework to include company service providers as reporting entities?
- If so, what AML/ATF obligations should apply?
- Would this proposal help mitigate risks of corporations being misused for money laundering or terrorist financing purposes?

White Label Automated Teller Machines

White Label Automated Teller Machines (WLATMs) provide cash withdrawal services. They are privately owned and not branded by a financial institution. Financial institutions and the services they provide via their branded Automated Teller Machines (ATMs) are subject to the AML/ATF Regime, unlike WLATMs. This gap makes WLATMs vulnerable to misuse for money laundering or terrorist financing.

The critical vulnerability of the WLATM sector is that they can be owned and operated by criminals who can load the WLATMs with large amounts of illicit proceeds. Furthermore, companies owning and loading WLATMs for themselves or for other legitimate businesses may be criminally controlled.

In the 2018 Parliamentary Review, the Parliamentary Committee recommended that the Government of Canada amend the PCMTLFA so that the WLATM sector be subject to AML/ATF obligations (Recommendation 7).

- Should the government expand the coverage of the AML/ATF framework to include white label automated teller machines as reporting entities?
- If so, should they be covered under the category of money services businesses (MSBs)?
- What AML/ATF obligations should apply?

Factoring Companies

In general, factoring companies supply short-term loans or upfront payment for the accounts receivable of another business to address their cash-flow needs. The factoring sector is integrated with the financial, corporate, and manufacturing sectors, as well as import and export companies. These companies allow a variety of payment methods such as cash, electronic funds transfers, money orders and cheques, thereby offering opportunities to be used in money laundering. Additionally, factoring services can be used by import and export companies, which can expose them to trade-based money laundering risks.

- Should the government expand the coverage of the AML/ATF framework to include factoring companies as reporting entities?
- If so, what AML/ATF obligations should apply?

Financial Crown Corporations

Crown corporations are government organizations that serve the public interest in a commercial environment. Their day-to-day operations are at arm's-length from the government, and they operate under their own enabling legislation. Crown corporations range from small appropriation-dependent organizations with limited commercial activities, to large corporations operating on a self-sustaining basis akin to entities in the private sector. In practice, most Crown corporations do not have formal AML/ATF mandates, aside from those with activities specifically captured by the PCMLTFA (e.g., related to deposit liabilities, money orders, or precious metals).

Federal Crown corporations engaged in financial activities (e.g., Bank of Canada, Business Development Bank of Canada, Canada Mortgage and Housing Corporation, Export Development Canada, and Farm Credit Canada) may face money laundering and terrorist financing risks and vulnerabilities. Currently, these financial Crown corporations voluntarily follow policies and procedures that align with the PCMLTFA to varying extents. A formal money laundering and terrorist financing prevention and detection mandate for federal financial Crown corporations may enhance the integrity of Canada's Regime, while respecting their operational autonomy and the privacy rights of Canadians.

- Should the government introduce a more formal money laundering and terrorist financing prevention and detection mandate for federal financial Crown corporations?
- If so, what should this entail, and should specific AML/ATF obligations apply?

7.4 – Streamlining Regulatory Requirements

End Period for Business Relationships

Identifying the "business relationship" is a requirement that applies to all reporting entities, based on specific triggers. The government is considering clarifying when a business relationship is considered to have ended, such as when the last account has been closed or when the last transaction took place. This may help to relieve some reporting entities of their obligation for ongoing monitoring of a business relationship that no longer exists or where significant time has passed. However, the end point of a business relationship would vary between reporting entity sectors, as not all business relationships are account-based, and risk/vulnerabilities differ.

In instances where new accounts are opened shortly after the closing of the last account of a corresponding business relationship, the requirement for ongoing monitoring would provide for the establishment of linkages between the two accounts. This identification of linkages is important for AML/ATF purposes.

- Should the concept of "business relationship" in the PCMLTFA and its Regulations be clarified to specify when it is considered to have ended?
- How could the end period for "business relationship" be made consistent and applicable across all reporting entities?
- Should a proposed end period correspond to existing obligations to keep records (e.g., 5 years from account closure or last transaction)?
- Should a proposed end period correspond to risk (e.g., longer period for high-risk and shorter period for low-risk relationships)?

Opportunities to Streamline Other AML/ATF Obligations

As the financial sector and AML/ATF risks evolve and change over time, it is worth reviewing whether AML/ATF obligations for reporting entity sectors could be streamlined to reduce regulatory burden in appropriate areas. For instance, specific triggers and monetary thresholds applicable to certain sectors may become outdated over time. In addition, the AML/ATF Regime may develop a better understanding of where risks lie within and across sectors, enabling it to craft more risk-based obligations. Considerations around modernizing certain obligations and monetary thresholds must be balanced against the risk-based approach and Canada's commitment to uphold international FATF Standards.

- What are other opportunities to streamline AML/ATF requirements?
- Feedback provided on this section should clearly identify:
- How would any proposed change be in keeping with the risk-based approach?
- Are the risks demonstrably lower?
- How would any proposed change continue to uphold international standards?

Chapter 8 – Regulatory Compliance Framework

As Canada's AML/ATF regulator and financial intelligence unit, FINTRAC's mandate is to ensure the compliance of businesses subject to the PCMLTFA and its associated Regulations, and to generate actionable financial intelligence for law enforcement and national security agencies to assist in the investigation of money laundering and terrorist financing offences or threats to the security of Canada.

Broadly speaking, the PCMLTFA requires reporting entities to identify, assess, and mitigate money laundering and terrorist financing risks through a variety of obligations, including identifying clients, monitoring transaction activity, keeping records, and reporting certain transactions to FINTRAC. By complying with the PCMLTFA, reporting entities play a crucial role in Canada's AML/ATF Regime. Compliance with the PCMLTFA allows FINTRAC to receive from reporting entities the quantity and quality of reports it requires to produce actionable financial intelligence and assures law enforcement and security agencies of quick access to information because of improved client identification and record keeping practices. In other words, by creating a compliance program that is effective, efficient, and responsive to risk, reporting entities become part of a larger effort to combat money laundering and terrorist financing.

To assess compliance, the PCMLTFA provides FINTRAC with certain powers to undertake compliance examinations of any person or entity covered under the Act. FINTRAC also has the authority to levy administrative monetary penalties for compliance violations with the PCMLTFA and its associated Regulations. In support of compliance efforts, FINTRAC engages with reporting entities to help them understand their obligations, including to discuss examination approach and findings as well as assist with other compliance issues. Additionally, FINTRAC has a published detailed assessment manual pertaining to compliance examination.

This chapter focuses on potential measures to enhance FINTRAC's supervisory capabilities for ensuring compliance with the PCMLTFA, as well as other ways to broaden the AML/ATF framework to mitigate risks and receive further information from businesses.

8.1 – Modernizing Compliance Tools

Compliance Program Review

Reporting entities are required to institute and document a review of their AML/ATF compliance program to test its effectiveness every two years. Reviews, assessments, and audits are important tools for reporting entities to ensure that their programs, policies, and procedures are aligned with the evolving AML/ATF environment. Reviews also serve as proactive means of demonstrating responsive remedial measures to keep their compliance programs current.

In certain circumstances of urgent or significant non-compliance matters, allowing FINTRAC to direct reporting entities to undertake a review of their compliance program, independent of the biennial review, would help improve compliance and reduce risks. The review would be conducted by an independent external or internal reviewer, at the expense of the reporting entity. This regulatory tool, also known as "special audit" or "skilled person review" is regularly used by both domestic regulators (e.g., OSFI, Bank of Canada) and international financial regulators such as AUSTRAC (Australia's Financial Intelligence Unit and AML Supervisor), and the Financial Conduct Authority in the United Kingdom.

The scope and manner of the review requested by FINTRAC would be determined on a case-by-case basis, commensurate with size and overall risk of the compliance matter. Reporting entities would be further required to share the results of the review, as well as any remedial measures identified, with FINTRAC.

- Should the government amend the PCMLTFA to allow FINTRAC, in circumstances of urgent or significant non-compliance, to direct reporting entities to undertake a review of their compliance program by an independent external or internal reviewer and share the results with FINTRAC?
- Should there be any specific criteria for FINTRAC to make use of this provision?

Compliance Officer

Reporting entities are responsible for appointing an AML/ATF compliance officer and giving them the necessary responsibilities for implementing an AML/ATF compliance program. The compliance officer and compliance program play an important role in mitigating money laundering and terrorist financing risks faced by an entity, and in maintaining compliance with the PCMLTFA.

The current language of the regulations may limit FINTRAC's assessment and enforcement of the effectiveness of the compliance officer role. Defining attributes of the compliance officer and regulatory expectations would provide more clarity and enhance compliance.

- Should the government amend the PCMLTFA to specify the knowledge and competencies required of a qualified compliance officer?
- What knowledge and competency requirements would be appropriate, if any?

Recording

FINTRAC compliance examinations are extremely detailed, involving multiple exchanges to share information, qualify statements and confirm understanding. Compliance examinations are increasingly conducted over video conference and FINTRAC makes use of software to document questions and answers during the examination process. However, FINTRAC compliance officers remain reliant on written notes to document the information provided by reporting entities.

Examinations of large-scale entities may be conducted by a team of compliance officers, however, for smaller businesses, it is often a single compliance officer that is both conducting the examination and taking notes. This can result in incomplete notes and necessitate further follow-up clarification in subsequent meetings. This creates inefficiencies for both the compliance officer and reporting entity being examined.

The ability to make use of audio and video recording technologies, along with appropriate file retention safeguards and the consent of participants would support a more efficient examination process, while protecting rights to privacy.

- Should the government amend the PCMLTFA to allow FINTRAC to use audio and video recording during compliance examinations to improve the efficiency of the process?
- Does this proposal raise any privacy considerations?

Publicizing Violations and Penalties

FINTRAC has legislative authority to issue administrative monetary penalties (AMPs) to reporting entities that are in non-compliance with the PCMLTFA. FINTRAC must make public all AMPs imposed as soon as feasible, describing the penalized party, nature of violation or default and the amount of the penalty issued.

Based on what is permitted to be published under the PCMLTFA, as well as FINTRAC's broader prohibitions on disclosure of information, FINTRAC publicizes limited information about the penalties issued. By comparison, domestic regulators (such as the Financial Consumer Agency of Canada), and international counterparts (including AUSTRAC and the United States' Financial Crimes Enforcement Network) make use of public notices to communicate the basis for violations and penalties imposed to give an indication of their size, scope, and magnitude, as well as prescribed remedial measures and final decisions made by adjudicators of penalties.

Providing greater published descriptions of AMPs imposed and the reasons why could better educate reporting entities and the public about FINTRAC's compliance and enforcement activities, as well as increase FINTRAC's transparency and deterrence capability. Publishing additional details on the penalties would also allow other penalized reporting entities and the public to compare the violations.

- Should the government amend the PCMLTFA to expand the details that FINTRAC publishes in respect of violations and penalties imposed?
- If so, what additional information should be included?

Issuing Administrative Penalties Against Individuals

Under the PCMLTFA, if a criminal offence for non-compliance is committed (either by a person or an entity) any director, officer, or agent associated with that entity or person is held liable for the committed offence. However, there is no corresponding provision in the case of AMPs. While FINTRAC has the legislative authority to issue AMPs to persons or entities subject to the Act, FINTRAC does not have the explicit ability to levy penalties against directors, officers, and/or agents within an entity, except in the case of a sole proprietorship.

In exceptional cases where an individual is identified as having committed the violation, there may be cause to issue a penalty to the individual. This determination would be made on a case-by-case basis to ensure the situation warrants levying a penalty against an individual.

Providing a broader ability for FINTRAC to apply AMPs to individuals in certain cases would improve deterrence against non-compliance violations. This would align with the FATF's recommendation for effective, dissuasive, and proportionate sanctions for persons that fail to comply with AML/ATF requirements. Internationally, the United States has a similar ability to impose penalties on individuals in the event of egregious non-compliance.

- Should the government amend the PCMLTFA to grant FINTRAC the authority to levy administrative penalties against directors, officers, and agents within an entity in certain cases of violations of the PCMLTFA?
- Under what circumstances should FINTRAC be authorized to levy a penalty against directors, officers, or agents?
- What would be an appropriate penalty structure?

8.2 – Effective Oversight and Reporting Framework

False Information Offence

Failure to comply with Parts 1 and 1.1 of the PCMLTFA may result in administrative monetary penalties (AMPs) for violations or criminal charges for offences under the PCMLTFA. FINTRAC has the legislative authority to disclose information to law enforcement when it suspects on reasonable grounds that the information would be relevant to investigating or prosecuting a non-compliance offence under the PCMLTFA. FINTRAC may also disclose to law enforcement instances of non-compliance by reporting entities when legislative thresholds have been met.

Assessing compliance with the PCMLTFA relies on reporting entities providing truthful, relevant, and correct information. Accurate information also serves as the basis for developing financial intelligence to inform money laundering and terrorist financing investigations.

At present, the PCMLTFA contains an offence related to knowingly providing false or misleading information in the context of registering an MSB or foreign MSB. There is no similar offence in the PCMLTFA for other reporting entities or other circumstances, despite the fact that intentionally misleading or withholding information from FINTRAC may be performed to further other criminal activity, including money laundering.

- Should the government amend the PCMLTFA to create an offence against reporting entities for knowingly providing false or misleading information to FINTRAC, or omitting information that should be provided to FINTRAC, in the course of fulfilling any requirement under the PCMLTFA and its associated Regulations?
- Would this offence promote greater compliance among reporting entities subject to the PCMLTFA?
- What would be an appropriate penalty structure for this offence?

Reporting Framework

Reports submitted to FINTRAC from businesses subject to the PCMLTFA are the building blocks for FINTRAC to develop financial intelligence for Canada's AML/ATF Regime. FINTRAC's financial intelligence disclosure packages to law enforcement and partners can include hundreds, or even thousands of such reports from businesses.

Reporting entities must submit a suspicious transaction report (STR) to FINTRAC if there are reasonable grounds to suspect that a financial transaction that occurs or is attempted in the course of their activities is related to the commission or the attempted commission of a money laundering or terrorist financing offence. Having a non-monetary threshold for STRs ensures a flexible approach for covering all manner of suspicious transactions and attempted transactions, recognizing that the value of the transaction or attempted transaction may not be what identifies it as suspicious. The STR, based on grounds for suspicion, is one of the most valuable and unique report types submitted to FINTRAC and is a valuable product for the development of financial intelligence. For this reason, FINTRAC reviews and assesses every STR it receives.

In addition to STRs, reporting entities must report to FINTRAC all cash and virtual currency transactions of $10,000 or more, the initiation and receipt of international electronic funds transfers of $10,000 or more, terrorist property reports, and, in the case of casinos, disbursements of $10,000 or more.

The government recognizes that the reporting requirements of the PCMLTFA impose a regulatory burden on industry and that, collectively, reporting entities submit a large volume of reports annually to FINTRAC.

- How can the government assist reporting entities in fulfilling their reporting obligations in a manner that provides FINTRAC with information necessary to prepare financial intelligence?
- How can the government clarify reporting obligations?
- Should the government consider adjusting the reporting timelines for threshold reporting?
    - If so, how would the proposed change ensure that FINTRAC still receives timely and accurate reporting?

Money Services Businesses (MSB) and Foreign MSB Registration Framework

MSBs and foreign MSBs provide valuable services to Canadians, including remitting and transmitting funds across Canada and globally, including to jurisdictions that may have limited access to traditional financial institutions. While the majority of MSBs and foreign MSBs operate legitimately and are not complicit in illegal activity, the *Updated Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada* notes that the MSB sector is inherently susceptible to money laundering risks due to the array of products and services it offers, its integration with the financial system, and its wide geographic reach across Canada and internationally.

MSBs and foreign MSBs must fulfill specific obligations to help combat money laundering and terrorist financing, like registering with FINTRAC before they can operate in Canada. Additionally, they must implement a compliance program, which forms the basis of meeting their regulatory requirements under the PCMLTFA. The government has previously strengthened the MSB registration framework to expand the ineligibility criteria to include further criminal offences and announced further intended changes in Budget 2023.

The MSB registration framework helps protect the integrity and security of the MSB sector. The Department is considering ways to strengthen the registration framework to better identify non-compliant and ineligible actors, and to revoke or deny registrations when the circumstances require. Options available to improve regulatory controls and address non-compliance include vetting MSB applicants to assess their compliance readiness prior to registration, and revoking registration when an MSB fails to comply with a FINTRAC enforcement measure, such as payment of an Administrative Monetary Penalty.

- How can the government strengthen the money services business (MSB) registration framework to protect the sector from illicit and non-compliant actors and detect unregistered MSBs?
- Should the government amend the PCMLTFA to require FINTRAC to vet MSB applicants to assess their compliance readiness prior to registration?
- Should the government amend the PCMLTFA to allow FINTRAC to revoke registration when an MSB fails to comply with a FINTRAC enforcement measure?

Universal Registration for All Reporting Entities

While all MSBs and foreign MSBs must register with FINTRAC, submitting detailed information about their business, ownership, and senior management, no other reporting entities are required to register or declare themselves to FINTRAC. Consequently, FINTRAC does not have a precise picture of the number and distribution of reporting entities across each sector, particularly if these businesses are not subject to licensing or registration requirements elsewhere.

To improve FINTRAC's line of sight into the reporting entity population, the Department of Finance is considering requiring all non-MSB reporting entities to register with FINTRAC and provide certain relevant information about their businesses. Comprehensive, up-to-date information on the reporting entity population could support sharing timely updates on new guidance and regulatory changes, better risk-based compliance and examination processes, and the regular collection of business information relevant to administrating the PCMLTFA and its Regulations, including for FINTRAC's forthcoming cost assessment scheme.

- Should the government amend the PCMLTFA to introduce registration requirements for all reporting entities?
- What other enforceable ways could FINTRAC obtain a more accurate picture of the reporting entity population?
- How could this potential measure be structured to minimize any additional regulatory burden for reporting entities?

Exemptive Relief for Testing New Technologies

Businesses subject to the PCMLTFA are continuously modernizing their business practices and technologies to keep pace with the evolving financial services sector and novel risks of money laundering and terrorist financing. A nimble legislative and regulatory framework that allows experimentation of promising new business-enabling technologies, subject to appropriate guardrails, can further foster innovation and development of new tools and solutions aimed at increasing efficiency, effectiveness and/or burden reduction.

Providing authorities for FINTRAC to give short-term exemptive relief to reporting entities to allow testing of new technologies and methods to comply with AML/ATF obligations could help enhance administrative flexibility while maintaining the integrity of Canada's AML/ATF Regime and delivering FINTRAC's core mandate. At the same time, AML/ATF statutes reflect decisions taken by elected political officials on the appropriate scope of requirement to mitigate money laundering and terrorist financing risks. Any exemption from these requirements should therefore only be contemplated under limited circumstances, with clearly defined parameters, checks and balances. Consideration would also be given to time-bound relief, as well as requirements for reporting on progress and outcomes.

- Should the government amend the PCMLTFA to allow FINTRAC to provide short-term exemptive relief to reporting entities to allow testing of new technologies and methods to comply with AML/ATF obligations?
- Under what limited circumstances should this permitted?
- What safeguards should apply to ensure the integrity of Canada's AML/ATF Regime is maintained and FINTRAC continues to deliver its core mandate?

De-Risking

Under the PCMLTFA, reporting entities are expected to manage (but not necessarily eliminate) their risk exposure by taking a risk-based approach with respect to their clients. This assessment is expected to take place on a case-by-case basis.

The government has observed that some financial institutions have been opting to terminate banking relationships with some clients in particular sectors, whom they collectively perceive to be high risk, rather than managing risk in line with a risk-based approach. This trend is known as "de-risking". The issue of de-risking is a global trend based upon a complex set of factors that include, but are not limited to, a change in business focus, costs, and changes in the level of risk tolerance.

The FATF has studied the issue of de-risking and noted its impacts on the MSB sector and the non-profit organization sector. International de-risking of these sectors can affect global remittance payments and financial inclusion.

- What businesses and sectors in Canada are affected by de-risking? What impact does this have on their business and operations?
- Are Canadian financial institutions de-risking certain clients? For what reason?
- Should the government take any action regarding de-risking? If so, what?
    - What would be the benefits?
    - What would be the drawbacks?

8.3 – Additional Preventive and Risk Mitigation Measures

Geographic and Sectoral Targeting Orders

Recognizing the varying levels of money laundering and terrorist financing risks throughout Canada, FINTRAC began issuing non-binding Sectoral and Geographic Advisories (SGAs) in 2022 to heighten awareness of risks in specific sectors and regions. Under these advisories, reporting entities are encouraged to take measures to monitor the risks identified and undertake additional financial transaction reporting as appropriate.

Now that the SGA framework is in place to advise reporting entities of geographic and sectoral risks, it could be expanded to ensure reporting entities mitigate the risks identified. This evolution of the SGA framework would be called Geographic and Sectoral Targeting Orders (GSTOs), similar to Geographic Targeting Orders issued by the United States' Financial Crimes Enforcement Network.

GSTOs would foster a flexible and risk-based approach by allowing the Department of Finance or FINTRAC to enact temporary enhanced obligations targeted at businesses in geographic areas or sectors deemed to be of significant risk. In addition to imposing enhanced measures on existing reporting entities, consideration could be given to having GSTOs impose obligations on businesses that are not reporting entities under the PCMLTFA, such as requiring them to report suspicious and large cash or virtual currency transactions to FINTRAC. This additional financial transaction reporting could help FINTRAC generate valuable intelligence to law enforcement or national security agencies, as well as inform strategic intelligence products.

A GSTO framework would require appropriate governance and safeguards. Any obligations imposed by a GSTO framework would also be expected to create compliance burden for the private sector. Additionally, consideration would need to be given to how GSTOs would necessitate additional education and outreach, as well as IT solutions to facilitate reporting. These considerations would likely be magnified in instances of adding entirely new reporting entities through a GSTO.

- Should the government create a framework for Geographic and Sectoral Targeting Orders (GSTOs)?
- Would GSTOs help mitigate money laundering and terrorist financing risks in the Canadian economy?
- What parameters and checks and balances should apply to the governance of GSTOs?
- How could the AML/ATF Regime effectively educate and conduct outreach to the private sector on GSTOs?
- What operational burden and other impacts might this place on stakeholders?

Source of Wealth/Funds Determinations

Money laundering activity is most successful in situations where the criminal origin of the funds can be concealed or disguised. Therefore, measures to identify the source of funds or wealth play an important role in detecting and combatting money laundering.

Currently, reporting entities must take reasonable measures to establish the source of a client's wealth, or the source of cash or virtual currency used in a transaction under specific circumstances if the client is a politically exposed person (PEP) or the head of an international organization (HIO), or a family member or close associate of a PEP or HIO. When reporting large cash or virtual currency transactions, or international electronic funds transfers of $10,000 or more to FINTRAC, reporting entities must also report the source of the cash, virtual currency, or funds, as applicable.

Criminals may seek to take advantage of the limited obligations to establish source of wealth or funds, particularly in high-value transactions where there is opportunity to launder a large amount of money all at once. Real estate transactions may be particularly vulnerable to this risk, but it also applies to other reporting entity sectors. The Cullen Commission's final report recommended that it should be mandatory for real estate licensees to inquire into the source of funds used in a real estate transaction.

Reporting entities should ensure they are not being unwittingly used as a vector to transmit illicit sources of wealth or funds into the Canadian economy. To that end, requirements to establish clients' sources of wealth could be expanded to include all financial transactions and transfers involving large sums, for instance, $100,000 or more.

- Should the government amend the PCMLTFA and/or its Regulations to require all reporting entities to take reasonable measures to establish the source of wealth of an individual when conducting a financial transaction or transfer of a certain threshold?
- If so, what would be an appropriate threshold (e.g., $100,000 or more)?
- Are there are other circumstances in which reporting entities should be required to take reasonable measures to establish the source of wealth or source of cash or virtual currency?

Restricting Third-party Cash Deposits

A commonly observed method employed by money laundering networks to reintegrate proceeds of crime into the legitimate economy is through the use of third-party cash deposits. One example of this technique, known as cuckoo smurfing, entails the interception of legitimate funds through corrupt or criminal money services business, and then the deposit of illicit cash into the accounts of individuals and businesses who are expecting inward remittances. Account holders are often unaware of the illicit source of funds and are simply expecting the transfer of funds into their account from another country.

Law enforcement in Canada have observed this type of money laundering activity across the country and in all major financial institutions. As over-the-counter cash transactions have long been associated with money laundering activity and attract greater scrutiny from financial institutions, suspected money launderers use multiple accounts in numerous financial institutions and conduct transactions in a manner that circumvents mandatory client identification and reporting thresholds to offset detection and avoid being de-banked by financial institutions.

This same typology has been observed globally, and other jurisdictions such as the United Kingdom and New Zealand have implemented restrictions on third-party cash deposits, or their financial institutions have volunteered to implement such restrictions.

Different considerations may apply between personal and business bank accounts. As businesses often have multiple employees depositing cash into corporate accounts, mitigation measures such as a registered list of depositors could be implemented, allowing banks or other financial institutions to limit their exposure to potential money laundering schemes.

- Should the government amend legislation to prohibit or otherwise restrict third-party cash deposits into personal bank accounts?
- Should the government amend legislation to impose tighter identification measures on cash depositors for business bank accounts?

Part IV – National and Economic Security

Chapter 9 – National and Economic Security

The PCMLTFA received royal assent on June 29, 2000, with the objective to implement specific measures to detect and deter money laundering and to facilitate the investigation and prosecution of money laundering offences. Following the events of terrorist attacks in the United States on September 11, 2001, the financing of terrorist activities was incorporated into the Act.

While money laundering and the financing of terrorist activities continue to remain prominent threats to the security of Canada and its economy, the last 20 years have brought about significant changes to the global threat landscape that increasingly put Canada's national and economic security at risk. This undermines Canada's security, its strategic interests, and ultimately the safety of Canadians. These challenges are compounded by the fact that the means used by threat actors to undermine Canada's national security can involve complex financial transactions that have similar properties to money laundering but are conducted for a different purpose and therefore do not fall under the current scope of the AML/ATF Regime. The review of the PCMLTFA presents an opportunity to evaluate if the Act is equipped to address these resulting challenges and whether departments and agencies have the appropriate tools to ensure the financial sector is not used to facilitate illicit activities. Consultation questions are included at the end of this chapter.

9.1 – Threats to the Security of Canada

For purposes of the PCMLTFA, threats to the security of Canada refer to espionage, sabotage, foreign influenced activities, terrorism, and domestic subversion, as per section 2 of the *Canadian Security Intelligence Service Act*. Threats to the security of Canada may overlap with money laundering or terrorist financing concerns; however, that is not always the case.

Improving the Detection of Terrorist Financing

Terrorism remains a leading threat to Canada's national security. Countering terrorism, including its financing, at home and abroad is a key priority for the government. Detecting terrorist financing raises different considerations as compared to money laundering. In many cases, terrorist plots carried out by small cells and lone actors are low cost, and the financial activity of those involved may appear similar to routine financial behaviors.

The Updated Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada highlights various terrorist financing methods involving both financial and material support for terrorism, such as the payment of travel expenses and the procurement of goods. The government also continues to assess the rise of Ideologically Motivated Violent Extremism (IMVE), a subset of terrorist actors motivated by xenophobic, anti-authority, gender identity-driven violence and other grievances. In its July 2021 Special Bulletin on Ideologically Motivated Violent Extremism, FINTRAC noted that organized IMVE groups in Canada use both personal and business accounts to conduct their financial activities, relying on electronic money transfers and cash deposits for their fundraising activities. These transfers typically involved small amounts. Funds were suspected of being used to buy firearms and gear, as well as for donations and membership fees.

Reviewing and, if necessary, enhancing the AML/ATF framework to improve the detection and analysis of terrorist financing activity, particularly where transactions may be in small amounts or difficult to distinguish from activity that would otherwise appear legitimate, would help ensure the framework remains responsive to the shifting threat landscape.

Broadening the PCMLTFA to help counter the financing of threats to the security of Canada

Currently, FINTRAC's mandate and the object of the PCMLTFA is focused on AML/ATF. FINTRAC's role in combatting threats to the security of Canada is narrow. FINTRAC has the authority under s. 55.1 of the PCMLTFA to disclose designated information to the Canadian Security Intelligence Service (CSIS), law enforcement and certain other agencies when specific legislative thresholds are met. However, unlike with money laundering and terrorist financing, reporting entities under the PCMLTFA have no requirement or mechanism to report transactions to FINTRAC that they suspect to be related to threats to the security of Canada. This leaves a potential information gap since FINTRAC's financial intelligence disclosures to national security and law enforcement are premised on incoming reports with a narrow framing of money laundering or terrorist financing. To partially mitigate this risk, Budget 2023 proposes targeted legislative changes allowing the Minister to direct businesses to take enhanced due diligence measures when needed for national security reasons. However, the government is exploring whether the object of the PCMLTFA should be expanded to better scope in countering the financing of threats to the security of Canada in a more comprehensive way.

Expanding the scope of the PCMLTFA could involve requiring businesses subject to the Act to report to FINTRAC if they have grounds to suspect a transaction is related to threats to the security of Canada, beyond terrorist financing. This reporting, along with associated authorities for FINTRAC to receive this information, could help FINTRAC improve its intelligence disclosures related to the financing of threats to the security of Canada, including where this activity may be conducted or facilitated by a reporting entity. FINTRAC could also enforce compliance on any transaction reporting on threats to the security of Canada that would be required under the PCMLTFA.

9.2 – Sanctions

Once a measure of last resort, events such as Russia's illegal invasion of Ukraine demonstrate how economic sanctions have become a more important foreign policy tool. This makes sanctions evasion a more salient economic threat to Canada than ever in the past. Further, FATF standards require governments to take a more active role in understanding financial sector risks and provide appropriate guidance to support effective sanctions implementation.

Under its current mandate and legal framework, FINTRAC can only undertake analysis of suspected sanctions evasion where it intersects with potential money laundering. This limits the ability of FINTRAC to identify sanctions evasion trends, typologies and indicators that could be valuable to the financial sector and law enforcement.

Given that the techniques and means used to evade sanctions can often closely resemble the techniques used in money laundering, FINTRAC may present a unique opportunity to bolster support government's efforts to combat sanctions evasion. In support of this, Budget 2023 proposes legislative changes to set up obligations for the financial sector to report sanctions-related information to FINTRAC.

9.3 – Economic Security

Canada has an open economy and is an attractive destination for foreign investments. While our government continues to welcome foreign direct investment, we need to be vigilant and protect Canadian interests from activity that threatens our national security. For instance, CSIS notes that state-sponsored threat actors seek to advance their strategic political, economic, and military objectives by exploiting investment and trade with Canada.

The access and use of Canada's financial sector to facilitate transactions is central to the ability of foreign actors to make the desired investments and purchases in critical sectors. Given the types of information FINTRAC receives, it may be well-positioned to provide intelligence and advice to better support the broader government objective to safeguard Canada's economic security. Expanding the current scope of the PCMLTFA and FINTRAC's mandate could help counter threats to Canada's economic security.

9.4 – Ministerial and Emergency Powers

The PCMLTFA contains provisions under Part 1.1 that enable the government to take certain targeted actions to protect Canada's financial system. For instance, the Minister of Finance may recommend the issuance of regulations imposing a limitation and prohibition on financial transactions between Canadian businesses subject to the Act and a foreign entity, in defined circumstances linked to money laundering or terrorism financing. However, a parallel provision does not exist enabling the Minister of Finance to make a similar recommendation should a Canadian entity (or entities) pose the same risk. There is also no provision that would allow the Minister of Finance to act if there is a risk that Canadian entities are facilitating the financing of threats to the security of Canada or if there is an emergency resulting in adverse impacts on the integrity or reputation of the Canadian financial system.

Budget 2023 announced the government's intention to amend several laws to modernize the federal financial framework to address emerging risks to Canada's financial sector. This includes providing new powers under the PCMLTFA to allow the Minister of Finance to impose enhanced due diligence requirements to protect Canada's financial system from the financing of national security threats. The Department of Finance is exploring whether additional powers are needed for the Minister of Finance to better mitigate risks in exceptional circumstances.

Chapter 9 Discussion Questions:

The government is seeking views on the nature and scope of FINTRAC's role in helping to counter threats to Canada's national and economic security, and contribute to its sanctions and counter-proliferation framework:

- Should reporting requirements to FINTRAC and/or other obligations be amended to help better detect the financing of terrorist activities, including those conducted by lone actors and where transactions may be in small amounts or difficult to distinguish from activity that would otherwise appear legitimate?
- Is the definition of threats to the security of Canada under the CSIS Act (which is used in the PCMLTFA) sufficient to capture the range of illicit financing activities that could compromise Canada's economic integrity and prosperity?
- Should FINTRAC take a more proactive role in combatting sanctions evasion?
- Should businesses with obligations under the PCMLTFA be required to report to FINTRAC on suspicions of threats to the security of Canada, economic security, proliferation financing or sanctions evasion, in addition to money laundering or terrorist financing?
- Should FINTRAC's mandate be expanded to include a stronger intelligence or compliance role related to threats to the security of Canada, economic security, proliferation financing, and sanctions evasion?
    - Would these authorities be better split among other government departments?
    - What issues could arise from the implementation of a broader mandate?
- Should the Minister of Finance have additional tools under the PCMLTFA to help mitigate national security or other risks to Canada's financial system, including risks to its integrity or reputation?
- Should the Minister of Finance be allowed to recommend, through a regulatory process, the limitation or prohibition of financial transactions with Canadian reporting sectors or entities (as is currently the case with foreign entities) if there are materials money laundering, terrorist financing or national security risks?

Annex 1 – Technical Proposals

The Department of Finance is seeking views on the technical measures proposed below to improve specific aspects of the AML/ATF framework and streamline obligations.

Proposal and Description	Considerations
Record Keeping for Crowdfunding Platforms Align the record-keeping requirements for crowdfunding platforms with other reporting entities by requiring them to keep records of people who pledge $1,000 or more.	Would this requirement be commensurate to the potential risk posed by pledgers to crowdfunding platforms? Would it have a chilling or negative impact on pledges?
Additional Beneficial Ownership Information Require reporting entities to collect the dates of birth and gender of beneficial owners.	Would reporting entities have challenges collecting this information?
Definition of Affiliated Entities Amend the definition of "affiliated entities" to include entities with combined financial statements, thereby allowing such entities to exchange information related to money laundering and terrorist financing.	How would this change impact reporting entities? Are there views on potential privacy considerations?
Large Cash Transaction Reporting Exception Exempt the obligation to report large cash transactions to FINTRAC when an employee conducts the transaction on behalf of their employer.	Would this change create exploitable gaps or risks? The Department of Finance has heard this proposal from stakeholders and is seeking input to better understand the desired impact.
Clarify the Notion of "Third Party" Align the distinct concepts of "third party" between the requirements concerning large cash transaction reporting and account opening.	The Department of Finance has heard this proposal from stakeholders and is seeking input to better understand this proposal and its desired impact.
Authorized Signers on Business Accounts Remove the requirement to verify the identity of up to three authorized signers on a business account.	Would this change create exploitable gaps or risks? The Department of Finance has heard this proposal from stakeholders and is seeking input to better understand the desired impact.
Life Insurance Industry Exempt life insurance companies from having to verify the identity of a plan member's beneficiary in cases where the life insurance company was not required to verify the identity of the plan member. In cases where a life insurance company remitted funds or virtual currency to the beneficiary of an annuity or life insurance policy before verifying the identify of the beneficiary, require the life insurance company to take reasonable measures to verify the beneficiary's identity, and keep a record of the measures taken and whether they were successful. Consider removing or streamlining reporting obligations concerning electronic funds transfers for this sector.	Would these changes create exploitable gaps or risks? The Department of Finance is seeking input on the volume of electronic funds transfers performed by this sector.

Proposal and Description	Considerations
Provide Records to FINTRAC Promptly Require reporting entities to keep records in such a manner that they can be more promptly provided to FINTRAC than the current 30-day period.	Taking note of the FATF requirement for financial entities to be able to provide records to competent authorities "swiftly," what time period would be appropriate to specify for this requirement?
Exceptions for Reporting Large Virtual Currency Transactions Consider adding exceptions for reporting virtual currency transactions of $10,000 or more to FINTRAC, considering that there are exceptions for reporting cash transactions of $10,000 or more.	What exceptions would be appropriate?

Annex 2 – List of Consultation Questions

Chapter 3 – Federal, Provincial, and Territorial Collaboration

- How can different orders of government work together better to address money laundering and terrorist financing?
- How can different orders of government better collaborate and prioritize AML/ATF issues related to beneficial ownership, the legal profession, and civil forfeiture?
- Are there examples of successes in other jurisdictions that Canada should consider? Are there examples of approaches in other jurisdictions that Canada should avoid?
- Are there other areas or issues related to money laundering and terrorist financing that could benefit from greater federal, provincial, and territorial engagement?
- The government also seeks views on whether unexplained wealth order measures could be incorporated into the federal legislative framework. What could be the options? What would be the benefits? What would be the drawbacks?

Part II – Operational Effectiveness

Chapter 4 – Criminal Justice Measures to Combat Money Laundering and Terrorist Financing

4.1 – Investigation and Prosecution of the Offence of Laundering Proceeds of Crime

- Should the offence of laundering proceeds of crime be amended to better address third-party money laundering, such as by altering the nexus required between the predicate offence and the laundering activity?
- What would such a reform look like from your perspective?
- What would be the benefits to such reforms?
- What would be the drawbacks to such reforms?
- Could operational approaches enhance outcomes? What would such approaches entail?
- Are efforts needed to enhance education, awareness, and reporting to authorities among at-risk groups and sectors to better address third-party money laundering?
- Is enhanced capacity building for criminal justice system participants needed to better address third-party money laundering? What could this look like?

4.2 – Offences for other Economically-Motivated Crime

- Would additional offences in the *Criminal Code* effectively contribute to combating fraud, notably through "phishing" or "spoofing"?
- What would be the benefits?
- What would be the shortcomings?

4.3 – Sentencing for Laundering Proceeds of Crime

- Should the government consider sentencing reforms for the offence of laundering proceeds of crime?
- What could this look like?
- What would be the benefits to such reforms?
- What would be the drawbacks to such reforms?

4.4 – Access to Subscriber Information under the *Criminal Code*

- Should the Criminal Code be amended to include an order for subscriber information?
- What should be the extent of information available through such an order?
- Should legislative solutions be explored to address the issues raised by law enforcement regarding turnaround times?
- What would be the benefits?
- What would be the challenges?

4.5 – Electronic Devices

- Should the Criminal Code be amended to provide explicitly for the inclusion of a power to search a person for a thing or property set out in a warrant under section 487 or under section 462.32 where the peace officer has reasonable grounds to believe that the person has the thing on their person?
    - What would be the benefits?
    - What would be the drawbacks?
- What are options to facilitate searches of electronic devices where there is a concern that such a device may contain material protected by solicitor-client privilege, that would meet the constitutional protections afforded to such material?
- Is there a need to consider options for searches involving other forms of materials that may be protected by solicitor-client privilege?
    - What would be the benefits?
    - What would be the drawbacks?

4.6 – Digital Assets and Related Challenges

- Should the Criminal Code be amended to better enable the seizure and restraint of digital assets including cryptocurrency for evidentiary purposes or as offence-related property?
- Are other measures needed?
- Is there a need to amend the Canada Evidence Act to provide for the admissibility of blockchain data as evidence? Is blockchain data already covered by existing rules?
- Should the Canada Evidence Act be amended so that the authenticity of records created using blockchain technology may be presumed? In what circumstances could this be presumed? Are existing rules adequate for this purpose?
- Can information be obtained from centralized exchanges through existing production order provisions? Should amendments be considered?
- What would be the benefits of the above reforms?
- What would be the drawbacks?

4.7 – Pre-Trial Seizure and Restraint of Property Associated with Crime

- Should the *Criminal Code* be amended to enable a peace officer to apply directly to a justice of the peace or judge for an interim seizure or restraint order?
- Are there are other measures that could facilitate preservation of proceeds of crime under the *Criminal Code*?
- What would be the benefits to such reforms?
- What would be the drawbacks?

4.8 – Criminal Forfeiture

- Should the scope of the rebuttable presumption provision in the *Criminal Code* be expanded to include a number of additional profit-oriented offences, such as laundering proceeds of crime and major fraud or extortion on the basis that these offences are increasingly associated with a criminal lifestyle, and to recognize the serious societal harms they represent in their own right? Should other offences be contemplated?
- Should minimum thresholds apply, such as a dollar value, the minimum number of victims, or similar, or is the Crown's obligation to establish a pattern of criminal activity or income that exceeds lawful sources in the rebuttable presumption provisions sufficient?
- What other measures could be considered to enhance the criminal forfeiture of proceeds of crime?
- What would be the benefits to such reforms?
- What would be the drawbacks?

4.9 – Intelligence and Evidence

- How could the government improve the legislative framework governing the protection and use of sensitive intelligence and information during court proceedings in relation to money laundering and terrorist financing?
- What would be the benefits to such reforms?
- What would be the drawbacks?

4.10 – Criminal Jurisdiction

- Are reforms to jurisdiction elements of the laundering of proceeds of crime offence needed?
- Should the law be amended so that the issuance by judges of production orders in Canada - where such orders may apply to entities that operate in the digital realm both within and outside of Canada and over whom Canada may seek to exercise jurisdiction in the context of such orders even where these entities are known to be primarily headquartered outside of Canada - be explicitly set out in statute notwithstanding inherent limitations of such orders?

4.11 – Keep Open Accounts Under Investigation

- Should a legislated "keep-open" regime be implemented?
- How should such a regime operate vis-à-vis circumstances under which law enforcement would make a "keep open" request, the discretion of financial institutions to accept or deny the request, whether legal and reputational protections are required for financial institutions that comply with the request, and ensuring privacy rights are protected?
- What would be the benefits to such reforms?
- What would be the drawbacks?

Chapter 5 – Canada Financial Crimes Agency

5.1 – The Mandate and Structure of the Canada Financial Crimes Agency (CFCA)

The government is seeking views on the mandate of the CFCA, specifically:

- Should the mandate of the CFCA include combatting fraud?
- Should the mandate of the CFCA include combatting sanctions evasion?
- Should the mandate of the CFCA include combatting fiscal crimes (e.g., tax evasion)?
- Are there other crimes that should be included in the CFCA's mandate? For example, corruption, markets-based offences, terrorist financing, etc.

The government is seeking input on how a CFCA should be structured to enable more effective investigation, prosecution, and recovery of proceeds of crime.

5.2 – Core Elements of Effective Financial Crime Enforcement

The government is seeking views on the core activities and functions of the CFCA, including:

- What tools or programs (e.g., legal authorities, organizational policies, technological solutions, whistleblower programs) should be provided to the CFCA to ensure it obtains the information required to conduct effective financial crime enforcement?
- How can the CFCA best attract, develop, and/or retain the expertise required to conduct financial crime investigations, enable prosecutions, and enhance criminal forfeiture?
- Should the CFCA hire or house officials from other AML/ATF Regime partners, such as FINTRAC, RCMP, CSIS, and potentially others?
- What types of public outreach (e.g., research, awareness campaigns, public-private partnerships) should the CFCA engage in to help keep Canadians safe from financial crime threats?

Chapter 6 – Information Sharing

6.1 – Private-to-Private Information Sharing

The government is seeking views on the potential expansion of a framework for private-to-private information sharing for AML/ATF purposes, and is seeking feedback on the following:

- What types of information would be most valuable to share amongst reporting entities to detect, disrupt, and facilitate prosecution of money laundering and terrorist financing offences?
- Are there specific tools, mechanisms, or models from other jurisdictions that could be incorporated into Canadian legislation to support greater information sharing?
- What guardrails would best protect personal information while allowing for additional information to be exchanged between organizations?
- Are there opportunities to leverage technology to enhance information while protecting personal information?

6.2 – Public-to-Private Information Sharing

Sharing Information Between FINTRAC and Reporting Entities

- How can the government enhance two-way information sharing between FINTRAC and the private sector?
- Should FINTRAC be provided with additional powers to request information from reporting entities? If so, what kinds of information and why?
- What sort of additional information should FINTRAC be able to provide to reporting entities regarding compliance and/or intelligence?
- Are there additional guidance or strategic intelligence products FINTRAC should look to provide to reporting entities and the public?

Database of Politically Exposed Persons and Heads of International Organizations

- Should the government create and maintain a database of politically exposed persons (PEPs), heads of international organizations (HIOs), and their family members and close associates?
- Should the government charge an access fee to help offset costs of such a registry?
- Does this proposal raise any privacy considerations?
- Is there a need for such a database given the existing resources and other databases available?

Modernizing Data Collection Authorities

- Should the government amend the PCMLTFA to clarify FINTRAC's data collection authorities to enable the acquisition of publicly available (including commercial) datasets that are relevant to FINTRAC's analysis and assessment of money laundering and terrorist financing?
- Should the government amend the PCMLTFA to clarify FINTRAC's data collection authorities to enable the acquisition of administrative datasets maintained by or on behalf of federal and provincial governments and where such data-sharing is permitted by the enabling legislation?
- Does this proposal raise any privacy considerations?

Non-Profit Sector Outreach

- How could the government improve outreach and engagement with the non-profit sector on AML/ATF matters?

Naming Foreign Entities in Strategic Intelligence

- Should the government amend the PCMLTFA to authorize FINTRAC to identify foreign individuals or foreign entities in its strategic intelligence products related to money laundering, terrorist financing, and the financing of threats to the security of Canada?
- Does this proposal raise any privacy considerations?

6.3 – Public-to-Public Information Sharing

Targeted Information Sharing Between Operational Regime Partners and Law Enforcement

- How can the government improve the timely access to targeted information amongst operational partners in Canada's AML/ATF Regime to increase money laundering charges, prosecutions and convictions, and asset forfeiture results in Canada?
- Does this proposal raise any privacy considerations?

Enhancing Financial Intelligence Disclosures

- How can the government facilitate more timely, accessible, and actionable financial intelligence disclosures from FINTRAC to law enforcement and national security agencies?
- Should the government amend the PCMLTFA to expand the list of disclosure recipients to which FINTRAC discloses designated information when legislative thresholds are met?
- Which organizations/agencies should be added to the list of disclosure recipients?
- Does this proposal raise any privacy considerations?

Sharing Information Between FINTRAC and Canada's Environmental Enforcement Organizations

- Should the government amend the PCMLTFA to expand FINTRAC's disclosure authorities to permit the sharing of financial intelligence with Canada's environmental enforcement organizations to help advance their investigative and enforcement mandates?
- Are there other measures the government should consider to further combat environmental crime and its nexus to money laundering and terrorist financing?
- Does this proposal raise any privacy considerations?

Sharing Information Between FINTRAC and Other Regulators

- Should the government amend the PCMLTFA to provide FINTRAC the ability to leverage findings from other regulators in its compliance examinations and share FINTRAC compliance information with other regulators to inform compliance assessments and help improve supervisory strategy?
- What impact would this have, if any, on reporting entities' relationships with their other regulators, including in terms of openness to share information?
- Does this proposal raise any privacy considerations?

Training

- How can the AML/ATF Regime better train investigators and prosecutors to support and contribute to effective outcomes for the Regime?
- Are there any existing training platforms/curricula that have demonstrated the ability to effectively achieve results across industries with practitioners?

Part III – PCMLTFA Legislative and Regulatory Framework

Chapter 7 – Scope and Obligations of AML/ATF Framework

7.1 – Review Existing Reporting Entities

Accountants

- Should the definition of "accountant" be expanded to include uncertified accountants who perform the triggering activities under the PCMLTFA?
- Should AML/ATF obligations be applied to certified and uncertified accountants when they prepare for and provide advice about triggering activities?
- Should the scope of triggering activities be expanded to include other services provided by accountants, and if so, which ones?

Casinos

- Should the PCMLTFA definition of a "casino" be shifted to one that is more activity-based? If so, what should a new definition encompass and what are the implications of such a change?
- Should the PCMLTFA cover a broader range of gaming activities and betting types?
- Should pari-mutuel betting and horse racing be scoped in under the PCMLTFA?
- Are any changes to the PCMLTFA or compliance requirements needed to ensure better visibility into high-risk gaming activities and appropriate reporting to FINTRAC?
- How can information sharing around money laundering risks in the casino sector be improved?

Dealers in Precious Metals and Stones

- Should the $10,000 triggering threshold to be considered a dealer in precious metals and stones under the PCMLTFA be lowered or removed to cover a broader set of transactions and entities?
    - If so, how would this affect small businesses in Canada?
- Should the coverage of the AML/ATF framework be expanded to include precious metals, precious stones, and jewellery sold at auction?
- Should new obligations be added for dealers in precious metals and stones to report transactions of $10,000 or more involving gift cards or cash cards, or those involving cash in combination with another form of payment?
- Should the government amend the Precious Metals Marking Act (PMMA) to lengthen the retention period of seized property beyond 90 days and making certain offences liable on indictment?
- Are there other suggestions for enhancements to the PMMA to assist law enforcement in pursuing crimes involving jewellery, including money laundering and terrorist financing?

Payment Service Providers

- Should there be a new approach to distinguish payment service providers (PSPs) from money services businesses (MSBs) under the PCMLTFA in a way that provides definitional clarity and takes a risk-based approach to the different services PSPs perform?
- What should this approach look like?

Virtual Currency, Digital Assets, and Technology-Enabled Finance

- Are there money laundering and terrorist financing risks posed by new financial technologies that are insufficiently covered or mitigated by the AML/ATF framework?
- What legislative and regulatory remedies could be used to address the risks posed by new FinTech products or services (e.g., Anonymity Enhancing Coins (AEC) / PrivacyCoins, crypto-mixers, DeFi)?
- Should reporting entities be prohibited from transferring (and receiving) virtual currencies to (and from) crypto-mixers/crypto-tumblers that are not registered with FINTRAC?
- What AML/ATF obligations are needed for organizations hosting a Metaverse or having a platform for MSB-like activity conducted through their technology?
- What AML/ATF requirements should be extended to fintechs that are currently not regulated? Which types of fintechs would be implicated?
- How can the government ensure that AML/ATF obligations for this sector are technologically neutral so that new technologies that pose AML/ATF risks are incorporated into the Regime in a timely manner?

7.2 – Expanding AML/ATF Coverage in the Real Estate Sector

Real Estate Sales by Owner and Auction

- Should the government expand the coverage of the AML/ATF framework to include for-sale-by-owner (FSBO) companies and real estate auction platforms as reporting entities?
- If so, what AML/ATF obligations should apply?
- Would this proposal help mitigate money laundering risks in the real estate sector?
- What impact would this proposal have on FSBO companies and real estate auction platforms?
- What is the market share of real estate transactions conducted by FSBO companies and by auction?

Unrepresented Parties in a Real Estate Transaction

- Should it be obligatory for real estate representatives under the PCMLTFA to identify unrepresented parties and conduct third-party determinations in real estate transactions involving unrepresented parties?
- Would this proposal help mitigate money laundering risks in the real estate sector?
- Would this pose compliance challenges for real estate representatives?

Building Supply and Renovation Companies

- Should the government expand the coverage of the AML/ATF framework to include building supply and renovation companies as reporting entities?
- If so, what AML/ATF obligations should apply?
- Should all building supply and renovation companies be included, or should there be a certain threshold for inclusion and what would be an appropriate threshold?
- Would this proposal help mitigate money laundering risks in the real estate sector?
- What impact would this proposal have on building supply and renovation companies?

Title Insurers and Mortgage Insurers

- Should the government expand the coverage of the AML/ATF framework to include title insurers and mortgage insurers as reporting entities?
- If so, what AML/ATF obligations should apply?
- Would this proposal help mitigate money laundering risks in the real estate sector?
- How can the government ensure consistent AML/ATF requirements for both government-funded and private mortgage insurers?

7.3 – Expanding Regime Scope to Other New Sectors

High-Value Goods

- Should the government expand the coverage of the AML/ATF framework to include high-value goods dealers as reporting entities, including the financial leasing of these goods?
- Which high-value and/or luxury products are most at risk of facilitating money laundering or terrorist financing?
- If coverage were expanded, what would be an appropriate reporting threshold that balances addressing AML/ATF risks while minimizing administrative burden? For example, would sellers and leasers of cars and artwork worth $100,000 or more, or of boats worth $250,000 or more, meet these objectives?
- Overall, would the standard obligations of the PCMLTFA and its Regulations be appropriate for high-value goods dealers? Is there a need for more tailored obligations to account for the risks and properties of this sector?
- Would some obligations or concepts not be suitable or effective, such as “business relationship”, “ongoing monitoring”, and terrorist property reporting?
- Would additional obligations be appropriate, such as verifying a client’s source of funds on all transactions of $100,000 or more?
- What would be the estimated administrative compliance costs for businesses?

Bulk Cash

- Should the government amend legislation to mitigate vulnerabilities of large cash transactions, for instance by:
- Extending large cash reporting requirements to all businesses in Canada over a certain threshold, or
- Prohibiting cash purchases over a certain threshold?
- For each option, what would be an appropriate threshold?

Company Service Providers

- Should the government expand the coverage of the AML/ATF framework to include company service providers as reporting entities?
- If so, what AML/ATF obligations should apply?
- Would this proposal help mitigate risks of corporations being misused for money laundering or terrorist financing purposes?

White Label Automated Teller Machines

- Should the government expand the coverage of the AML/ATF framework to include White Label Automated Teller Machines as reporting entities?
- If so, should they be covered under the category of money services businesses (MSBs)?
- What AML/ATF obligations should apply?

Factoring Companies

- Should the government expand the coverage of the AML/ATF framework to include factoring companies as reporting entities?
- If so, what AML/ATF obligations should apply?

Financial Crown Corporations

- Should the government introduce a more formal money laundering and terrorist financing prevention and detection mandate for federal financial Crown corporations?
- If so, what should this entail, and should specific AML/ATF obligations apply?

7.4 – Streamlining Regulatory Requirements

End Period for Business Relationships

- Should the concept of "business relationship" in the PCMLTFA and its Regulations be clarified to specify when it is considered to have ended?
- How could the end period for "business relationship" be made consistent and applicable across all reporting entities?
- Should a proposed end period correspond to existing obligations to keep records (e.g., 5 years from account closure or last transaction)?
- Should a proposed end period correspond to risk (e.g., longer period for high-risk and shorter period for low-risk relationships)?

Opportunities to Streamline Other AML/ATF Obligations

- What are other opportunities to streamline AML/ATF requirements?
- Feedback provided on this section should clearly identify:
- How would any proposed change be in keeping with the risk-based approach?
- Are the risks demonstrably lower?
- How would any proposed change continue to uphold international standards?

Chapter 8 – Regulatory Compliance Framework

8.1 – Modernizing Compliance Tools

Compliance Program Review

- Should the government amend the PCMLTFA to allow FINTRAC, in circumstances of urgent or significant non-compliance, to direct reporting entities to undertake a review of their compliance program by an independent external or internal reviewer and share the results with FINTRAC?
- Should there be any specific criteria for FINTRAC to make use of this provision?

Compliance Officer

- Should the government amend the PCMLTFA to specify the knowledge and competencies required of a qualified compliance officer?
- What knowledge and competency requirements would be appropriate, if any?

Recording

- Should the government amend the PCMLTFA to allow FINTRAC to use audio and video recording during compliance examinations to improve the efficiency of the process?
- Does this proposal raise any privacy considerations?

Publicizing Violations and Penalties

- Should the government amend the PCMLTFA to expand the details that FINTRAC publishes in respect of violations and penalties imposed?
- If so, what additional information should be included?

Issuing Administrative Penalties Against Individuals

- Should the government amend the PCMLTFA to grant FINTRAC the authority to levy administrative penalties against directors, officers, and agents within an entity in certain cases of violations of the PCMLTFA?
- Under what circumstances should FINTRAC be authorized to levy a penalty against directors, officers, or agents?
- What would be an appropriate penalty structure?

8.2 – Effective Oversight and Reporting Framework

False Information Offence

- Should the government amend the PCMLTFA to create an offence against reporting entities for knowingly providing false or misleading information to FINTRAC, or omitting information that should be provided to FINTRAC, in the course of fulfilling any requirement under the PCMLTFA and its associated Regulations?
- Would this offence promote greater compliance among reporting entities subject to the PCMLTFA?
- What would be an appropriate penalty structure for this offence?

Reporting Framework

- How can the government assist reporting entities in fulfilling their reporting obligations in a manner that provides FINTRAC with information necessary to prepare financial intelligence?
- How can the government clarify reporting obligations?
- Should the government consider adjusting the reporting timelines for threshold reporting?
- If so, how would the proposed change ensure that FINTRAC still receives timely and accurate reporting?

Money Services Businesses (MSB) and Foreign MSB Registration Framework

- How can the government strengthen the money services business (MSB) registration framework to protect the sector from illicit and non-compliant actors and detect unregistered MSBs?
- Should the government amend the PCMLTFA to require FINTRAC to vet MSB applicants to assess their compliance readiness prior to registration?
- Should the government amend the PCMLTFA to allow FINTRAC to revoke registration when an MSB fails to comply with a FINTRAC enforcement measure?

Universal Registration for All Reporting Entities

- Should the government amend the PCMLTFA to introduce registration requirements for all reporting entities?
- What other enforceable ways could FINTRAC obtain a more accurate picture of the reporting entity population?
- How could this potential measure be structured to minimize any additional regulatory burden for reporting entities?

Exemptive Relief for Testing New Technologies

- Should the government amend the PCMLTFA to allow FINTRAC to provide short-term exemptive relief to reporting entities to allow testing of new technologies and methods to comply with AML/ATF obligations?
- Under what limited circumstances should this permitted?
- What safeguards should apply to ensure the integrity of Canada's AML/ATF Regime is maintained and FINTRAC continues to deliver its core mandate?

De-Risking

- What businesses and sectors in Canada are affected by de-risking? What impact does this have on their business and operations?
- Are Canadian financial institutions de-risking certain clients? For what reason?
- Should the government take any action regarding de-risking?

8.3 – Additional Preventive and Risk Mitigation Measures

Geographic and Sectoral Targeting Orders

- Should the government create a framework for Geographic and Sectoral Targeting Orders (GSTOs)?
- Would GSTOs help mitigate money laundering and terrorist financing risks in the Canadian economy?
- What parameters and checks and balances should apply to the governance of GSTOs?
- How could the AML/ATF Regime effectively educate and conduct outreach to the private sector on GSTOs?
- What operational burden and other impacts might this place on stakeholders?

Source of Wealth/Funds Determinations

- Should the government amend the PCMLTFA and/or its Regulations to require all reporting entities to take reasonable measures to establish the source of wealth of an individual when conducting a financial transaction or transfer of a certain threshold?
- If so, what would be an appropriate threshold (e.g., $100,000 or more)?
- Are there are other circumstances in which reporting entities should be required to take reasonable measures to establish the source of wealth or source of cash or virtual currency?

Restricting Third-party Cash Deposits

- Should the government amend legislation to prohibit or otherwise restrict third-party cash deposits into personal bank accounts?
- Should the government amend legislation to impose tighter identification measures on cash depositors for business bank accounts?

Part IV / Chapter 9 – National and Economic Security

The government is seeking views on the nature and scope of FINTRAC's role in helping to counter threats to Canada's national and economic security, and contribute to its sanctions and counter-proliferation framework:

- Should reporting requirements to FINTRAC and/or other obligations be amended to help better detect the financing of terrorist activities, including those conducted by lone actors and where transactions may be in small amounts or difficult to distinguish from activity that would otherwise appear legitimate?
- Is the definition of threats to the security of Canada under the CSIS Act (which is used in the PCMLTFA) sufficient to capture the range of illicit financing activities that could compromise Canada's economic integrity and prosperity?
- Should FINTRAC take a more proactive role in combatting sanctions evasion?
- Should businesses with obligations under the PCMLTFA be required to report to FINTRAC on suspicions of threats to the security of Canada, economic security, proliferation financing or sanctions evasion, in addition to money laundering or terrorist financing?
- Should FINTRAC's mandate be expanded to include a stronger intelligence or compliance role related to threats to the security of Canada, economic security, proliferation financing, and sanctions evasion?
- Would these authorities be better split among other government departments?
- What issues could arise from the implementation of a broader mandate?
- Should the Minister of Finance have additional tools under the PCMLTFA to help mitigate national security or other risks to Canada's financial system, including risks to its integrity or reputation?
- Should the Minister of Finance be allowed to recommend, through a regulatory process, the limitation or prohibition of financial transactions with Canadian reporting sectors or entities (as is currently the case with foreign entities) if there are materials money laundering, terrorist financing or national security risks?

List of Abbreviations

AML/ATF - anti-money laundering and anti-terrorist financing

AMP - administrative monetary penalty

APG - Asia-Pacific Group on Money Laundering

ATM - automated teller machine

AUSTRAC - Australian Transaction Reports and Analysis Centre

CBSA - Canada Border Services Agency

CDSA - Controlled Drugs and Substances Act

CFCA - Canada Financial Crimes Agency

CMHC - Canada Mortgage and Housing Corporation

CPMA - Canadian Pari-Mutuel Agency

CSIS - Canadian Security Intelligence Service

CRA - Canada Revenue Agency

CRTC - Canadian Radio-Television and Telecommunications Commission

FATF - Financial Action Task Force

FC3 - Financial Crime Coordination Centre

FINTRAC - Financial Transactions and Reports Analysis Centre of Canada

FSBO - for-sale-by-owner

G7/G20 - Group of 7 / Group of 20

GSTOs - geographic and sectoral targeting orders

HIO - head of an international organization

IMLIT - Integrated Money Laundering Investigative Teams

IMET - Integrated Market Enforcement Teams

IMVE - ideologically motivated violent extremism

ISIL - Islamic State in Iraq and the Levant

MSB - money service business

NPO - non-profit organization

OSFI - Office of the Superintendent of Financial Institutions

PCMLTFA - Proceeds of Crime (Money Laundering) and Terrorist Financing Act

PEP - politically exposed person

PIPEDA - Personal Information Protection and Electronic Documents Act

PMMA - Precious Metals Marking Act

PSP - payment service provider

RCMP - Royal Canadian Mounted Police

RPAA - Retail Payments Activities Act

SGA - sectoral and geographic advisory

STR - suspicious transaction report

TPML - third party money laundering (or launderer)

WLATM - white label automated teller machine

Links to Documents

2018 Parliamentary Review

Committee Report - Confronting Money Laundering and Terrorist Financing: Moving Canada Forward

Government Response to Confronting Money Laundering and Terrorist Financing: Moving Canada Forward

Reviewing Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime

Acts and Regulations

Canada Business Corporations Act

Canada Evidence Act

Canadian Charter of Rights and Freedoms

Canadian Security Intelligence Service Act

Cannabis Act

Controlled Drugs and Substances Act

Criminal Code

Draft Regulations Amending Certain Regulations Made Under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act

Income Tax Act

Personal Information Protection and Electronic Documents Act

Precious Metals Marking Act

Privacy Act

Proceeds of Crime (Money Laundering) and Terrorist Financing Act and Associated Regulations

Retail Payments Activities Act

Telecommunications Act

AML/ATF Regime Documents

Advisory Committee on Money Laundering and Terrorist Financing

Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime Strategy 2023-2026

Report on Performance Measurement Framework

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

British Columbia

Commission of Inquiry into Money Laundering in British Columbia: Final Report

Dirty Money – Part 2

Financial Action Task Force Documents

4th Enhanced Follow-up Report of Canada - October 2021

Declaration of the Ministers of the FATF

Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals

Money Laundering from Environmental Crimes

Mutual Evaluation of Canada - September 2016

FINTRAC Documents

FINTRAC Guidance: Reporting Large Virtual Currency Transactions to FINTRAC

FINTRAC Special Bulletin on Ideologically Motivated Violent Extremism

Other

Minister of Public Safety Mandate Letter - 2021

Unsolicited Telecommunications Rules