Department of Finance Canada
Ministère des Finances Canada

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

February 7, 2018

Canada

Table of Contents

Preface

Actions 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. A strong legislative and regulatory framework is required to effectively detect and deter criminal activity. Maintaining current international best practices assist Canada in fulfilling our international commitments to participate in the fight against transnational crime. Canada's efforts also serve to safeguard its financial system against its use as a vehicle for money laundering and the financing of terrorist activities.

The Government of Canada is committed to a strong anti-money laundering and anti-terrorist financing legislative framework which also provides important safeguards for citizens' rights and privacy. This framework is established by the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA) and its Regulations. The Department of Finance's review of Canada's anti-money laundering and anti-terrorist financing (AML/ATF) legislative framework supports the upcoming Parliamentary Review of the PCMLTFA.

Section 72(1) of the *PCMLTFA* requires that the administration and operation of the Act shall be reviewed by a committee of Parliament every five years. The legislative requirement to review the Act every five years provides the opportunity to keep the framework current in response to market developments as well as new and evolving risks. Feedback from the private sector and other stakeholders supports our analysis of the framework's effectiveness. A well-functioning framework is critical to combatting money laundering and terrorist financing in Canada and globally.

The money laundering and terrorist financing environment has evolved since the last review was completed in 2013 and these crimes continue to pose a threat to national security. There have been significant advancements in technology which include: developments related to virtual currencies, which offer new ways to move value with anonymity; the development of new financial technologies (fintech) which are changing the ways Canadians interact with the financial system; and digital identity recognition, which can facilitate the customer due diligence process which is a cornerstone of the framework. These developments present challenges to maintaining a current and comprehensive Regime, but they can also provide opportunities as well. For example, reporting entities can use new technologies to better understand and mitigate their risks and/or meet their obligations under the framework (i.e., RegTech).

The threat and risk environment of money laundering and terrorist financing in Canada has also changed as new methods to launder money and finance terrorism are developed. These risks were assessed in the first *Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada*, published in 2015. Released in 2016, a Mutual Evaluation report by the Financial Action Task Force (FATF) found that Canada has strong anti-money laundering and anti-terrorist financing legislation and Regulations but noted there are several areas where action could be taken to ensure the framework meets technical standards and is even more effective.

This paper is intended to support Parliament's upcoming study of the PCMLTFA and its consideration of issues relating to money laundering and terrorist financing in Canada. At the same time, the Department of Finance is seeking input from stakeholders in response to this paper to support the development of forward policy and technical measures that could lead to legislative changes or inform the Department's longer-term approaches to anti-money laundering and anti-terrorist financing.

The Department of Finance is undertaking this work in concert with the federal government departments and agencies that are part of Canada's AML/ATF Regime.[1] Along with ideas developed internally, the Department sought input on areas for improvement with departments and agencies and members of the Advisory Committee on Money Laundering and Terrorist Financing.[2] These suggestions were then distilled into the contents of this paper. As part of this process, we will take your views and share them with the appropriate department or agency.

[1] Department of Finance, Financial Transactions and Reports Analysis Centre of Canada, Royal Canadian Mounted Police, Canada Border Services Agency, Canadian Security Intelligence Service, Canada Revenue Agency, Department of Justice Canada, Public Prosecution Service of Canada, Public Safety Canada, Office of the Superintendent of Financial Institutions, Global Affairs Canada, Innovation, Science and Economic Development Canada, and Public Services and Procurement Canada.

[2] The Advisory Committee on Money Laundering and Terrorist Financing is a public-private sector committee comprised of representatives from the Regime departments and agencies as well as representatives from each reporting entity sector. It is co-chaired by the Department of Finance and private sector representatives.

Process

Submissions on this discussion paper will close on May 18, 2018.

Written comments should be sent to:

Director General
Financial Systems Division
Financial Sector Policy Branch
Department of Finance Canada
James Michael Flaherty Building
90 Elgin Street
Ottawa ON K1A 0G5
Email: fin.fc-cf.fin@canada.ca

The Department of Finance will make public some or all of the comments received or may provide summaries in its public documents. Stakeholders providing comments are asked to clearly indicate the name of the individual or the organization that should be identified as having made the submission.

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

- consent to the 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 be kept confidential (if so, clearly identify the confidential portions);

Information received through this comment process is subject to the *Access to Information Act* and the *Privacy Act*. Should you express an intention that your comments, or any portions thereof, be considered confidential, the Department of Finance will make all reasonable efforts to protect this information.

Introduction

The Importance of Combatting Money Laundering and Terrorist Financing

Money laundering and terrorist financing are a threat to domestic and global safety and security and compromise the integrity of the financial system. Money laundering is the process used by criminals to conceal or disguise the origin of criminal proceeds to make them appear as if they originated from legitimate sources.[3] Terrorist financing is the process of collecting funds from legitimate (or illegitimate) sources and concealing or disguising their purpose, namely to support terrorist activity in Canada or abroad, causing loss of life and destruction. While money laundering and terrorist financing may differ in their objectives they often exploit the same vulnerabilities in financial systems.

Money laundering and terrorist financing have criminal and economic effects and they both contribute to rewarding and perpetuating criminal activity. Money laundering and terrorist financing harm the integrity and stability of the financial sector and the broader economy and threaten our quality of life. Because they act as a deterrent to financial crime, effective regimes to combat these threats are essential to protect Canadians, the integrity of markets, and the global financial system. The International Monetary Fund has stated: "action against money laundering and terrorist financing thus responds not only to a moral imperative but also to an economic need […] In an increasingly interconnected world, the harm done by these activities is global. Money launderers and terrorist financiers exploit the complexity inherent in the global financial system as well as differences between national laws; jurisdictions with weak or ineffective controls are especially attractive to them."[4]

Financial surveillance and enforcement efforts are carried out within the wider context of criminal and terrorism deterrence and enforcement and are balanced by rights and protections afforded to Canadians of individual privacy and respect for due process.

The Regime imposes stringent requirements on financial intermediaries in the private sector, additional to the resources that public sector entities directly allocate to the prevention of crime and terrorism. This review seeks to advance the efficiency and effectiveness of the Regime to ensure that private and public sector resources are better aligned to current technological, business and threat realities.

[3] Money laundering involves three distinct stages: the placement stage, the layering stage, and the integration stage. The placement stage is the stage at which funds from the illegal activity, or funds intended to support an illegal activity, are first introduced into the financial system. The layering stage involves further disguising and distancing the illicit funds from their illegal source through the use of a series of transactions and/or parties which is designed to conceal the source of the illicit funds. The integration phase of money laundering results in the illicit funds being considered "laundered" and more fully integrated into the financial system so that the criminal may utilise "clean" funds.

[4] The IMF - https://www.imf.org/en/About/Factsheets/Sheets/2016/08/01/16/31/Fight-Against-Money-Laundering-the-Financing-of-Terrorism.

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

Canada has a stable and open economy, an accessible and advanced financial system, and strong democratic institutions. Those seeking to launder proceeds of crime or, raise, transfer and use funds for terrorism purposes, try to exploit some of these strengths. Canada takes a comprehensive and coordinated approach to combating money laundering and terrorist financing to promote the integrity of the financial system and the safety and security of Canadians.

Canada's Regime is comprised of legislation and Regulations, federal departments and agencies, including regulators and supervisors; law enforcement agencies; and reporting entities. Canada's AML/ATF legal framework is comprised of the PCMLTFA and its Regulations, which are an essential component of Canada's broader AML/ATF Regime. The Regime involves 13 federal departments and agencies with authorities provided by the PCMLTFA or other Acts, eight of which receive dedicated funding totalling approximately $70 million annually.[5] In addition to federal organizations, provincial and municipal law enforcement bodies and provincial regulators (including those with a role in the oversight of the financial sector) are also involved in combating these illicit activities. Within the private sector, there are almost 31,000 Canadian financial institutions and designated non-financial businesses and professions (DNFBPs)[6] with reporting obligations under the PCMLTFA, known as 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) disruption.

(i) Policy and Coordination

The Regime's policy and legislative framework as well as its domestic and international coordination is led by the Department of Finance Canada. The Department provides policy advice to the Minister on proposed legislative and regulatory measures; advises the Minister on emerging developments related to combating money laundering and terrorist financing; and provides advice related to Regime activities and funding issues as well as advice with respect to his oversight role and responsibility for the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). Further, the Department leads Canada's delegation to the Financial Action Task Force (FATF) and other regional and international AML/ATF fora.

[5] The eight funded partners are: Canada Border Services Agency, Canada Revenue Agency, Canadian Security Intelligence Service, Department of Finance Canada, Department of Justice Canada, Financial Transactions and Reports Analysis Centre of Canada, Public Prosecution Service of Canada and Royal Canadian Mounted Police.

[6] Designated non-financial businesses and professions (DNFBPs) include accountants and accounting firms; real estate brokers, sales representatives; real estate developers; casinos; lawyers and legal firms; dealers in precious metals and stones; and British Columbia notaries.

The PCMLTFA, the legislation that establishes Canada's AML/ATF framework, is supported by other key statutes, including the *Criminal Code*. The PCMLTFA requires reporting entities to identify their clients, keep records and establish and administer an internal AML/ATF compliance program. The PCMLTFA creates mandatory reporting requirements for suspicious financial transactions, large cash transactions, cross-border currency transfers and other prescribed transactions. It also creates obligations for the reporting entities to identify money laundering and terrorist financing risks and to put in place measures to mitigate those risks, including through ongoing monitoring of transactions and enhanced customer due diligence measures.

(ii) Prevention and Detection

The second pillar provides strong measures to prevent individuals from placing illicit proceeds or terrorist-related funds into the financial system, while having correspondingly strong measures to detect the placement and movement of such funds. At the centre of this prevention and detection approach are the reporting entities (specifically the financial institutions and designated non-financial businesses and professions) that are the gatekeepers of the financial system in implementing the various measures under the PCMLTFA, and the regulators (principally FINTRAC and the Office of the Superintendent of Financial Institutions (OSFI)), which supervise them. The transparency of corporations and trusts contributes to preventing and detecting money laundering and terrorist financing, including the requirements for financial institutions to identify the beneficial owners[7] of the corporations and trusts with whom they do business. Provincial and federal corporate laws and registries and securities regulation also contribute to preventing and detecting money laundering and terrorist financing in Canada.

The information disseminated under the PCMLTFA can be used as intelligence to support domestic and international partners in the investigation and prosecution of money laundering and terrorist financing related offences. The information can also be in the form of trend and typology reports used to educate the public, including the reporting entities, on money laundering and terrorist financing issues.

(iii) Disruption

The final pillar deals with the disruption of money laundering and terrorist financing. Regime partners, such as the Canadian Security Intelligence Service (CSIS), the Canada Border Services Agency (CBSA) and the Royal Canadian Mounted Police (RCMP), supported by FINTRAC's intelligence gathering and analysis activities, undertake investigations in relation to money laundering, terrorist financing, other profit-oriented crimes and threats to the security of Canada in accordance with their individual mandates. The Canada Revenue Agency (CRA) also plays an important role in investigating tax evasion (and its associated money laundering) and in detecting charities that are at risk, to ensure that they are not being abused to finance terrorism. The Public Prosecution Service of Canada (PPSC) along with provincial prosecutors ensure that crimes are prosecuted to the fullest extent of the law. The restraint and confiscation of proceeds of crime is also an important law enforcement component of the regime. Public Services and Procurement Canada (PSPC) manages all seized and restrained property for criminal cases prosecuted by the Government of Canada as well as providing forensic accounting expertise to the RCMP. The CBSA enforces the

[7] Beneficial ownership refers to the identity of the natural person who ultimately controls the corporation or entity, which cannot be another corporation or another entity.

Cross-Border Currency Reporting Program, and transmits information from reports and seizures to FINTRAC. The Regime also has robust terrorist listing processes to freeze terrorist assets, pursuant to the *Criminal Code* and the *Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism*, which are led by Public Safety Canada (PS) and Global Affairs Canada (GAC), respectively.

Protecting Privacy and *Charter* Rights

The Government of Canada is committed to combating money laundering and terrorist financing while respecting the Constitutional division of powers, the *Canadian Charter of Rights and Freedoms* (*Charter*) and the privacy rights of Canadians.

The PCMLTFA requires certain businesses to disclose private financial information to FINTRAC. Because FINTRAC may disclose this private financial information to law enforcement and intelligence agencies for investigation, this could impact privacy rights protected by section 8 of the *Charter* (the right to be secure against unreasonable search or seizure). However, the PCMLTFA has safeguards in place to ensure that those rights are protected. First, the PCMLTFA prescribes the information that FINTRAC can receive and disclose. The PCMLTFA sets out the specific law enforcement and intelligence agencies to which FINTRAC may disclose its financial intelligence. The PCMLTFA also limits the circumstances in which FINTRAC can disclose information to these agencies. FINTRAC must also 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. As such, FINTRAC is independent from law enforcement agencies and does not conduct investigations.

Further, the PCMLTFA requires the Privacy Commissioner of Canada to conduct regular 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 the review to Parliament.

The potential policy measures in this paper seek to maintain the balance between the need to deter and detect money laundering and terrorist financing activities while protecting the constitutional and privacy rights of Canadians.

The Last Parliamentary Review: Report and Recommendations

The last Parliamentary Review of the PCMLTFA was completed in 2013 with a report by the Standing Senate Committee on Banking, Trade and Commerce titled *Follow the Money: Is Canada Making Progress in Combatting Money Laundering and Terrorist Financing? Not Really*. In undertaking the Review, the Committee focused on three areas in the broad context of ensuring that the Regime provides "value for money" to the Canadian taxpayer.

Recommendations focused on the desired structure and performance of Canada's AML/ATF Regime regarding supervision, performance review, funding and expertise, as well as striking the appropriate balance between the sharing of information and the protection of personal information. Recommendations focused largely on greater and more timely information sharing amongst stakeholders and those government bodies directly involved in the Regime to assist in investigations and prosecutions of money laundering and terrorist financing. Finally, the Committee's work also resulted in recommendations surrounding the optimal scope and focus of the Regime. It was felt that Canada's Regime needed to be able to respond to developments in the global standards on money laundering and terrorist financing, advancements in technology and an increase in public awareness about the Regime.

The 2013 Report highlighted the inherent tension that is built into Canada's AML/ATF Regime between competing objectives: effectively detecting and deterring money laundering and terrorist financing while at the same time protecting privacy and the constitutional rights of Canadians.

Key Developments Since the Last Review

Since the last review in 2013, the environment in which Canada's AML/ATF Regime operates has continued to evolve. For example, the way people interact with and receive financial services has changed with the emergence of technologies that allow non-face-to-face interactions or foster an increasing array of complex financial products, including virtual currencies. In addition, financial crime is more sophisticated with the use of professional money launderers; complex corporate and legal structures that are increasingly being used to hide proceeds of crime and ensure anonymity; and the increase of cybercrime. Further, an important recent legal development in Canada was the Supreme Court decision in the *Federation of Law Societies of Canada*[8] case which ruled that the PCMLTFA provisions, as currently drafted for application to lawyers, are unconstitutional. This is an important decision in the history of the Regime and in light of the money laundering and terrorist financing risks that the legal profession poses, the Department is considering all of the options available. This issue is discussed further in Chapter 1 of this paper.

In addition, the Department and Regime partners have worked on a number of key projects, outlined below, that have all contributed to Canada's efforts to combat money laundering and terrorist financing.

Legislative and Regulatory Amendments

Since the last review, a number of legislative and regulatory amendments have been made to enhance Canada's legislative framework and further its mandate of deterring and detecting money laundering and terrorist financing activities. Some of these amendments have also improved Canada's compliance with the international standards set out by the Financial Action Task Force.

[8] Canada (Attorney General) v. Federation of Law Societies of Canada, 2015 SCC 7, [2015] 1 S.C.R. 401.

In 2014, legislative changes were enacted to address emerging risks, including virtual currencies, make online casinos subject to the PCMLTFA, and enhance the ability of FINTRAC to make disclosures related to threats to the security of Canada, consistent with the Government's response to the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182.

In 2015, legislative amendments were made to fight white-collar crime by allowing FINTRAC to disclose information related to money laundering to provincial securities regulators.

Further, regulatory amendments were made in 2016, pursuant to the legislative amendments made in 2014, to strengthen customer due diligence standards; close gaps in the Regime; improve compliance, monitoring and enforcement; and strengthen information sharing in the Regime. Examples include the introduction of more flexible client identification requirements and the introduction of obligations related to domestic politically exposed persons.

Most recently, legislative amendments were made in 2017 to expand the list of disclosure recipients that can receive financial intelligence related to threats to the security of Canada to include the Department of National Defence and the Canadian Armed Forces, to support more effective intelligence on beneficial owners of legal entities, and to make various technical and other changes to: strengthen the framework, support compliance, improve the ability of reporting entities to operationalize the PCMLTFA, and ensure the legislation functions as intended.

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

Carried out through coordinated efforts by Regime departments and agencies, the 2015 *National Inherent Risk Assessment* identified inherent money laundering and terrorist financing risks in Canada. This report was meant to increase the situational awareness of Canada's financial institutions, designated non-financial businesses and professions, and of all Canadians about money laundering and terrorist financing risks in Canada. The report provides an overview of the risks of money laundering and terrorist financing in terms of threats and vulnerabilities before the application of any mitigation measures, such as legislative, regulatory and operational actions that prevent, detect and disrupt money laundering and terrorist financing.

The assessment found that the money laundering threat was rated very high for corruption and bribery; counterfeiting and piracy; certain types of fraud; illicit drug trafficking; illicit tobacco smuggling and trafficking; and, third-party money laundering. Transnational organized crime groups and professional money launderers are the key money laundering threat actors in the Canadian context.

The terrorist financing threat was assessed for the groups and actors that are of greatest concern to Canada. The assessment indicates that there are networks operating in Canada that are suspected of raising, collecting and transmitting funds abroad to various terrorist groups. Despite these activities, the terrorist financing threat in Canada is not as pronounced as in other regions of the world, where weaker ATF regimes can be found and where terrorist groups have established more of a foothold, both in terms of terrorist activities and their financing.

Of the assessed sectors and products and services, domestic banks, corporations (especially private for-profit corporations), certain types of money services businesses and express trusts were rated the most vulnerable, or very high on the risk assessment scale. Many of the sectors and products are highly accessible to individuals in Canada and internationally and are associated with a high volume, velocity and frequency of transactions. They may also conduct a significant number of transactions with high-risk clients and be exposed to high-risk jurisdictions that have weak AML/ATF regimes and significant money laundering and terrorist financing threats. There are also opportunities in many sectors to undertake transactions with varying degrees of anonymity and to structure transactions in a complex manner.

Among the sectors assessed as presenting a high vulnerability to money laundering and terrorist financing are virtual currencies, especially convertible ones. This type of financial product is easy to access and presents a high degree of anonymity and transferability, which are attractive to a range of actors who wish to conceal the nature of financial transactions. This trend was identified in the most recent Parliamentary review of the AML/ATF regime, which led to amendments to the PCMLTFA in 2014 to govern activities related to virtual currencies within the regime. Since then, considerable work has been undertaken to develop technical and, in many cases, novel regulations in this space. Given their complexity and precedence, these new regulations have required a series of consultations with industry, legal and enforcement communities, and will be subject to public consultation once they are pre-published in the Canada Gazette.

It is important to note that money laundering and terrorist financing methods are constantly evolving as criminals develop new ways to exploit the financial system and legitimate businesses for their criminal purposes. Thus, it is important for the Government to be continually renewing its risk assessments.

Canada's Contribution to International Efforts

Strong national AML/ATF regimes enhance the integrity and stability of individual national financial sectors, but given the interconnectedness of the financial system, they contribute to protect the financial sectors of other countries and the global financial system as a whole.

As noted above, FATF is an inter-governmental body that sets standards for combating money laundering and terrorist financing, and ensures all members' AML/ATF regimes are held to the same criteria. The FATF monitors the implementation of these standards among its own 37 members and the more than 190 countries in the global network of FATF-Style Regional Bodies through peer reviews and public reporting. Canada is a founding member of the FATF and participates actively in its deliberations.

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. In addition, Canada supports regions where there is a higher risk for money laundering and terrorist financing, such as the Caribbean, the Middle East and North Africa through technical assistance. This assistance is designed to strengthen the capacity of financial systems in these regions to prevent them from being exploited as vehicles for money laundering and terrorist financing.

Canada's Mutual Evaluation Report by the FATF

In 2015, Canada underwent the FATF peer review process and the final report was published in September 2016. 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 a strong set of AML/ATF legislation and Regulations but with some weaknesses noted, which include: the limited availability of accurate beneficial ownership information to be used by competent authorities; the fact that the legal profession is not covered by the PCMLTFA; and that improvements could be made to increase the number of money laundering investigations and prosecutions.

In addition, the report found that Canada's AML/ATF framework could be strengthened by expanding the scope of the legislation to cover finance and leasing companies as well as unregulated mortgage lenders, and to apply new obligations to the designated non-financial businesses and professions sector in relation to politically exposed persons (PEPs), heads of international organizations and beneficial ownership information requirements.
The report also found that Canada could better combat money laundering and terrorist financing through investigating and prosecuting more complex money laundering and terrorist financing schemes, such as third party professional money launderers. The regulation of bulk cash transfers and of certain activities of lawyers and accountants and enhanced access to beneficial ownership information would assist in this pursuit.

Further, the report notes that making the penalties for violating these laws more proportionate and dissuasive would assist in the deterrence of money laundering and terrorist financing.

If implemented, the potential policy measures contained in this paper would contribute to strengthening Canada's AML/ATF Regime and improve Canada's overall compliance with the FATF Recommendations on AML/ATF, thereby helping to safeguard the integrity of the global financial system.

Tangible Results – Project Protect: A Case Study

Notwithstanding challenges identified in the international review, the Regime is making tangible contributions to the safety and security of Canadians within authorities currently provided.

Canada's AML/ATF Regime has been striving towards collaboration and perseverance, which are an integral part of producing financial intelligence and combatting money laundering and terrorist financing.

One such example is Project Protect, a reporting entity-led initiative that mobilized partners across the country to combat human trafficking in the sex trade. This collaboration resulted in the December 2016 publication of FINTRAC's Operational Alert, Indicators: The Laundering of Illicit Proceeds from Human Trafficking for Sexual Exploitation. The Alert focused on the types of financial transactions, financial patterns and account activity that may raise suspicions of money laundering and trigger the requirement to send a suspicious transaction report to the Centre. These efforts led to a significant increase in the awareness of reporting entities towards this type of money laundering and a corresponding increase in the number of suspicious transaction reports submitted to FINTRAC.

The financial intelligence provides insight into the operation of a human trafficking scheme. By following the money trail, police can identify assets purchased with the proceeds of crime, uncover other perpetrators and victims through their financial relationships, and corroborate a victim's story, which could help to secure convictions.

Scope and Outline of the Discussion Paper

The potential policy measures described in this paper focus on improving the PCMLTFA and its Regulations to support the effectiveness of the broader AML/ATF Regime. Reporting entities play a very important role in detecting and deterring money laundering and terrorist financing activities. At the same time, the framework must strive to minimize the compliance burden and cost associated with the measures required to detect and deter money laundering and terrorist financing activities. In addition to framework-focused measures, a number of potential measures touch on other legislative provisions that support the objectives of the AML/ATF Regime. Potential areas for improvement have been identified through discussions with Regime departments and agencies and members of the Advisory Committee on Money Laundering and Terrorist Financing.

The analysis and motivations that led to these ideas include:

- reviewing Canada's AML/ATF legislative framework to respond to developments in the risk environment and in the marketplace;
- responding to stakeholder concerns, raised by both the private sector and federal government partners, particularly law enforcement and intelligence agencies;
- responding to findings of the Assessment of Inherent Risks of Money Laundering and Terrorist Financing in 2015; and,
- meeting Canada's international commitments, notably by improving our compliance with the Recommendations of the FATF and in particular, responding to the findings contained in Canada's Mutual Evaluation published by the FATF in 2016.

The measures are organized around the following key themes:

- Legislative and Regulatory Gaps
- Enhancing the Exchange of Information While Protecting Canadians' Rights
- Strengthening Intelligence Capacity and Enforcement
- Modernizing the Framework and its Supervision
- Administrative Definitions and Provisions

The Government recognizes that measures to enhance Canada's AML/ATF legislative framework should strike the appropriate balance among sometimes-conflicting objectives at play in the conduct of the Regime. These include the aim to not place an undue burden on reporting entities, which are on the front lines of the fight against money laundering and terrorist financing. Similarly, risk-based approaches should continue to be incorporated where appropriate to maximize the effectiveness of efforts. The more expansive use of financial intelligence can support the effectiveness of the Regime to improve the safety and security of Canadians, while respecting their privacy and constitutional protections.

This discussion paper makes reference to persons and entities that have obligations under the PCMLTFA, which include:

- financial entities (banks, credit unions and caisses populaires, trust and loan companies);
- Crown corporations that take deposits, or sell or redeem money orders;
- life insurance companies, brokers and agents;
- securities dealers;
- money service businesses;
- accountants and accounting firms;
- legal counsel and legal firms;[9]
- British Columbia notaries, public and Notary Corporations;
- real estate brokers, sales representatives and developers;
- dealers in precious metals and stones; and
- casinos.

As well, if new provisions were adopted, new businesses and sectors or persons in Canada that could be covered by the regime's provisions include the white-label ATM industry; pari-mutuel or horse racing sector; auto dealers; company service providers; mortgage insurers, land registries and title insurance companies; non-federally regulated mortgage lenders; armoured car companies; jewellery auction houses; and financing, and leasing and factoring companies.

Finally, other changes in policy directions could also have implications for parties other than those who have obligations under the PCLMTFA, including clients of reporting entities such as politically exposed persons (PEPs).

The Department of Finance is seeking views on these potential policy directions in order to position Canada's anti-money laundering and anti-terrorist financing legislative framework for the future. The intention is to provide an opportunity for stakeholders to review these propositions, including for the benefit of the Parliamentary Committee that will undertake a review of the administration and operation of the PCMLTFA, as required under the legislation.

Other amendments and issues for future consideration may also be considered at a later time. For example, it is anticipated that recommendations will be put forward through the Parliamentary review of the PCMLTFA.

Full consideration will be given to the input and comments received, including in relation to potential compliance challenges that reporting entities could face as a result of the measures contained in this paper and the timing of possible implementation.

[9] The provisions relating to the legal profession are non-operative, as they have been ruled unconstitutional by the Supreme Court of Canada in 2015.

Chapter 1 – Legislative and Regulatory Gaps

This chapter explores a broad range of issues that could be implemented to improve Canada's AML/ATF framework. These include many areas that involve high risk activities. However, it is important to note the balance that must be struck between capturing financial activity that poses money laundering and terrorist financing risk and the amount of resources, either public or private, that needed to comply with obligations and analyze that activity. Part of achieving this balance is to design a framework, and any subsequent obligations that flow from it, to be aligned with the risk. This is supported by adopting a collaborative approach with the private sector focusing on risks, including consideration for their own reputational risk.

Corporate Transparency

The Panama Papers and Bahamas leaks of 2016 and the Paradise Papers release of 2017 highlighted how corporate vehicles (e.g., companies and trusts) can be used to conceal the true ownership of assets for the purposes of money laundering, terrorist financing, and tax evasion and avoidance. This resulted in heightened and sustained international and domestic attention to the importance of corporate ownership transparency.

Timely access for competent authorities to accurate and up-to-date beneficial ownership information is recommended within the FATF standards and is vital for combatting illicit financial flows including money laundering, terrorist financing and tax evasion. The G20 has called on countries to strengthen implementation of the international standards on transparency and beneficial ownership of legal persons and legal arrangements set by the FATF and availability of beneficial ownership information and its international exchange. International peer reviews have highlighted areas for improvement for Canada to effectively implement these standards.

Canada does not have a central registry of beneficial ownership information, and information requirements are spread across a number of different statutes, including incorporation, tax, and financial authorities. Jurisdiction over incorporation is shared between the federal and provincial/territorial governments, with approximately 9% of corporations in Canada established under the federal *Canada Business Corporations Act* (CBCA). Provinces and territories have jurisdiction over incorporation of companies with provincial objects, and partnerships.

Corporate information reporting requirements are in place at the federal and provincial levels; however, there are differences between jurisdictions in requirements related to the collection, disclosure, and access to this information. In addition, risks associated with bearer shares[10] are not fully mitigated across all jurisdictions and there are few measures to mitigate risks associated with nominee shareholders which can be used to conceal true controlling interests.

In terms of record keeping responsibilities, there are no requirements to collect or disclose beneficial ownership information at the corporate level. Existing corporate registries have minimal, if any, enforcement of reporting requirements and there is limited capacity in place to ensure the information that is collected is accurate and up-to-date.

A critical first step toward improved corporate transparency for competent authorities in Canada's federal system is to provide clear, standardized direction to corporations as to what information they should record and maintain in terms of their beneficial ownership. The specification of information standards, ideally harmonized across jurisdictions and statutes, will in turn facilitate the consideration of different models of collecting this information, for example, into repositories or registries – and allow a more tangible debate among Canadians as to whether such information should be open to the public.

Since 2014, the PCMLTFA requires financial institutions, securities dealers, life insurance and money services businesses to collect beneficial ownership information for corporations, trusts and other entities and take reasonable measures to confirm the accuracy of information collected.

The Minister of Innovation Science and Economic Development tabled Bill C-25 in September 2016 to support Canada's compliance with the FATF standards with respect to the prohibition from using bearer shares. While the CBCA has required that shares be in registered form since 1975, the Bill includes amendments to the CBCA and the *Canada Cooperatives Act* that, once passed, will prohibit the issuance of options and rights in bearer form, and require that corporations presented with bearer instruments convert them into registered form.

The 2017 federal Budget indicated the Government's commitment to improving corporate and beneficial ownership transparency to provide safeguards against money laundering, terrorist financing, tax evasion and tax avoidance, while continuing to facilitate the ease of doing business in Canada. As announced in Budget 2017, the Government of Canada has been collaborating with the provinces and territories to develop a national strategy to strengthen the transparency of legal persons and legal arrangements and improve the availability of beneficial ownership information. In addition, the Department of Finance is examining ways to enhance the tax reporting requirements for trusts in order to improve the collection of beneficial ownership information.

[10] A bearer share is an equity security wholly owned by whoever holds the physical stock certificate. The issuing company does not register the owner of the stock or any transfer of ownership. The company disperses dividends to bearer shares when a physical coupon is presented to the company and because the share is not registered, transferring the ownership of the stock involves only delivering the physical document.

At the December 2017 meeting of Canada's Finance Ministers, Ministers announced an agreement in principle to pursue legislative amendments to federal, provincial and territorial corporate statutes to i) ensure corporations hold accurate and up to date information on beneficial owners that will be available to law enforcement, tax and other authorities; and ii) eliminate the use of bearer shares and bearer share warrants or options and to replace existing ones with registered instruments. Best efforts will be made to bring these amendments into force in all jurisdictions by July 1, 2019. Beyond this important first step towards a national strategy, Ministers also agreed to continue to examine mechanisms to improve timely access to beneficial ownership information by law enforcement and other authorities and to assess risks associated with other legal vehicles.

Key considerations to inform further work towards a national strategy that supports good corporate governance and ensures safeguards against misuse of corporations include defining where and how information should be accessed (e.g., whether beneficial information should be collected in a central registry(s) or repository, whether it should be made publicly available) and cost and administrative burdens for the private sector in Canada.

The Department is seeking views on how to improve corporate ownership transparency and mechanisms to improve timely access to beneficial ownership information by authorities while maintaining the ease of doing business in Canada. This includes considering different beneficial ownership registry models and whether information should be made public. The Department is also seeking views on risks associated with legal entities that are not corporations, such as legal partnerships.

The Legal Profession in Canada

Legal professionals who conduct financial transactions on behalf of clients can pose a money laundering and terrorist financing risk, in particular at the placement and layering stages of money laundering, and therefore present risks to the integrity of both domestic and global financial systems. This risk has also been recognized by the FATF. In a report titled *Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals*, the FATF found that criminals seek out the involvement of legal professionals in their money laundering and terrorist financing activities, sometimes because a legal professional is required to complete certain transactions, and sometimes to access specialised legal and notarial skills and services which could assist the laundering of the proceeds of crime and the funding of terrorism.[11]

In the 2015 National Inherent Risk Assessment, the legal sector was assessed as posing a high risk of money laundering and terrorist financing in Canada. This sector has a large number of practitioners with specialized knowledge and expertise that is vulnerable to being exploited, wittingly or unwittingly, for illicit purposes. It is the financial services offered by lawyers that make lawyers gatekeepers to the financial system and that make them the most vulnerable. In addition to conducting wire transfers, issuing cheques and accepting cash,

[11] For a copy of the Report see - http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20and%20TF%20vulnerabilities%20legal%20professionals.pdf

these services include establishing trust accounts, forming and managing corporations and legal trusts, carrying out real estate and securities-related transactions and setting up and managing charities. The legal profession offers vulnerable services to a range of individuals and businesses and frequently act as a third party in transactions. The client profile of the legal sector is believed to include a combination of Politically Exposed Persons, who are people who occupy a position of influence in a government or military, clients in vulnerable businesses and professions, and clients whose activities are conducted in locations of concern, though this list is not exhaustive. The legal profession normally interacts directly with clients but can also conduct business indirectly as well. For these reasons, the application of the rules from Canada's AML/ATF framework to lawyers is important to support efforts to detect and deter money laundering and terrorist financing.

The provision of some key services by legal counsel is protected by solicitor-client privilege, which can make the business relationship more opaque to law enforcement investigations. In February 2015, the Supreme Court of Canada ruled that the PCMLTFA provisions, as currently drafted for application to lawyers, are unconstitutional. In particular, the Court found that provisions requiring lawyers to collect client information, keep records and have lawyers' offices undergo compliance searches violated section 7 (right to life, liberty and security of the person) and section 8 (protection against unreasonable interference with a reasonable expectation of privacy) of the *Charter*. However, 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.

Over the past couple of years, media reports have highlighted the role lawyers can play in various questionable dealings including: setting up shell corporations; appointing nominee directors; and falsifying records as referenced in the Panama Papers; or the inappropriate use of trust accounts with or without offshore connections for corporate or real estate transactions here in Canada. The lack of inclusion of the legal profession in Canada's AML/ATF framework is a major deficiency that negatively affects Canada's global reputation as was highlighted in Canada's recent FATF evaluation report in 2016.

As the Government continues to work on this issue, we look forward to further exploring with the law societies how we can address the issue of legal professionals being used to facilitate money laundering and terrorist financing. We also note that the Federation of Law Societies of Canada is currently consulting on amendments to the profession's model rules on anti-money laundering and anti-terrorist financing. The Government believes that legal professionals are an integral part in combatting money laundering and terrorist financing. Through this lens, we look forward to engaging with the law societies so they may become a meaningful part of Canada's AML/ATF Regime.

The Department continues to believe that the application of the rules to the legal profession is important to maintain the integrity of Canada's AML/ATF framework. It is important that when lawyers act as financial intermediaries they take measures to ensure they are not unwittingly used to launder money or to finance terrorism. We would seek to engage Canada's law societies and bar associations to work with the Government to find solutions. Furthermore, it is the Department's intention to develop constitutionally compliant legislative and regulatory provisions that would subject legal counsel and legal firms to the PCMLTFA. The Department is working with Justice Canada on the impact of the decision toward next steps in due course.

Expanding the Scope of the PCMLTFA to High Risk Areas

Several legislative and regulatory gaps in regime coverage were identified since the last Review of the framework, notably through the *Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada* and the recent FATF evaluation of Canada. Many of these gaps involve clarifying existing requirements for reporting entities or expanding the scope and depth of the obligations under the PCMLTFA to new types of businesses in Canada. Adding new types of reporting entities would mean establishing new requirements relating to client identification, due diligence, record-keeping and reporting of certain transactions for those sectors.

Many of the measures that have been identified could potentially create a large number of new reporting entities, creating burden on the private sector and posing challenges to those responsible for overseeing compliance. As such, there could be significant costs associated with implementing some of these measures for both the private and public sector entities involved. The increased reporting that would ensue could also create privacy concerns for Canadians. In evaluating each measure, the costs of addressing the identified risk must be weighed against the potential benefit of preventing or tracing ML/TF activity in the identified sectors.

Expanding Requirements for Designated Non-Financial Businesses and Professions (DNFBPs) in relation to Politically Exposed Persons (PEPs), Head of International Organizations (HIOs) and Beneficial Ownership

PEPs and HIOs are persons entrusted with a prominent position that typically comes with the opportunity to influence decisions and the ability to control resources. The influence and control a PEP or HIO has puts them in a position to impact policy decisions, institutions and rules of procedure, as well as the allocation of resources and finances, which can make them vulnerable to corruption and money laundering. Corruption is an international issue that impacts all countries, and for that reason, the FATF recommends that all countries have PEP and HIO obligations in place for all reporting entities.

Currently, only four reporting entity sectors have obligations relating to PEPs and HIOs in Canada. These are: financial entities, securities dealers, money service businesses, and life insurance companies. They are required to take reasonable measures in certain situations to determine if a client is a foreign PEP, a domestic PEP, a HIO, a prescribed family member[12] or a close associate. Other reporting entity sectors currently covered by the PCMLTFA do not have such obligations.

[12] A prescribed family member is their spouse or common-law partner; their child; their mother or father; the mother or father of their spouse or common-law partner; or a child of their mother or father.

As above, beneficial ownership refers to the identity of the natural person who ultimately controls a corporation or entity, which cannot be another corporation or another entity. Currently, only four reporting entity sectors have obligations to collect beneficial ownership information from corporations or other complex legal entities. These are: financial entities, securities dealers, money service businesses, and life insurance companies, brokers and agents. The Government recognizes the challenges faced in confirming beneficial ownership information, which is why the Government continues to work collaboratively on the issue of corporate ownership transparency as described above.

Canada's FATF Mutual Evaluation report found that the requirements related to PEPs, HIOs and beneficial ownership were not broad enough and did not extend to designated non-financial businesses and professions.

Definition of Head of an International Organization (HIO)

As described above, a HIO is a person entrusted with a prominent position that typically comes with the opportunity to influence decisions and the ability to control resources. A given HIO's influence and control puts them in a position to impact policy decisions, institutions and rules of procedure, as well as the allocation of resources and finances; this can make them vulnerable to corruption. The PCMLTFA currently defines a HIO as "the head of an international organization that is established by the governments of states or the head of an institution of any such organization". For example, this includes organizations established by means of a formally signed agreement between governments such as the International Criminal Court or the United Nations.

Over the past several years, corruption and bribery scandals have been linked to organizations such as the International Olympic Committee, the Fédération Internationale de Football Association, the Union of European Football Association and the Fédération Internationale de l'Automobile. While not established by governments of states, these types of international bodies also have considerable political influence in society and on the global economy, and they control significant financial resources. Some countries, such as Switzerland, have already incorporated these types of organizations into their definition of HIOs. Such an amendment would help strengthen Canada's AML/ATF framework by including HIOs of organizations where increased risks of money laundering and terrorist financing may appear.

Politically Exposed Person (PEP) Determination of Beneficial Owners

As described above, the influence and control of PEPs can make them vulnerable to corruption and money laundering. Moreover, as the release of the Panama and Paradise Papers highlighted, corporate vehicles such as companies and trusts may be used to conceal ownership of assets and potentially proceeds of crime and corruption, including by PEPs. Currently, the PCMLTFA requires financial institutions, securities dealers, life insurance companies, brokers and agents and money services businesses to obtain and take reasonable measures to confirm information on the beneficial ownership of clients that are corporations, trusts or other entities. However, determination of whether beneficial owners identified are PEPs, and application of prescribed measures to mitigate risks associated with PEPs, is not currently required by the Regulations.

Clarify the Definition of Politically Exposed Domestic Person (PEPs)

As described above, designated reporting entities (financial entities, life insurance companies, agents and brokers, securities dealers and money services businesses) are required under the PCMLTFA to undertake measures to determine if their clients are PEPs, as described above. The definition of a domestic PEP means:

- a Governor General;
- lieutenant governor or head of government;
- member of the Senate or House of Commons or member of a legislature;
- deputy minister or equivalent rank;
- ambassador, or attaché or counsellor of an ambassador;
- military officer with a rank of general or above;
- president of a corporation that is wholly owned directly by Her Majesty in right of Canada or a province;
- head of a government agency;
- judge of an appellate court in a province, the Federal Court of Appeal or the Supreme Court of Canada;
- leader or president of a political party represented in a legislature; or
- a mayor.

A more technical matter relates to the implementation of the domestic PEP requirements, as FINTRAC has received inquiries on the meaning of various positions contained in the definition. For example, questions were asked to clarify if the term "mayor" applied to other equivalent positions (e.g., Reeves, Wardens, etc.) and to clarify if the definition also includes First Nation Chiefs. First Nations Chiefs are considered part of the definition of PEPs as they are public officials leading organizations with control and influence over large amounts of public funds due to the nature of their position. The explicit inclusion of First Nations Chiefs would place these positions on the same level as other people who hold similar positions.

White Label Automated Teller Machines (WLATMs)

Privately-owned automated teller machines, referred to as "white label" since they are not branded by a financial institution, provide cash dispensing services by linking financial institutions via payment networks such as Interac, VISA, and MasterCard.

In 1996, the Competition Tribunal ruled that the major financial institutions in Canada were abusing their dominant position with regards to ATMs. Among the remedies stipulated in the ruling was ATMs could be privately-owned as opposed to being owned by a financial institution, leading to the creation of the WLATM industry. In this context, independent operators (acquirers) are allowed to be part of the networks and provide network access to persons or companies who own WLATMs, charging fees for doing so.

WLATMs may be vulnerable to abuse because they can be owned by any person or entity, including criminals, either directly or through nominees, and can be loaded with large amounts of cash that are proceeds of crime as part of the placement stage of the money laundering process.

In 2008, the Department worked with representatives from the Canadian payment networks to develop a set of voluntary and self-enforced industry rules in order to address money laundering and terrorist financing risks posed by WLATMs, including measures such as client identification, record keeping and an annual review by a qualified auditor. However, law enforcement continues to express concerns with the WLATM industry, including the use of these ATMs by organized crime groups in Canada.

In 2012, Quebec became the first province to strengthen its regulation of the WLATM industry by defining privately-operated ATMs as money services businesses, implementing a registration process and requiring information regarding the business owner and their planned activities prior to registration.

Although this industry can be highly vulnerable to money laundering and terrorist financing, as evidenced in the *Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada*, none of the participants involved in the WLATM industry are currently subject to the PCMLTFA. While there is a spectrum of regulatory options available, this different treatment represents both a money laundering and terrorist financing risk and a commercial level-playing field issue in that ATMs associated with more established financial institutions are subject to more strict oversight.

Pari-Mutuel Betting and Horse Racing

Pari-mutuel betting is a betting system in which 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. The pari-mutuel system is used in gambling on horse racing.

This sector presents money laundering vulnerabilities similar to the casino sector, given that the methods used to launder money through horse racing are similar to those used in casinos, which have been covered by the PCMLTFA since 2007. For example, criminals can convert small denominations of cash generated from criminal activities into larger bills through pari-mutuel betting. Similarly, funds can be deposited into player accounts, either in person or online, in exchange for cashier's cheques or wire transfers. The FATF has found that there is significant money laundering risk through this type of activity in Canada.

In the casino sector, the provinces conduct, manage and regulate the gaming. In horse racing, 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.

Leveraging Information in the Real Estate Sector

Entities and persons in the real estate sector that are already covered in the PCMLTFA include real estate brokers, sales representatives and developers. However, other organizations such as mortgage insurers, land registries and title insurance companies[13] are not and play an integral role within the real estate sector in Canada. Due to the type of information that they currently receive in the normal course of their activities, these entities are in a unique position to gather and report information related to money laundering and terrorist financing. They can offer a different view or lens into financial transactions.

The *Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada* identified four commonly employed methods to launder the proceeds of crime through real estate transactions: purchasing or selling properties; accessing financial institutions through gatekeepers; assisting the purchase or sale of property; and using mortgage and loan schemes. These activities were assessed as presenting a high risk for money laundering in Canada and this different treatment represents a level-playing field issue. In addition, other countries such as the United States have already introduced requirements for these types of entities.

Non-Federally Regulated Mortgage Lenders

The non-federally regulated mortgage sector is complex and composed of various kinds of entities subject to different regulatory obligations. Mortgage lenders can be publicly-traded; privately-held or owned by private equity companies; wholly or partly owned by a Canadian federally regulated financial institution or by a foreign financial institution. They include companies such as mortgage finance companies, real estate investment trusts, mortgage investment corporations, mutual fund trusts, syndicated mortgages or individuals acting as private lenders.

[13] Companies that offer insurance policies that protect residential and commercial property owners and/or their lenders against losses related to the property's title or ownership.

Mortgages can be used to launder money by purchasing property using a mortgage and making the mortgage payments using proceeds of crime. The property can then be recycled into the real estate sector to generate what appears to be legitimate sources of income. In addition, there are various complex loan and mortgage schemes, including mortgage fraud, that have been identified as a money laundering risk in the *Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada* and in Canada's FATF evaluation.

Designated Non-Financial Businesses and Professions (DNFBPs) Non-Transactional Based Activities

Currently, DNFBPs include accountants and accounting firms; real estate brokers, sales representatives; real estate developers; casinos; dealers in precious metals and stones; and British Columbia notaries public and notary Corporations. They are covered in the PCMLTFA for activities that involve financial transactions, such as conducting large cash transactions of $10,000 or more. However, some DNFBPs such as accountants, are also involved in other activities that have been assessed as high risk through the *Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada* and in Canada's FATF Mutual Evaluation. These activities include creating, operating or managing legal persons or arrangements, including organizing contributions for these activities, as well as managing a client's money, security or other assets (including managing bank, savings and securities accounts). These activities represent the same risk that legal professionals are exposed to when they conduct similar activities, including addressing the issue of beneficial ownership.

Company Service Providers

Businesses and professionals that provide services related to the formation and administration of companies are exposed to high inherent money laundering risks, particularly when they are engaged in managing corporations for their clients. These services can include company or partnership formation, providing a registered business address, acting as (or arranging for someone to act as) a director or nominee shareholder of a company, managing financial affairs and annual corporate and tax filings for a company. As discussed above, legal and accounting firms, as well individual lawyers and accountants, may provide these types of corporate services; however, there are also entities specialized in the provision of such services. Company service providers can be used wittingly or otherwise to facilitate the misuse of corporations for money laundering, terrorist financing and tax evasion. For example, offshore corporations and trusts can be quickly established and managed by a local company services provider, and can be structured to conceal the beneficial owner and to disguise and convert illicit proceeds. These activities represent the same risk that legal professionals pose when they conduct similar activities including addressing the issue of beneficial ownership.

Prohibiting the Structuring of Transactions to Avoid Reporting

Structuring transactions by breaking them down into many smaller ones in order to avoid financial transaction reporting, also known as "smurfing", can either be done by the institution or by the client themselves.

The PCMLTFA requires reporting entities to report financial transactions that are prescribed in the Regulations, including large cash transaction, international electronic funds transfers and casino disbursement reports. There is also an obligation to report if multiple smaller transactions equal $10,000 or more within a 24-hour period. However, there is no explicit prohibition against reporting entities structuring their business models and delivery channels or mechanisms for conducting transactions in such a way as to avoid triggering reporting requirements. Also, it is not illegal for clients to structure their financial transactions in order to avoid scrutiny and financial transaction reporting. In other countries, such as the United States and Australia, it is a criminal offence to structure financial transactions in this way.

The Department is considering the creation of a criminal offence for an entity or individual to structure transactions and to specifically prohibit reporting entities from conducting transactions in such a way as to avoid transaction reporting.

Standardize Record Keeping and Client Identification

Under the PCMLTFA, record keeping and client identification obligations are triggered for certain types of activities or when financial transactions reach a certain threshold. For example, financial entities and money services businesses identify clients for foreign currency exchange transactions at $3,000 or more and certain businesses must keep a record of receipt of funds at $1,000 or more.

While financial transaction reporting is essential for FINTRAC to conduct its analysis and produce financial intelligence, records that are kept are primarily for law enforcement and other competent authorities to request and obtain under different legislative and judicial mechanisms for their operations and investigations. Moreover, accurate and comprehensive records help reporting entities to conduct ongoing monitoring and assess the risks of money laundering and terrorist financing of their business activities. The Department has heard that the varied dollar amount thresholds sometimes creates complexity which may result in a barrier to compliance and is not balanced against the desired outcomes of the regulatory framework.

Finance, Lease and Factoring Companies

The financing and leasing sector in Canada is large, consisting of large domestic and international lessors and small independent ones. This sector provides a range of leasing services to individuals and businesses across Canada and internationally. The factoring sector in Canada supplies loans to businesses to address short-term cash flow needs.

These companies allow a variety of payment methods such as cash, electronic funds transfers (EFTs), money orders and cheques, thereby offering opportunities to be used in the placement, layering and integration stages of the money laundering process. In Canada's FATF Mutual Evaluation, the absence of coverage of finance, leasing and factoring companies was noted. In addition, these sectors have been identified as a money laundering risk in the *Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada.*

Armoured Cars

Armoured car companies in Canada offer services that specialize in the secure transportation of cash and other valuable materials, such as precious metals (e.g., gold). In recent years, the services offered by armored car companies have expanded to include collecting and delivering cash from white label ATMs, transporting other bulk cash and valuable materials between businesses, and taking customer account deposits.

A key source of concern is that funds are collected and pooled into accounts controlled by the armored car company, and are then transferred electronically into the accounts of their customers, ultimately obscuring the true origin of the cash. This anonymity can be leveraged by other businesses, such as white label ATMs, at a high-risk for money laundering.

Other jurisdictions, such as the United States, have integrated the armoured car sector as part of their AML/ATF regimes. The absence of AML/ATF regulation in Canada of the armoured car industry creates an environment that enables and facilitates the anonymous movement of bulk cash. Without mitigation measures in place, these types of services could facilitate money laundering and terrorist financing, as there are no requirements to conduct client identification, keep records, collect source of funds information, or report.

High-Value Goods Dealers

High-value goods such as luxury goods, automobiles, boats and yachts, as well as art and antiquities can be a useful way to store value or proceeds of crime. The purchase of luxury goods can also form part of a criminal lifestyle. There are many ways to launder proceeds of crime through such goods, including giving them to family, friends and employees of criminal enterprises as payment for services; returning high-value goods paid for in cash and obtaining a refund by way of cheque; or selling such goods on the secondary market.

Various jurisdictions around the world, including the United States and the United Kingdom, have already integrated high-value goods dealers as part of their AML/ATF regimes given the high money laundering risk that they pose. Canada's FATF Mutual Evaluation report identified that dealing in high-value goods, including auction houses, is an activity that is highly vulnerable to money laundering and terrorist financing risks. The report noted that Canada's AML/ATF requirements have not been extended to these sectors, except for dealers in precious metals and stones (DPMS). There is a spectrum of regulatory options available, taking into account the potential administrative burden, to find the appropriate regulatory framework.

Jewellery Auction Houses

As mentioned above, dealers in precious metals and stones (DPMS) currently have requirements under the PCMLTFA; however, the activity of jewellery auction houses is excluded from these requirements. Many of the DPMS risks and vulnerabilities are also present in the jewellery auction house industry. Potential methods to launder money include: the purchase of precious metals and jewellery with the proceeds of crime and their subsequent sale; the use of accounts held with auction houses for laundering the proceeds of crime; and the ability to purchase or sell precious metals and jewellery with relative anonymity.

Bringing the activities of jewellery auction houses into the PCMLTFA legislative framework would create a level-playing field within the DPMS sector and ensure consistency in reporting and information requirements for all businesses dealing in precious metals and stones.

The Department is seeking views on risks associated with the areas referenced in this chapter and measures that would address them.

Chapter 2 – Enhancing the Exchange of Information While Protecting Canadians' Rights

While protecting the privacy of Canadians is paramount, information sharing, especially between public and private sector entities, is critical for combatting money laundering and terrorist financing. For that reason, there is a need both for safeguards against the unrestricted flow of information to protect Canadians' rights and privacy and having the ability to share the information necessary to protect the financial security of Canadians and the Canadian financial system. This section examines options to improve information sharing, through adding additional disclosure recipients; improving the understanding of information sharing options between the private sector to address cases of fraud; enhancing information sharing on methods and trends of ML/TF between FINTRAC and the private sector; and improving information sharing under international legal cooperation agreements. Better aligning the timing of the review of the Act by the Privacy Commissioner with experience to date also bears some discussion.

Each of these possible initiatives should be examined in light of the impact that they would have on the privacy of Canadians as well as their utility in enhancing efforts to combat ML/TF. This inherent tension helps to ensure that information sharing is informed by the utility of the information for both law enforcement and the private sector in their operations.

More Effectively Sharing Information Within Government

FINTRAC is currently authorized to disclose designated information (e.g., account holder name, transaction amount and date) to Canadian law enforcement agencies and other agencies such as the Canada Border Services Agency, the Canada Revenue Agency and the Canadian Security Intelligence Service in specific circumstances where there are reasonable grounds to suspect that information would be relevant to investigating or prosecuting money laundering or terrorist financing or threats to the security of Canada.

The Competition Bureau

The Competition Bureau is an independent federal law enforcement agency that is responsible for the administration and enforcement of the *Competition Act,* as well as the *Consumer Packaging and Labelling Act* (except as it relates to food), the *Textile Labelling Act* and the *Precious Metals Marking Act*. The Bureau ensures that Canadian businesses and consumers prosper in a competitive and innovative marketplace. The key provisions of the *Competition Act* relate to ensuring truth in advertising (e.g. through combatting deceptive marketing practices and mass marketing fraud), investigating cartels, preventing abuse of market power and reviewing mergers. The Bureau also has a wide range of powers to investigate anti-competitive behaviour and litigate alleged civil and criminal violations before the courts. In order to fulfill this objective, the Bureau would benefit from becoming a disclosure recipient in the PCMLTFA in order to receive financial intelligence from FINTRAC. According to the *Assessment of Inherent Risks of Money Laundering and Terrorist*

Financing in Canada, mass marketing fraud is considered to be a very prevalent threat in Canada. As such, it is proposed to amend subsection 55(3) of the PCMLTFA to give FINTRAC the authority to disclose financial intelligence to the Competition Bureau.

Revenu Québec

Revenu Québec has similar responsibilities to the Canada Revenue Agency (CRA) in administering personal income tax in Québec. In recent years, Revenu Québec has intensified its efforts to combat tax fraud and tax evasion by conducting criminal investigations. However, Revenu Québec, unlike CRA, is not a disclosure recipient listed in the PCMLTFA and therefore cannot receive financial intelligence from FINTRAC. Given the nexus between money laundering, terrorist financing, and tax related offences, and given the nature of the work undertaken by the provincial agency, it is proposed to amend subsection 55(3) of the PCMLTFA to give FINTRAC the authority to disclose financial intelligence to Revenu Québec.

A Stronger Partnership with the Private Sector

Information Sharing and the Personal Information Protection and Electronic Documents Act (PIPEDA)

The Government takes privacy and the protection of personal information very seriously. PIPEDA sets out measures to protect personal information and requirements for private-sector organizations to obtain consent when they collect, use or disclose an individual's personal information. For example, PIPEDA gives individuals the right to know why an organization collects, uses or discloses their personal information, the right to expect an organization to protect their personal information by taking appropriate security measures, and the right to complain about how an organization handles their personal information if they feel their privacy rights have not been respected.

In certain circumstances, in order to protect the financial security of Canadians and the Canadian financial system, PIPEDA allows for the disclosure of certain personal information without consent or knowledge of the individual, for example in cases of suspected fraud.

Circumstances and protocols surrounding the effective and appropriate exchange of information not only with government institutions but also between private sector organizations should be examined with a view to ensure clarity for all stakeholders and to protect from criminal/civil liability.

Engagement Model for Information Sharing with the Private Sector

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. The information can also be in the form of studies, methods and trends used to educate the public, including the reporting entities, on money laundering and terrorist financing issues, such as Project Protect discussed earlier in this paper.

Good collaboration between reporting entities, FINTRAC, national security agencies and law enforcement is an important aspect to combatting money laundering and terrorist financing. It allows for the sharing of expertise and intelligence on money laundering and terrorist financing methods, and information on clients or transactions potentially related to money laundering and terrorist financing.

Other countries such as the United Kingdom, the United States, and Australia have initiatives in place where expertise and information are shared both within Government and with the private sector on methods, trends, and financial transactions. This exchange of information, on a timelier basis, makes for more effective decision making by reporting entities in due diligence, transaction monitoring and reporting for AML/ATF purposes. It also enhances law enforcement's ability to investigate and prosecute money laundering and terrorist financing.

Strengthening our Partnerships Internationally

Mutual Legal Assistance

The ability of countries to engage in effective international cooperation, including the capacity to effectively provide and obtain mutual legal assistance in criminal matters, is critical to the fight against money laundering and terrorist financing, including their successful prosecution, given the international nature of the crimes (e.g., the movement of money across borders to facilitate money laundering and terrorist financing). This is a longstanding feature of international law. Concerns about Canada's effectiveness in the area of international cooperation, including mutual legal assistance, were raised during Canada's FATF evaluation.

A steady and significant increase in the volume of mutual legal assistance requests made to and from Canada in recent years, coupled with gaps identified in Canada's mutual legal assistance framework, adversely impact Canada's capacity in the area of mutual legal assistance. This is particularly the case for digital evidence requests which have increased exponentially due to the increase in the use of personal electronic devices (e.g., smart phones) and social networking. Further, Canada's existing mutual legal assistance treaty network requires modernization to adequately reflect evolving technology and the increasing globalization of crime to ensure that Canada can provide and obtain mutual legal assistance in money laundering and terrorist financing legal proceedings without undue delay.

Evidence and the Mutual Legal Assistance in Criminal Matters Act (MLACMA)

In general, evidence must comply with the requirements of the Canada Evidence Act (CEA) to be admitted into Canadian criminal proceedings. The MLACMA provides Canadian Courts with more flexibility in admitting and dealing with foreign gathered evidence obtained via a Mutual Legal Assistance Treaty request. However, foreign officials and the employees of foreign businesses who provide evidence, such as documents and business records, sometimes have difficulty complying with the requirements of evidence admissibility in Canada laid out in both the CEA and the MLACMA, which can result in significant delays in obtaining admissible foreign evidence for Canadian police and prosecutors.

In Canada's evaluation, the FATF noted that Canada seldom requests or obtains international assistance in relation to Canadian investigations and prosecutions of money laundering and terrorist financing. A key issue in mutual legal assistance is ensuring that the evidence will be admissible when it is obtained from abroad. Potential legislative amendments would take into account recent court decisions pertaining to privacy rights in digital evidence and would increase the efficiency and effectiveness of Canada's mutual legal assistance framework. This, in turn, could increase Canada's capacity to prosecute money laundering or terrorist financing cases using information from abroad given the increasingly global nature of money laundering and terrorist financing schemes.

Privacy Review of the PCMLTFA

The Privacy Commissioner is granted the authority to audit the personal information handling practices of all federal departments and agencies under the *Privacy Act*. In addition, as per s. 72(2) of the PCMLTFA, the Commissioner must conduct a review of the measures taken by FINTRAC to protect information it receives or collects every two years. However, since this requirement was established in 2006, the Office of the Privacy Commissioner (OPC) has carried out audits on a less frequent basis than the biennial reviews mandated by the PCMLTFA, with reports published in 2009, 2013 and 2017. When the 2-year requirement was under consideration by Parliament, Canada's then Privacy Commissioner had raised concerns about the feasibility of this requirement and asked Parliamentarians to revisit the frequency of mandatory reviews.[14]

In this context, the Department seeks views on the merits of changing the frequency of the Privacy Commissioner's mandatory review of FINTRAC from two years to four years. A longer period between privacy reviews would reflect OPC's current practice which allows for a deeper periodic review. This would not impact the OPC's ability to conduct reviews of FINTRAC activities on a more frequent basis if the OPC deemed it necessary, pursuant to existing authorities under s. 37 of the *Privacy Act*. Further, FINTRAC is subject to oversight by the National Security and Intelligence Committee of Parliamentarians, and subject to Parliamentary approval, by the National Security and Intelligence Review Agency as outlined in Bill C-59.

The Department has consulted the OPC on this measure.

The Department is seeking views on whether to expand disclosure recipients and on how to improve partnerships related to the exchange of information.

[14] https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2006/parl_061213/

Chapter 3 – Strengthening Intelligence Capacity and Enforcement

This chapter addresses the challenge that law enforcement, intelligence agencies and the private sector face in an ever-changing environment including evolving crime practices and the pace of technological advancements. In addition, the measures discussed draw from the international policy environment in which other countries are utilizing new tools and methods to detect and deter money laundering and terrorist financing. In evaluating whether or not to adopt these measures in Canada, these issues are assessed through the need to balance important protections such as *Charter* and privacy rights as well as the balance between any burden these measures might impose against the benefits they might bring to the fight against money laundering and terrorist financing. Measures to address enforcement activities will also have to be balanced against other priorities and risks in border enforcement.

Professional Money Launderers and Recklessness

One of the most widely recognized difficulties in Canada in investigating and prosecuting money laundering offences is the legal requirement to link the act of money laundering to specific knowledge of an underlying criminal offence that produced the illicit funds, for example, drug trafficking or fraud. This requirement is especially problematic given the increased use of professional money launderers who purposely distance themselves from the criminal organizations and associated predicate offences in order to insulate their business against successful prosecution.

Section 462.31 of the *Criminal Code* requires that prosecutors establish knowledge or belief that all or part of the property or proceeds was obtained or derived, either directly or indirectly, as a result of the commission of a designated offence Canada or an act or omission anywhere that, if it had occurred in Canada, would have constituted a designated offence. Establishing knowledge of the specific offence is a significant challenge that may contribute to Canada's relatively low rate of successful convictions of money laundering. Other countries, such as the United Kingdom and Australia, have other types of offence standards where the knowledge component (or *mens rea*) of the offence is different, such as suspicion or recklessness (showing no regard for the danger or consequences or acting carelessly).

Electronic Funds Transfers (EFTs)

Under the PCMLTFA, incoming and outgoing international EFTs over $10,000 are reported to FINTRAC when they are initiated by a client. However, this does not capture the transfers that pass through Canadian financial institutions where Canada is not the sending or recipient destination such as those originating through correspondent banking relationships. In addition, there are other types of transfers that relate to new and evolving payment methods - e.g. letters of credit and finance, trade, precious metals and securities - that are not currently captured.

This creates a gap in the information that FINTRAC receives and prevents FINTRAC from identifying potential money laundering or terrorist financing transactions that are occurring in and transiting through the Canadian financial system. Recognizing the existing mechanisms already in place for EFT reporting to FINTRAC, this measure looks to incorporate non-client initiated transfers into existing systems without creating excessive burden.

Bulk Cash

Despite the increasing prevalence of non-cash payment methods in Canada, cash remains an important means of payment. There are a range of historical and cultural reasons for some people in Canada to not use traditional financial services and instead rely on cash. In addition, cash is still widely used by criminals and it remains intrinsically linked to most criminal activity. In Canada's FATF Mutual Evaluation report, the use of bearer instruments (e.g., cash) to facilitate illicit transactions was identified as a key concern. Large denominations are especially an issue, as they are likely supporting the transportation and smuggling of large values in a manner that avoids drawing the suspicion of law enforcement officials. Recognizing that large denominations are used by organized crime and in money laundering, Canada stopped producing $1,000 banknotes in 2000. Removing legal tender status for large denominations could be considered as a practical next step to strengthen confidence that Canadian currency is being used for legitimate transactions domestically and internationally. This step would be consistent with recent practices of other countries.

The physical transportation of cash across an international border is one of the oldest and most basic forms of money laundering, and it is still widespread today. A FATF study has noted that "there are no fully reliable estimates for the amount of cash laundered in this way, but the figure would seem to be between hundreds of billions and a trillion U.S. dollars per year."[15] In addition, bulk cash is often used in the purchasing of real estate and other high-value goods as a way for criminals to launder their illicit funds.

In Canada, there are criminal networks across the country that are responsible for the processing of hundreds of millions of proceeds of crime in bulk cash. These transactions are often observed by law enforcement in public places as bags or boxes of cash are exchanged. Those who are providing cash in these situations have links to criminal organizations and criminal activity and do not otherwise have legitimate reasons for possessing these amounts in cash. However, the use of multiple cash transfers, the recourse to professional money movers, and the placement of cash in the financial system often make it difficult for law enforcement to establish the link between the cash and the commission of a specific criminal offence.

In thinking about issues surrounding bulk cash, consideration could be given to whether it is appropriate to place a limit on the amount of bulk cash a person could carry in Canada without a legitimate purpose, whether Canada should develop a business registry for those businesses that deal in high volumes of cash and whether there should be a limit on the

[15] http://www.fatf-gafi.org/media/fatf/documents/reports/money-laundering-through-transportation-cash.pdf

amount of cash a business in Canada could accept and/or report on. These types of mitigation measures to deal with the issue of bulk cash have all been implemented in some form by other countries such as the United States, France and the United Kingdom.

Geographic Targeting Orders

Geographic targeting orders set out specific obligations for persons and entities in certain geographic areas to face heightened scrutiny in respect of specified transactions on the basis of the higher money laundering and terrorist financing risks they face. They are generally set for a specified time period.

Geographic areas are generally targeted because they are popular destinations for luxury goods and real estate. They may have a higher than average percentage of bulk cash transactions or are the focus of heightened attention by law enforcement. Geographic targeting orders have been used extensively in the United States to target real estate and other transactions for high-value goods.

Geographic targeting orders are not currently provided for in the PCMLTFA; however, they could be useful to improve financial intelligence on money laundering and terrorist financing activities for segments that are seen to be higher risk for money laundering and terrorist financing. They could provide flexibility to facilitate a risk-based approach by allowing the Government to set out temporary obligations targeted at persons or entities in certain geographic areas. There are different ways that this tool could be implemented in Canada and it would be important to give careful consideration to oversight of such a mechanism should it be introduced into the Canadian AML/ATF Regime.

The Department is seeking views on these areas related to intelligence gathering and enforcement where vulnerabilities have been identified.

Border Enforcement

Part 2 of the PCMLTFA is administered by the Canada Border Services Agency (CBSA) and requires persons or entities to report the importation and exportation of currency or monetary instruments of $10,000 or more. Monetary instruments are stocks, bonds, treasury bills, bank drafts, promissory notes, travellers' cheques, endorsed cheques and money orders, in bearer form or in such other form that title passes on delivery.

Part 2 also enables the CBSA to perform searches where there are reasonable grounds to suspect a person or entity is carrying unreported currency or monetary instruments. Unreported amounts may be seized by the CBSA or forfeited where there are reasonable grounds to suspect that they are proceeds of crime or funds for terrorist financing.

Definition of Monetary Instrument

Canada's definition of monetary instrument, as described above, is relatively narrow and does not capture the cross-border movement of other types of value that could be used for money laundering or terrorist financing purposes. This was also noted in Canada's FATF

Mutual Evaluation. Other types of instruments could include diamonds, gold and other precious metals, prepaid payment products, and others. The risk associated with these items lies in their transportability and the relative ease of moving and potentially accessing monetary value anonymously.

Cross Border Currency Penalties

In Canada, the penalties associated with failure to declare currency and monetary instruments in excess of $10,000 ranges from $250 to $5,000. Canada's FATF Mutual Evaluation noted that these penalties structure are neither proportionate nor dissuasive. In comparison to other countries, the penalties in Canada are low. Some countries, such as Spain, impose a blanket minimum penalty over double our own; in Australia, the minimum penalty varies based on the value of currency not declared. In the United States, all currency may be seized and forfeited in instances where there is a false or no declaration by assessing a penalty equal to the amount not declared. In order to ensure that the Canadian penalties are a sufficient deterrent, revising the penalty structure is under consideration.

Trade Fraud Intelligence

Trade fraud is a growing global strategic risk and an umbrella term for techniques that manipulate legitimate trade, trade finance and customs processes either for direct illicit gain, or to disguise proceeds of crime, including terrorist financing. The latter is generally referred to as "trade-based money laundering". Trade fraud fuels global crime, terrorism, international sanctions evasion and corruption. It also deprives countries of duty and tax revenues and distorts legitimate economic competition. Trade fraud and trade-based money laundering hide within massive volumes of legitimate international commerce and cuts across the mandates and business lines of numerous government and private sector entities, making it extremely difficult to detect. Several estimates have pegged the value of trade-based illicit financial flows at as much as 7 percent of global gross domestic product.

The United States has made the investigation of trade fraud and trade based money laundering a priority and have implemented various programs, such as Trade Transparency Units that use U.S. and partner country trade data to examine suspect anomalies and identify likely targets of investigation. Great Britain has created a money laundering intelligence centre to pool the government and private sector expertise necessary to identify key money laundering risks, including trade-based money laundering.

The Department is seeking views on how to address the money laundering and terrorist financing vulnerabilities at the border.

Chapter 4 – Modernizing the Framework and its Supervision

This chapter discusses how the framework is managed and supervised. In looking at measures in this space, it is important to be mindful of the potential trade-offs that need to be taken into account when deciding on the use of legislation or regulatory mechanisms versus administrative tools that may be available such as the use of guidance, education, communication and moral suasion which can also prove effective.

Addressing the Issue of Money Services Business De-Risking

"De-risking" refers to the practice of financial institutions (or other businesses) exiting relationships with and closing the accounts of clients, either individuals or institutions, because the financial institution perceives the client to be high-risk. The issue of de-risking is a global trend based upon a complex set of factors which include, but are not limited to, a change in business focus and changes in the level risk tolerance. Given the potential impact of this trend on domestic financial inclusion and international remittance payments, de-risking has become the subject of study by groups such as the Financial Stability Board.

Under the PCMLTFA, reporting entities are expected to manage (but not necessarily eliminate) their 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 and not impact an entire industry. In addition, the customer due diligence requirements in the PCMLTFA apply a "know-your-customer" rule.

Some money services businesses (MSBs) have had challenges in maintaining accounts with financial institutions as a consequence of this de-risking trend. This reflects the perception that MSBs are inherently high-risk and the mistaken belief in some cases that financial institutions must "know your customer's customer". This in turn hampers their capacity to transmit remittances and therefore seriously impacts the business model for these MSBs. Furthermore, if they are unable to maintain accounts with legitimate financial institutions, this could drive financial transactions to informal channels which make these transactions more opaque to regulators and law enforcement when they are investigating money laundering and terrorist financing.

Strengthening Money Services Businesses (MSB) Registration

When MSBs do operate in Canada, they require access to financial services, as discussed above, and registration with FINTRAC. In order to ensure the integrity of the registry and of those who operate MSBs in Canada certain requirements are put in place.

Canada's *Assessment of Inherent Risks of Money Laundering and Terrorist Financing* recognizes that while the MSB sector is diverse, it is broadly vulnerable to money laundering and terrorist financing. In order to operate as an MSB in Canada, persons or entities must register with FINTRAC and subsequently renew their registration every two years. The PCMLTFA outlines existing requirements for MSBs to register, as well as circumstances

under which these persons or entities may be ineligible for registration (for example, certain criminal convictions related to money laundering and terrorist financing).

Despite these requirements, over the years, FINTRAC has found that the registration application and procedures could be improved to safeguard the integrity of the financial system. For example, the list of offences that would make an applicant ineligible could be expanded. Also, suspending the registration of a MSB could become possible on a discretionary basis, with appropriate legal safeguards, when the owners/operators of an MSB are subject to criminal court proceedings that, if they were to result in a conviction, would make them ineligible for registration.

Enhancing and Strengthening Identification Methods

The nature of banking and financial services is rapidly evolving. Financial institutions are harnessing the ever-changing and rapid world of digital technology solutions to enhance their ability to be more efficient and effective. This includes being on the cutting edge of secure means for conducting know-your-client procedures to meet the consumer demands of an online environment.

There is currently a reliance on physically viewing and validating identification documents to ensure they are original, valid and current. Advanced technology has the ability to perform remote validation, for example by supporting enhanced online scanning processes that enable validation, data extraction and document authentication processes to assess the legitimacy of ID documents such as passports, visas, identification cards, drivers' licenses, etc. The use of blockchain, identification using biometrics, facial recognition and other advanced methods, which can be more reliable and effective than the human eye, are all areas of intense focus and development.

The rapid rate of growth and innovation in the financial technology (fintech) sector, and concepts of "digital ID" more specifically, calls for strengthening current identification methods, exploring new identification methods, while trying to leverage new technologies to facilitate and enhance the effectiveness of customer due diligence for the purposes of the AML/ATF Regime.

Amendments to the Regulations in 2016 introduced flexibility for measures to ascertain the identity of a client, especially in the online context. This included the use of a credit file and the ability to refer to information from two independent and reliable sources to ascertain the identity of a client (e.g., a utility bill, a bank statement or a credit file). The ability to rely on information provided by federal or provincial government bodies that are authorized to ascertain the identity of people (e.g., drivers licence bureaus) has also been added. However, the Regulations need to continue to remain flexible and adaptive in an environment of rapid development and emerging technologies. Continuous progress towards more principles-based requirements could allow reporting entities to take a risk-based approach vis-à-vis new technologies. Such an approach to regulation would provide for a nimbler framework that would do a better job at leveraging technology solutions, which should ultimately enhance the effectiveness of the AML/ATF Regime.

Exemptive Relief and Administrative Forbearance

With the rapid growth of the fintech sector, several jurisdictions (e.g., the province of Ontario, United Kingdom, and Singapore) have developed regulatory pilots to allow start-ups to operate in a supervised environment without having to necessarily comply with all of the regulatory requirements that may otherwise apply. The regulatory pilot component allows fintech companies to apply for time-limited exemptive relief in order to test their products, services or applications in a live environment or to have more flexible approaches to complying with requirements as long as it would not pose a risk to the integrity of Canada's AML/ATF Regime.

Administrative forbearance is a broader authority that allows a regulator to exempt entire classes of businesses, or sectors, or all regulated entities, from certain obligations on either a temporary or permanent basis. Both exemptive relief and administrative forbearance would make the AML/ATF framework more flexible, risked-based and supportive of innovation, and as such contribute to a greater use of RegTech approaches; however, attention must be paid to the considerations surrounding the approval of such regulatory pilots.

Consultation Process for the Development of Guidance

After amendments to the PCMLTFA or its Regulations are developed, FINTRAC plays a key role in providing guidance to reporting entities on their obligations and requirements in implementing these changes. In addition, OSFI, through their prudential mandate with federally-regulated financial institutions, plays a significant role in supervising and providing guidance on an ongoing basis to these institutions. FINTRAC drafts guidance based on the PCMLTFA while OSFI drafts guidance based on supervisory expectations; discussions with industry on such guidance occur at various stages. This guidance is significantly strengthened when FINTRAC and OSFI are able to consult and discuss the draft guidance with the industry. Consultations already happen on an informal basis through meetings and discussions between the Government and private sector, including through ad hoc and standing advisory mechanisms. Other regulators such as the Financial Consumer Agency of Canada use a more formal stakeholder engagement and consultation framework to guide their activities.

Whistleblowing

Whistleblowing programs have proven to be a valuable tool for organizations to receive reports of wrongdoing and misconduct in different contexts. Various features of a whistleblowing framework already exist in the current AML/ATF framework as FINTRAC has the authority to receive information anonymously from the public with respect to suspected money laundering, terrorist financing offences as well as contraventions of the PCMLTFA. In addition, prescribed protections for personal and private information held by FINTRAC protect the anonymity of person submitting the information. There is a view that existing features are robust and could be communicated more clearly to the public. Yet some parties believe that the protections could go further and that other features of a typical whistleblowing framework, such as a mechanism to inquire about the status of their submission or dedicated funding, are not present.

Whistleblowing programs are now part of the organizational landscape across a range of business sectors in Canada. Examples of government departments and agencies having established such programs include the Canada Revenue Agency, the Competition Bureau, and the National Energy Board.

The Department is seeking views on how to modernize the framework to address issues related to MSBs, ID methods, and oversight.

Administrative Monetary Penalties (AMP)

The purpose of the AMP regime in the PCMLTFA is to encourage individuals and entities to comply with their obligations under the Act and Regulations. The AMP Regulations set out the violations, their level of severity, and prescribed maximum amount for each of these violations. These violations include failure to:

- identify clients and keep prescribed records;
- report suspicious transactions, large cash transactions, electronic funds transfers, casino disbursement and terrorist property;
- implement an appropriate compliance regime, including the appointment of a designated compliance officer and the establishment of appropriate policies, procedures and training programs for employees; provide accurate, timely and complete reports and information to FINTRAC; and
- co-operate with FINTRAC compliance officers.

Maximum penalties are established in Regulations and assessed by FINTRAC. Where appropriate, a notice of violation is issued to entities that are found to be non-compliant and corresponding penalty amounts are measured and proportionate to particular instances of non-compliance. Among other things, the notice of violation identifies the nature of the violation and the amount of the penalty as well as the right to make representations to the Director.

A variety of outcomes are possible including paying the initial AMP, entering into a compliance agreement with FINTRAC, requesting a review by the Director of FINTRAC, and making an appeal to Federal Court (only in the case of serious or very serious violations and only after representations have been made to the Director). Once all proceedings have been exhausted, FINTRAC may make public the name of the person or entity and the violations and penalty amount imposed).

Public Naming

Publicly naming an AMP recipient can act as a significant deterrent against violations of money laundering and terrorist financing rules. In many cases the reputational risk of an entity being named publically is a greater deterrent than the amount of the AMP itself.

The PCMLTFA sets out FINTRAC's discretionary power to make public certain information related to an AMP when proceedings with respect to a violation have ended,

including when all judicial appeals have been exhausted. Because FINTRAC is only able to make public certain information relating to an AMP once all proceedings have ended, which in many cases could be a considerable amount of time since the original violation was identified, the deterrence effect of naming can be greatly diluted and potentially creates an incentive to engage in protracted litigation. In exercising a discretionary power to publicly name a person or entity, consideration should be given to criteria or situations when it would be appropriate not to name, for example, when naming may affect the stability of Canada's financial system.

Confidentiality in Court Proceedings

As part of an AMP appeal process, a person or entity may apply to the court for a confidentiality order. These orders can vary from protecting the information filed in court to keeping the identity of the violator confidential. This represents a significant departure from usual litigation processes in other spheres of federal regulatory compliance where the identity of regulated persons and entities is made public when the entities challenge a penalty that was imposed.

The original policy intent to allow for confidentiality orders under the PCMLTFA was to serve as a precaution to avoid the disclosure of financial intelligence information and not to protect any and all information related to a reporting entity.

Penalty Calculation for AMPs

In determining the penalty amount, the AMP program takes into account the harm caused by the violation such as the degree to which the violation obstructs Canada's ability to detect and deter money laundering and terrorist financing; the compliance history of the reporting entity and the non-punitive nature of AMPs.

Recent court decisions have upheld the violations cited by FINTRAC but found that the formula used to calculate AMP was vague and lacked transparency. Including a formula in the Regulations for how AMPs should be calculated would increase transparency and provide more clarity.

The Department is seeking views on how to address issues related to Administrative Monetary Penalties.

Chapter 5 – Administrative Definitions and Provisions

This chapter discusses technical issues that would improve the administration and operation of the PCMLTFA and its Regulations as well as clarify requirements that would assist reporting entities in meeting their obligations.

Electronic Reporting of Cross-Border Movements of Currency and Monetary Instruments

The Canada Border Services Agency (CBSA) collects reports on the cross-border movements of currency and monetary instruments under the authority of the PCMLTFA. Currently, these reports are completed manually by travellers and entities in paper form and submitted to the CBSA. The CBSA then transcribes that information into an electronic FINTRAC database, faxes or sends the paper version of the reports. Copies of these reports are currently not kept nor analyzed by the CBSA. This manual process is problematic given that the information collected may be of low quality (sometimes the information is illegible) or incomplete.

With the Regime moving to a more automated collection of information system, there is an opportunity to move to a more effective means of collecting information from travellers once it has been verified by border services officers. The electronic collection and transmittal of reports would increase the accuracy of the information, timeliness of reports submitted, and overall intelligence value of this information for FINTRAC.

Further, permitting the CBSA to retain these reports would provide a new source of information when analyzing and managing the flow of people across borders, and would allow the CBSA to enhance their indicators for money laundering and terrorist financing and increase border safety and security. The CBSA's non-retention of these CBCRs was also a gap noted in Canada's FATF evaluation. Consideration should be given to implementation issues such as the cost, time and amount of resources that would need to be dedicated to electronic reporting of these reports.

Clarify the Electronic Funds Transfer (EFT) or the "Travel Rule"

The "travel rule", in section 9.5 of the PCMLTFA, states that every reporting entity shall include with the EFT the name, address, and account number or other reference number of the client who requested it and that they take reasonable measures to ensure that any transfer that the reporting entity receives includes this information.

The policy intent of this requirement is to pass the originating client's information along with the EFT, so that competent authorities and financial institutions can follow the money and be aware of risks and suspicions associated with EFTs. Contrary to this intent, FINTRAC has found that financial intermediaries are not passing along the originating client's information and instead treating the originating financial institution or another financial institution in the transaction process as the client who requested the EFT for the purposes of the travel rule.

Mitigation of Money Laundering and Terrorist Financing Commensurate with the Risks

Section 9.6 of the PCMLTFA requires reporting entities to self-assess the money laundering and terrorist financing risks of their business activities and to take special measures to mitigate that risk only if that risk is considered high. There is no explicit obligation to mitigate any risks that are assessed as being lower than the high benchmark according to their risk level.

Evaluation of Correspondent Relationships

Correspondent banking relationships are established between banks to facilitate transactions between banks made on their own behalf; enable transactions on behalf of their clients; and make services available directly to clients of other banks. Correspondent banking is an important component of facilitating international financial flows. When establishing the relationship, the PCMLTFA only requires that financial institutions evaluate the relationship at the outset.

At present, this requirement does not align with international standards which expect that financial institutions should evaluate the relationships on an ongoing basis and that correspondent institutions should identify and take reasonable measures to verify the identity of beneficial owners when entering into a business relationship with a respondent institution. The evaluation ensures that respondent institutions are subject to appropriate domestic supervision, there has been no change in the standing of the financial institution (e.g., fines or sanctions) and AML/ATF risk profile has not changed. Any changes would not require a termination in the relationship, only an adjustment in the risk based approach employed.

Defining Reporting Entity

Businesses and sectors who are subject to the PCMLTFA are defined in section 5 of the Act. Subsequently, they are referred to as "persons or entities as defined under section 5" or "person or entity" throughout the legislation and Regulations. In some provisions of the PCMLTFA, the language can be complicated when referring to "person or entity" multiple times, because provisions can refer to "persons or entities" as reporting entities as well as the clients of reporting entities. Defining the term reporting entity would provide clarity within the PCMLTFA and increase readability.

Creation of a Uniform Reporting Schedule

Contained in the PCMLTFA Regulations are several schedules that outline the specific information that reporting entities are required to report. This information is often repeated across the schedules as the information required is the same.

It can be time consuming to keep these schedules up to date and can be burdensome for reporting entities to create new forms and processes to comply with the various schedules. Streamlining the schedules and creating one uniform reporting schedule could be useful to reduce regulatory burden and unnecessary duplication.

Removal of the Alternative to Large Cash Transaction Reporting (Section 50)

Under the PCMLTFA, there is an alternative process, referred to as the Alternate Large Cash Transaction Record, to allow reporting entities to not send large cash transaction reports in specific circumstances; for example, when a client is a corporation with business activity in specific sectors (e.g., retail businesses, transportation companies, etc.). This was intended to ease the reporting burden on smaller reporting entities.

However, it is understood that the majority of reporting entities have never truly leveraged the Alternate Large Cash Transaction Record and continue to send reports to FINTRAC for all transactions, even if they would be eligible for the Alternative Record. The repeal of this exception would streamline the large cash transaction reporting process for reporting entities and provide valuable financial intelligence information to FINTRAC's analysis.

The Department is seeking views on these issues related to administrative definitions and provisions.

List of Abbreviations

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

ATMs - Automated Teller Machines

CBCA - Canada Business Corporations Act

CBSA - Canada Border Services Agency

CSIS - Canadian Security Intelligence Service

CRA - Canada Revenue Agency

DNFBPs - designated non-financial businesses and professions

FATF - Financial Action Task Force

FINTRAC - Financial Transactions and Reports Analysis Centre of Canada

GAC - Global Affairs Canada

HIO - head of an international organization

MSB - money service business

OSFI - Office of the Superintendent of Financial Institutions

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

PEP - politically exposed person

PPSC - Public Prosecution Service of Canada

PS – Public Safety Canada

PSPC - Public Services and Procurement Canada

RCMP - Royal Canadian Mounted Police

Links to Important Documents

The Financial Action Task Force Mutual Evaluation Report of Canada – September 2016 (http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-Canada-2016.pdf)

The Financial Action Task Force - International Standards on Combatting Money Laundering and the Financing of Terrorism and Proliferation (http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF Recommendations 2012.pdf)

The *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and Associated Regulations (http://laws-lois.justice.gc.ca/eng/acts/P-24.501/)

The Financial Transactions and Reports Analysis Centre of Canada - 2016 Annual Report (http://www.fintrac.gc.ca/publications/ar/2016/1-eng.asp)

Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada (https://www.fin.gc.ca/pub/mltf-rpcfat/mltf-rpcfat-eng.pdf)

Follow the Money: Is Canada Making Progress in Combatting Money Laundering and Terrorist Financing? Not Really (http://parl.gc.ca/Content/SEN/Committee/411/BANC/rep/rep10mar13-e.pdf)