Overview Report: Documents Created by Canada

I. Scope of Overview Report

1. This overview report attaches documents created by Canada:

II. Appendices

a. Appendix A:

Canada, Parliament, Senate, Standing Senate Committee on Banking, Trade and Commerce, *Follow the Money: Is Canada Making Progress in Combatting Money Laundering and Terrorist Financing? Not Really, Report of the Standing Senate Committee on Banking, Trade and Commerce*, 41st Parl, 1st Sess (March 2013) (Chair: Irving R. Gerstein).

b. Appendix B:

Canada, Department of Finance, *Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada 2015* (Ottawa: Department of Finance, 2015).

c. Appendix C:

Canada, Parliament, House of Commons, Standing Committee on Finance, *Confronting Money Laundering and Terrorist Financing: Moving Canada Forward, Report of the Standing Committee on Finance* 42nd Parl, 1st Sess (November 2018) (Chair: Wayne Easter).

d. Appendix D:

Canada, Parliament, House of Commons, Standing Committee on Finance, *Government Response to the Twenty-Fourth Report of the Standing Committee on Finance*.

e. Appendix E:

Canada, Criminal Intelligence Service Canada, *Public Report on Organized Crime 2019* (Ottawa: Criminal Intelligence Service Canada, 2019).

f. Appendix F:

Canada, Criminal Intelligence Service Canada, *2018-19 National Criminal Intelligence Estimate on the Canadian Criminal Marketplace: Illegal Drugs* (Ottawa: Criminal Intelligence Service Canada).

Appendix A:

Canada, Parliament, Senate, Standing Senate Committee on Banking, Trade and Commerce, *Follow the Money: Is Canada Making Progress in Combatting Money Laundering and Terrorist Financing? Not Really, Report of the Standing Senate Committee on Banking, Trade and Commerce*, 41st Parl, 1st Sess (March 2013) (Chair: Irving R. Gerstein).

SENATE SÉNAT
CANADA

FOLLOW THE MONEY: IS CANADA MAKING PROGRESS IN COMBATTING MONEY LAUNDERING AND TERRORIST FINANCING? NOT REALLY

Report of the
Standing Senate Committee on Banking, Trade and Commerce

The Honourable Irving R. Gerstein,
C.M., O. Ont, Chair
The Honourable Céline Hervieux-Payette,
P.C., Deputy Chair

March 2013

Ce rapport est aussi disponible en français

****

Available on the Parliamentary Internet:
www.parl.gc.ca
(Committee Business – Senate – Reports)
41st Parliament – 1st Session

TABLE OF CONTENTS

MEMBERS i

FOREWORD ii

ORDER OF REFERENCE iii

EXECUTIVE SUMMARY iv

SUMMARY OF RECOMMENDATIONS: vi

- **The Desired Structure and Performance** vi
- **The Appropriate Balance Between the Sharing of Information and the Protection of Personal Information** vii
- **The Optimal Scope and Focus** viii

CHAPTER ONE – INTRODUCTION 1

CHAPTER TWO – THE HISTORY AND IMPACT OF ANTI-MONEY LAUNDERING AND ANTI-TERRORIST FINANCING LEGISLATION IN CANADA 3

CHAPTER THREE – THE DESIRED STRUCTURE AND PERFORMANCE 8

CHAPTER FOUR – THE APPROPRIATE BALANCE BETWEEN THE SHARING OF INFORMATION AND THE PROTECTION OF PERSONAL INFORMATION 13

CHAPTER FIVE – THE OPTIMAL SCOPE AND FOCUS 18

CHAPTER SIX – CONCLUSION 22

APPENDIX A – CANADA'S ANTI-MONEY LAUNDERING AND ANTI-TERRORIST FINANCING REGIME A-1

APPENDIX B – SUMMARY OF THE EVIDENCE A-2

- **Strengthening Customer Identification and Due Diligence** A-2
- **Closing the Gaps in Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime** A-5
- **Improving Compliance, Monitoring and Enforcement** A-9
- **Strengthening the Sharing of Information in Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime** A-12
- **Countermeasures** A-14
- **Other Proposals** A-15
- **Technical Amendments** A-16

Proposals in the Department of Finance's November 2011 Consultation Paper in Relation to the *Proceeds of Crime (money laundering) and terrorist financing regulations* **A-16**

Other Witness Views and Proposals **A-20**

APPENDIX C – CAPRA INTERNATIONAL INC. RECOMMENDATIONS ... **A-35**

APPENDIX D – WITNESSES **A-36**

APPENDIX E – OTHER BRIEFS SUBMITTED TO THE COMMITTEE **A-42**

MEMBERS

The Honourable Irving R. Gerstein, C.M., O.Ont, Chair,
The Honourable Céline Hervieux-Payette, P.C., Deputy Chair

and

The Honourable Douglas Black, Q.C.
The Honourable Stephen Greene
The Honourable Mac Harb
The Honourable Ghislain Maltais
The Honourable Paul J. Massicotte
The Honourable Wilfred P. Moore, Q.C.
The Honourable Nancy Ruth, C.M.
The Honourable Donald H. Oliver, Q.C.
The Honourable Pierrette Ringuette
The Honourable David Tkachuk

Ex-officio members of the Committee:

The Honourable Senators Marjory LeBreton, P.C., (or Claude Carignan) and James S. Cowan (or Claudette Tardif).

Other Senators who have participated from time to time in the study:

The Honourable Senators Salma Ataullahjan, Diane Bellemare, Bert Brown, JoAnne L. Buth, Larry W. Campbell, Gerald Comeau, Joseph A. Day, Consiglio Di Nino, Nicole Eaton, Leo Housakos, Michael L. MacDonald, Michael A. Meighen, Q.C., Percy Mockler, Dennis Glen Patterson, Nancy Greene Raine, Michel Rivard, Gerry St. Germain, P.C., Larry Smith, Carolyn Stewart Olsen and Terry Stratton.

Parliamentary Information and Research Service, Library of Parliament:
John Bulmer, Brett Stuckey and Adriane Yong, Analysts.

Clerks of the Committee:

Barbara Reynolds
Adam Thompson

Senate Committees Directorate:

Brigitte Martineau, Administrative Assistant
Lori Meldrum, Administrative Assistant

FOREWORD

On behalf of the Standing Senate Committee on Banking, Trade and Commerce it is our pleasure to present the Committee's report on the five year Parliamentary review of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*. After more than a year of study, hearing from more than forty witnesses from various government departments, agencies, international partners, and stakeholders of Canada's anti-money laundering and anti-terrorism regime (the Regime), the Committee has put forward eighteen recommendations to the government on how the Regime may be improved.

Canadians have come to expect a strong analysis of the issues along with well researched and reasonable suggestions presented in a non-partisan manner from Senate Committees. The Banking, Trade and Commerce Committee has strived to do its best to maintain that high standard of excellence during this legislative review.

Committee members express their thanks for the support and hard work provided by the Committee Clerk and staff from the Senate Committees Directorate, the many witnesses who came before the Committee, as well as the staff of the Library of Parliament whose efforts brought about this report.

Respectfully,

Senator Irving R. Gerstein, C.M., O.Ont,
Chair

Senator Céline Hervieux-Payette, P.C.,
Deputy Chair

Standing Senate Committee on Banking, Trade and Commerce

ORDER OF REFERENCE

Extract from the *Journals of the Senate* of January 31, 2012:

With leave of the Senate,

The Honourable Senator Carignan moved, seconded by the Honourable Senator Rivard:

That the Standing Senate Committee on Banking, Trade and Commerce be authorized to undertake a review of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (S.C. 2000, c. 17), pursuant to section 72 of the said Act; and

That the committee submit its final report no later than May 31, 2012.

The question being put on the motion, it was adopted.

Extract from the *Journals of the Senate* of Tuesday, December 11, 2012:

The Honourable Senator Gerstein moved, seconded by the Honourable Senator Wallin:

That, notwithstanding the order of the Senate adopted on Tuesday, January 31, 2012, Tuesday, May 15, 2012, Tuesday, June 19, 2012, and Tuesday, June 26, 2012, the date for the final report of the Standing Senate Committee on Banking, Trade and Commerce in relation to its review of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (S.C. 2000, c.17) be extended from December 31, 2012 to March 31, 2013.

The question being put on the motion, it was adopted.

Gary W. O'Brien

Clerk of the Senate

EXECUTIVE SUMMARY

According to the United Nations, money laundering is "any act or attempted act to disguise the source of money or assets derived from criminal activity." The annual value of global money laundering is estimated to be between US$800 billion and US$2 trillion, while money laundering in Canada in 2011 was estimated to be between $5 billion and $15 billion.

The Standing Senate Committee on Banking, Trade and Commerce (the Committee) began a five-year statutory review of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* in February 2012. In addition to written briefs from those unable to appear in person, the Committee heard from more than 40 witnesses, including representatives from federal, provincial and international departments and agencies, as well as the private sector.

The report summarizes the oral and written evidence received by the Committee during the review, and contains 18 recommendations designed to improve the effectiveness of Canada's anti-money laundering and anti-terrorist financing regime (the Regime).

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.

- desired structure and performance;
- the appropriate balance between sharing of information and the protection of personal information; and
- optimal scope and focus.

Desired structure and performance

The Committee believes that Canada's Regime will only be effective, and its performance optimized, if it has the correct structure. The right oversight is required, sources of funds must be identified, specialists must be employed and ongoing review is necessary to ensure that the "results" of everyone's efforts are maximized in light of the time, monetary and other costs committed by governmental departments and agencies, and by reporting entities. To that end, the Committee makes five recommendations regarding supervision, performance review, funding and expertise.

Appropriate balance between the sharing of information and the protection of personal information

The Committee feels that the effectiveness of Canada's Regime is enhanced – that is, the "results" are greater – when appropriate and timely information is shared among relevant parties, including the Financial Transactions and Reports Analysis Centre of Canada, law enforcement agencies, reporting entities, the employees of reporting entities and other individuals. The Committee's eight recommendations in this area are designed to improve case disclosures and the sharing of information, bearing in mind the need to protect personal information, reduce the compliance burden on reporting entities, and

ensure the safety of those who assist in investigations and prosecutions of money laundering and terrorist financing.

Optimal scope and focus

The Committee's opinion is that changes are needed in response to global developments in money laundering and terrorist financing, advancements in technology and the need for public awareness about the Regime. From that perspective, the five recommendations made by the Committee focus on risk-based reporting and an adherence to global standards, and to create public awareness.

The Committee is of the view that implementation of the 18 recommendations would lead to a more effective anti-money laundering and anti-terrorist financing regime in Canada.

Please note that this summary of the recommendations should be read in the context of the reasoning presented in the body of the report. For an indication of the appropriate section of the report, please see the page number at the end of the recommendation.

SUMMARY OF RECOMMENDATIONS:

The Desired Structure and Performance

1. The federal government establish a supervisory body, led by the Department of Finance, with a dual mandate:

   - to develop and share strategies and priorities for combatting money laundering and terrorist financing in Canada; and
   - to ensure that Canada implements any recommendations by the Financial Action Task Force on Money Laundering that are appropriate to Canadian circumstances.

   This supervisory body should be comprised of representatives of federal interdepartmental working groups and other relevant bodies involved in combatting money laundering and terrorist financing. (p. 9)

2. The federal government require the supervisory body recommended earlier to report to Parliament annually, through the Minister of Finance, the following aspects of Canada's anti-money laundering and anti-terrorist financing regime:

   - the number of investigations, prosecutions and convictions;
   - the amount seized in relation to investigations, prosecutions and convictions;
   - the extent to which case disclosures by the Financial Transactions and Reports Analysis Centre of Canada were used in these investigations, prosecutions and convictions; and
   - total expenditures by each federal department and agency in combatting money laundering and terrorist financing. (p. 10-11)

3. The federal government ensure that, every five years, an independent performance review of Canada's anti-money laundering and anti-terrorist financing regime, and its objectives, occurs. The review could be similar to the 10-year external review of the regime conducted in 2010, and could be undertaken by the Office of the Auditor General of Canada. The first independent performance review should occur no later than 2014. (p. 11)

4. The federal government consider the feasibility of establishing a fund, to be managed by the supervisory body recommended earlier, into which forfeited proceeds of money laundering and terrorist financing could be placed. These amounts could supplement resources allocated to investigating and prosecuting money laundering and terrorist financing activities. The government should ensure that implementation of this recommendation does not preclude victims from

collecting damages awarded to them by a court of law in a suit brought under the *Justice for Victims of Terrorism Act*. (p. 12)

5. The federal government ensure that the Financial Transactions and Reports Analysis Centre of Canada and the Royal Canadian Mounted Police employ specialists in financial crimes, and provide them with ongoing training to ensure that their skills evolve as technological advancements occur. (p. 12)

The Appropriate Balance Between the Sharing of Information and the Protection of Personal Information

6. The federal government require the Royal Canadian Mounted Police, the Canadian Security and Intelligence Service, the Canada Border Services Agency and the Canada Revenue Agency to provide quarterly feedback to the Financial Transactions and Reports Analysis Centre of Canada regarding the manner in which they use case disclosures and how those disclosures could be improved. (p.14)

7. The federal government permit the Financial Transactions and Reports Analysis Centre of Canada to provide case disclosures in relation to offences under the *Criminal Code* or other Canadian legislation. (p. 14)

8. The federal government develop a mechanism by which the Royal Canadian Mounted Police, the Canadian Security and Intelligence Service, the Canada Border Services Agency and the Canada Revenue Agency could directly access the Financial Transactions and Reports Analysis Centre of Canada's database. The Privacy Commissioner of Canada should be involved in developing guidelines for access. (p. 14)

9. The federal government and the Financial Transactions and Reports Analysis Centre of Canada, in consultation with entities required to report under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and its regulations, annually review ways in which:

    - the compliance burden on reporting entities could be minimized; and
    - the utility of reports submitted by reporting entities could be optimized. (p. 15)

10. The Financial Transactions and Reports Analysis Centre of Canada provide entities required to report under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and its regulations with:

    - on a quarterly basis and specific to each entity, feedback on the usefulness of its reports;
    - on a quarterly basis and specific to each sector, information about trends in money laundering and terrorist financing activities; and
    - tools, resources and other ongoing support designed to enhance the training of employees of reporting entities in relation to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and its obligations. (pp. 15-16)

11. The Financial Transactions and Report Analysis Centre of Canada review its guidelines in relation to the period in which reports must be submitted to it by entities required to report under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and its regulations. The goal of the review should be to ensure that, to the greatest extent possible, reports are submitted in "real time". (p. 16)

12. The federal government, notwithstanding the recently proposed changes to Canada's *Witness Protection Program Act*, ensure that the safety of witnesses and other persons who assist in the investigation and prosecution of money laundering and/or terrorist financing activities is protected. (p. 16)

13. The federal government establish a mechanism by which employees of entities required to report under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and its regulations, and other individuals, could anonymously notify the Financial Transactions and Reports Analysis Centre of Canada about:

    - failures to comply with the requirements of the Act; and
    - individuals or entities possibly complicit in money laundering and/or terrorist financing. (p. 17)

The Optimal Scope and Focus

14. The federal government enhance Canada's existing anti-money laundering and anti-terrorist financing regime by placing additional emphasis on:

    - the strategic collection of information; and
    - risk-based analysis and reporting. (p. 19)

15. The federal government review, on an ongoing basis, the entities required to report under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and its regulations to ensure the inclusion of sectors where cash payments exceeding the current $10,000 threshold are made. (p. 19)

16. The federal government eliminate the current $10,000 reporting threshold in relation to international electronic funds transfers. (p. 20)

17. The federal government review annually, and update as required, the definition of "monetary instruments" in the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* in order to ensure that it reflects new payment methods and technological changes. (p. 20)

18. The federal government, in consultation with the proposed Financial Literacy Leader, develop a public awareness program about Canada's anti-money laundering and anti-terrorist financing regime, and about actions that individuals and businesses can take to combat money laundering and terrorist financing. (p. 21)

CHAPTER ONE – INTRODUCTION

> *According to the United Nations, money laundering is "any act or attempted act to disguise the source of money or assets derived from criminal activity." Essentially, it is the process whereby "dirty money" — produced through criminal activity — is transformed into "clean money," the criminal origin of which is difficult to trace. Money laundering is linked to various criminal activities, including terrorism, drug trafficking, corruption and organized crime.*
>
> *The United Nations estimates that the amount of money laundered globally each year is between 2% and 5% of the world's gross domestic product, or between US$800 billion and US$2 trillion. The Royal Canadian Mounted Police estimates that, in 2011, between $5 billion and $15 billion was laundered in Canada.*

On January 31, 2012, pursuant to section 72 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (the Act), the Standing Senate Committee on Banking, Trade and Commerce (the Committee) received authorization from the Senate to undertake a review of Canada's anti-money laundering and anti-terrorist financing regime (the Regime). This is the second five-year review. In 2006, the Committee released a report entitled *Stemming the Flow of Illicit Money: A Priority for Canada*, which contained 16 recommendations to the federal government, several of which were subsequently implemented through amendments to the Act.

Section 72 of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act *requires a parliamentary review of the administration and operation of the Act five years after the coming into force of that section, and every five years thereafter.*

The Committee's current review follows two consultation papers initiated by the Department of Finance. In November 2011, the Department released *Proposed Amendments to the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations on Ascertaining Identity*, of which proposed amendments to regulations were released in October 2012. In December 2011, the second report released was entitled *Strengthening Canada's Anti‑Money Laundering and Anti‑Terrorist Financing Regime*.

Furthermore, in 2010 Capra International Inc. conducted a 10-year external evaluation of the Regime at the request of the Department of Finance. It made recommendations regarding the funding allocations for the government agencies that participate in the Regime, and the need to conduct a public opinion survey to determine the level of public awareness of money laundering and terrorist financing, as well as of the Regime. It also recommended the creation of an interdepartmental working group to improve compliance with international commitments and to examine issues such as the sharing of information, concerns raised by reporting entities, statistics on the Regime's performance, and the roles and responsibilities of federal departments and agencies that participate in the Regime.

The Committee's current review represents the second five-year parliamentary review of the Act.

In the course of the study, the Committee received testimony from federal departments and agencies, the private sector and international entities about the various elements of the Regime, which is described in Appendix A. Appendix B notes the proposals contained in the Department of Finance's consultation papers, and summarizes the comments made by witnesses on the Department's proposals and on a number of other issues. Appendix C lists the recommendations contained in the report resulting from Capra International Inc.'s 10-year evaluation of the Regime. Appendix D is a list of witnesses and Appendix E is a list of other briefs submitted to the committee.

When reviewing legislation, the purpose and context in which it was initially enacted and subsequently amended should be considered in determining whether it is having the intended effect.

When reviewing legislation, the purpose and context in which it was initially enacted and subsequently amended should be considered in determining whether it is having the intended effect. The initial reasons for proceeds of crime legislation in Canada, some of the legislative changes over time, and the continued need for such legislation are discussed in Chapter Two.

Within the context that "value for money" should be an overarching goal of the Regime, the Committee's focus is threefold:

- *the desired structure and performance;*
- *the appropriate balance between the sharing of information and the protection of personal information; and*
- *the optimal scope and focus.*

Rather than commenting on each of the proposals in the Department of Finance's consultation papers, the Committee believes that – within the context that "value for money" should be an overarching goal – greater value can be added by making recommendations about three broad foundational issues:

- the desired structure and performance;
- the appropriate balance between the sharing of information and the protection of personal information; and
- the optimal scope and focus.

These three issues are discussed in Chapters Three through Five.

The report's conclusions are found in Chapter Six.

CHAPTER TWO – THE HISTORY AND IMPACT OF ANTI-MONEY LAUNDERING AND ANTI-TERRORIST FINANCING LEGISLATION IN CANADA

A. The History

Criminals launder money with the goal of making the funds gained from their illegal activities appear legitimate. Legislation, regulation and enforcement that make it more difficult to keep and use the profits of such activities should reduce the extent to which financial crimes occur. Mechanisms and entities focused on detecting, deterring, investigating and prosecuting money laundering and terrorist financing are key aspects of a nation's anti-money laundering and anti-terrorist financing strategy.

Criminals launder money with the goal of making the funds gained from their illegal activities appear legitimate. Legislation, regulation and enforcement that make it more difficult to keep and use the profits of such activities should reduce the extent to which financial crimes occur.

Approximately 25 years ago, a variety of international efforts were directed to combatting money laundering. These efforts included the 1988 *United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances*, as well as the establishment of the Financial Action Task Force on Money Laundering (FATF) following the July 1989 meeting of the Group of Seven nations. Canada signed the *United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances* in December 1988, and has been a member of the FATF since its establishment.

Money laundering became a criminal offence under Canada's *Criminal Code* in 1989, and the Office of the Superintendent of Financial Institutions began to issue guidelines and best practices in respect of combatting money laundering in 1990. One year later, the Royal Canadian Mounted Police (RCMP) established Integrated Proceeds of Crime units and the federal government introduced anti-money laundering legislation. Incremental changes have been made to that legislation in response to increases in organized crime, the emergence of terrorism on a global scale, comments by the FATF on Canada's anti-money laundering and anti-terrorist financing regime (the Regime), and changes in international standards in combatting money laundering.

Mechanisms and entities focused on detecting, deterring, investigating and prosecuting money laundering and terrorist financing are key aspects of a nation's anti-money laundering and anti-terrorist financing strategy.

Prior to 2000, Canada's Regime applied only to transactions conducted by financial institutions. Legislation enacted in 1991 required them to keep records of cash transactions of $10,000 or more, to undertake client identification procedures, and to report suspicious transactions directly to law enforcement agencies on a voluntary basis.

The Proceeds of Crime (money laundering) Act *was repealed and replaced in April 2000 as part of the National Initiative to Combat Money Laundering.*

In response to recommendations by the FATF about the increasingly global nature of money laundering and organized crime, and the limitations of Canada's Regime, the *Proceeds of Crime (money laundering) Act* was repealed and replaced in April 2000 as part of the National Initiative to Combat Money Laundering. The scope of the new, yet similarly named legislation, was expanded with the result that other sectors that conduct financial transactions – such as accounting, gaming and the legal profession – became subject to the obligations of the Regime. Due to an ongoing court challenge examining whether the application of the Act to the legal profession would contravene solicitor-client privilege, the provisions of the Act that apply to this profession are currently inoperative. Reporting of suspicious transactions and large cash transactions was also required. Moreover, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) – Canada's financial intelligence unit – was created to gather and analyze reports from reporting entities, and to disseminate relevant information to law enforcement and other government agencies.

Following the terrorist attacks in the United States in September 2001, the Proceeds of Crime (Money Laundering) Act *was amended as part of Canada's efforts to combat terrorism.*

Following the terrorist attacks in the United States in September 2001, the *Proceeds of Crime (Money Laundering) Act* was amended as part of Canada's efforts to combat terrorism. The renamed *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* is designed to assist law enforcement and other government agencies in detecting and deterring terrorist financing by prohibiting reporting entities from dealing with property linked to known terrorists and terrorist groups, and by requiring reporting entities to report any such properties to FINTRAC. At that time, it was emphasized that any anti-terrorist financing measures had to be balanced with Canadians' right to privacy and other civil liberties.

Amendments to the Proceeds of Crime (Money Laundering) and Terrorist Financing Act *introduced in October 2006 reflected concerns raised during the Committee's first five-year parliamentary review of the legislation.*

Amendments to the Act introduced in October 2006 reflected concerns raised during the Committee's first five-year parliamentary review of the legislation. Some of the changes included the addition of money services businesses as well as dealers in precious metals and stones as reporting entities, and the introduction of a biennial review – by the Office of the Privacy Commissioner of Canada – of the protective measures taken by FINTRAC regarding the information it collects and retains.

The most recent amendments to the Act were announced in the 2010 federal budget. Part 1.1 of the Act allows the federal government to impose financial countermeasures against foreign jurisdictions that do not have an effective regime. Although not yet in force, these measures are consistent with the Committee's conclusions in the 2006 review that Canada must support efforts that encourage the adoption of

anti-money laundering and anti-terrorist financing standards by as many countries as possible.

B. The Impact

Recognizing that Canada's anti-money laundering and anti-terrorist financing legislation has had incremental changes over the past 11 years, the Committee believes that it is appropriate to examine the extent to which Canada's Regime is effective in detecting and deterring the laundering of money and the financing of terrorist activities, and contributes to the successful investigation and prosecution of those who are involved in these criminal activities. The Committee is interested in the responses to several questions:

- Have the scope and magnitude of money laundering and terrorist financing in Canada diminished over time?
- Are the time, money and other resources dedicated to addressing these activities having sufficient "results?" and
- What changes are needed to bring about better "results?"

Responses to several questions are needed:

- *Have the scope and magnitude of money laundering and terrorist financing in Canada diminished over time?*
- *Are the time, money and other resources dedicated to addressing these activities having sufficient "results"? and*
- *What changes are needed to bring about better "results"?*

Throughout the hearings, the Committee questioned witnesses about the scope and magnitude of money laundering and terrorist financing in Canada. While the Committee learned that FINTRAC has a solid reputation internationally, witnesses shared only limited and imprecise information about the extent to which the Regime meets its objective of detecting and deterring money laundering and terrorist financing. The Committee believes that there continues to be a clear need for legislation to combat money laundering and terrorist financing in Canada.

The Committee feels that there is a lack of clear and compelling evidence that Canada's Regime is leading to the detection and deterrence of money laundering and terrorist financing, as well as contributing to law enforcement investigations and a significant rate of successful prosecutions. It is possible that some witnesses were unable to share confidential information in a public meeting. It is also possible that information about the success or failure of the Regime is not being collected. In any event, the Committee feels that the current Regime is not working as effectively as it should, given the time, money and other resources that are being committed by reporting entities, a variety of federal departments and agencies, other partners and taxpayers others.

The Committee feels that the current Regime is not working as effectively as it should, given the time, money and other resources that are being committed by reporting entities, a variety of federal departments and agencies, other partners and taxpayers.

Given that multinational financial institutions have recently been implicated in money laundering and terrorist financing, the Committee is concerned about non-compliance with the Act by reporting entities. While the majority of non-compliance charges

laid in Canada are in relation to cross-border reporting offences, the Committee is aware of the July 2012 report by the United States (U.S.) Senate Permanent Subcommittee on Investigations of the U.S. Senate Committee on Homeland Security and Governmental Affairs, entitled U.S. Vulnerabilities to Money Laundering, Drugs, and Terrorist Financing: HSBC Case History, in relation to HSBC and money laundering using international wire transfers. The U.S. Senate Committee made several recommendations designed to strengthen anti-money laundering and anti-terrorist financing controls, particularly in relation to large, multinational financial institutions with affiliates in jurisdictions that are considered to be at high risk of being targeted by money launderers and those who finance terrorism. As financial institutions play a critical role in preventing illicit money from entering the financial system, the Committee feels that FINTRAC must be vigilant in ensuring that Canada's reporting entities comply with their obligations under the Act.

The Committee believes that an approach involving incremental legislative and regulatory changes must end.

The Committee believes that an approach involving incremental legislative and regulatory changes must end. Consequently, ongoing efforts are needed to ensure that the resources committed to detecting, deterring, investigating and prosecuting money laundering and terrorist financing offences have the best "results" in the least costly, burdensome and intrusive manner. While it is virtually impossible to eliminate the illegal activities that lead to the need to launder money, a continuation of the current incremental approach – which appears to involve changes to fill gaps by adding reporting entities and to meet evolving FATF recommendations that may or may not have relevance for Canada – is not the solution that Canada needs at this time.

Ongoing efforts are needed to ensure that the resources committed to detecting, deterring, investigating and prosecuting money laundering and terrorist financing offences have the best "results" in the least costly, burdensome and intrusive manner.

Having conducted a comprehensive study, the Committee's view is that the Act should be amended to address three issues:

- the existence of a structure for Canada's Regime that leads to increased performance in relation to the detection, deterrence, investigation and prosecution of money laundering and terrorist financing;
- the existence of information-sharing arrangements that ensure that suitable information is being collected and shared with the right people at the appropriate time, bearing in mind the need to protect the personal information of Canadians; and
- the existence of a scope and focus for the Regime that is properly directed to ensuring that individuals and businesses report the required information to the appropriate entity in an expedient manner.

The time for incremental change to the Regime has ended. The time for examination of fundamental issues has arrived.

The time for incremental change to the Regime has ended. The time for examination of fundamental issues has arrived.

CHAPTER THREE – THE DESIRED STRUCTURE AND PERFORMANCE

A. The Desired Structure

Every entity that plays a role in Canada's Regime shares a common goal with four elements: detection, deterrence, investigation and prosecution.

Every entity that plays a role in Canada's anti-money laundering and anti-terrorist financing regime (the Regime) shares a common goal with four elements: detection, deterrence, investigation and prosecution. While there are statutory limitations in relation to their roles and responsibilities, the Committee is not convinced that the federal departments and agencies involved in Canada's Regime are working well together or are being held to account. The Committee believes that more cooperation and an alignment of priorities among these departments and agencies would lead to better performance.

The Committee is aware that the structure of a country's anti-money laundering and anti-terrorist financing regime reflects that country's needs, and that the design of a particular country's regime may be both similar to and different from the design of other countries' regimes. For example, in some respects, Canada's Regime has a structure that is similar to that of the United States: the financial intelligence units – FINTRAC in Canada and the Financial Crimes Enforcement Network (FINCEN) in the United States – are under the authority of the Department of Finance and the Department of the Treasury respectively. As well, the Committee knows that other structures are possible. Meanwhile, the United Kingdom Financial Intelligence Unit (UKFIU) reports to the Home Office, which is responsible for security, counterterrorism, immigration and policing.

Having FINTRAC under the authority of the Department of Finance reinforces the beneficial links that exist between FINTRAC and Canadian financial institutions; it also ensures that developments in the financial system are quickly communicated to FINTRAC.

Having FINTRAC under the authority of the Department of Finance reinforces the beneficial links that exist between FINTRAC and Canadian financial institutions; it also ensures that developments in the financial system are quickly communicated to FINTRAC. That said, this structure could result in a degree of detachment between FINTRAC and law enforcement agencies. Any such detachment could give rise to a need to develop one or more mechanisms – such as access to FINTRAC's database by law enforcement agencies – designed to lead to better outcomes in terms of investigations and prosecutions.

One recommendation resulting from the 10-year evaluation of Canada's Regime was the formation of an interdepartmental working group to examine such issues as the sharing of information, the concerns of reporting entities, statistics on the Regime's performance, and the roles and responsibilities of the various departments and agencies that participate in the Regime. The Committee supports this recommendation, and believes that such a group could play a supervisory role in developing anti-money laundering and anti-terrorist financing strategies for the Regime, ensuring that priorities are aligned among the departments and

agencies, and assisting in the sharing of relevant information with appropriate recipients as quickly as possible. Furthermore, this group could focus on the fundamental goals of the Regime, rather than on the concerns of any particular stakeholder within the Regime.

For these reasons, the Committee recommends that:

1. **the federal government establish a supervisory body, led by the Department of Finance, with a dual mandate:**
    - **to develop and share strategies and priorities for combatting money laundering and terrorist financing in Canada; and**
    - **to ensure that Canada implements any recommendations by the Financial Action Task Force on Money Laundering that are appropriate to Canadian circumstances.**

    This supervisory body should be comprised of representatives of federal interdepartmental working groups and other relevant bodies involved in combatting money laundering and terrorist financing.

An overarching goal for the Committee is "value for money," one aspect of which is the quantifiable and non-quantifiable "results" of Canada's Regime.

B. Statistical Information About "Results" and Costs

An overarching goal for the Committee is "value for money," one aspect of which is the quantifiable and non-quantifiable "results" of Canada's Regime. From a quantitative perspective, the Committee is currently unable to assess the efficacy of the Regime in terms of investigations and prosecutions, as insufficient information was presented, and no information was received from law enforcement agencies, the Canadian Security Intelligence Service (CSIS), the Canada Border Services Agency (CBSA) and the Canada Revenue Agency (CRA) about the contribution made by FINTRAC case disclosures to federal prosecutions. From a non-quantitative perspective, it is virtually impossible to determine the extent to which Canada's Regime has had a deterrent effect.

FINTRAC made 777 case disclosures to law enforcement and other government agencies in the 2010-2011 fiscal year.

That said, the Committee is aware that FINTRAC made 777 case disclosures to law enforcement and other government agencies in the 2010-2011 fiscal year. Some of the disclosures occurred in response to a request from agencies that already had sufficient information to begin an investigation, while other disclosures were made to these agencies proactively by FINTRAC. The Committee did not receive information indicating the extent to which FINTRAC disclosures contributed to the success of investigations or provided any new avenues for investigation when disclosures were made in response to a request.

The Royal Canadian Mounted Police (RCMP) told the Committee that, in 2010, it received 93 proactive disclosures from FINTRAC, which resulted in 92 new criminal investigations. Of those 92 investigations, 69 were concluded without charges being laid, while the remaining 23 were ongoing as of February 14, 2012.

The Public Prosecution Service of Canada (PPSC) informed the Committee that, in the 2010-2011 fiscal year, 4 out of 46 people who were charged with money laundering under the *Criminal Code* were convicted, while 8 people pleaded guilty. An additional 6,733 charges were laid for possession of property obtained through criminal activity, with 61 people being convicted and 578 people pleading guilty. Regarding terrorist financing, the PPSC also stated that 6 people have been charged since the 2005-2006 fiscal year; 1 person has been convicted and 1 person has pleaded guilty.

A second aspect of the overarching goal of "value for money" is the costs incurred in order to obtain "results."

FINTRAC produces an annual public report that may include data regarding the Regime's "results." However, these data are not presented consistently from year to year. Annual reporting of the same data would assist in the evaluation of "results."

Finally, the Committee was informed that a one-for-one link between case disclosures and successful prosecutions does not exist, and that there are dangers in using successful prosecutions to measure the performance of Canada's Regime.

In the 2010-2011 fiscal year, $64.3 million in direct funding was provided to the CBSA, the CRA, the Department of Finance, FINTRAC, the Department of Justice, the PPSC and the RCMP in support of the Regime.

A second aspect of the overarching goal of "value for money" is the costs incurred in order to obtain "results." Expenditures of taxpayer funds in all areas should occur with a view to providing as much value as possible for the amount that is spent. From that perspective, the "results" of Canada's Regime must be assessed in the context of the Regime's costs.

In the 2010-2011 fiscal year, $64.3 million in direct funding was provided to the CBSA, the CRA, the Department of Finance, FINTRAC, the Department of Justice, the PPSC and the RCMP in support of the Regime. These departments and agencies may have also contributed additional resources from their general operating budgets in support of the Regime. As well, provincial and local law enforcement agencies contributed resources to anti-money laundering and anti-terrorist financing activities in Canada, although no amounts were presented to the Committee.

From this perspective, the Committee recommends that:

2. the federal government require the supervisory body recommended earlier to report to Parliament annually, through the Minister of Finance, the following aspects of Canada's anti-money laundering and anti-terrorist financing regime:

- **the number of investigations, prosecutions and convictions;**
- **the amount seized in relation to investigations, prosecutions and convictions;**
- **the extent to which case disclosures by the Financial Transactions and Reports Analysis Centre of Canada were used in these investigations, prosecutions and convictions; and**
- **total expenditures by each federal department and agency in combatting money laundering and terrorist financing.**

It is not possible, with existing information, to determine the extent to which Canada's Regime is obtaining "results" that are adequate in light of the associated costs.

C. Assessing Performance and Enhancing "Value for Money"

It is not possible, with existing information, to determine the extent to which Canada's Regime is obtaining "results" that are adequate in light of the associated costs. Given the significant costs and efforts involved, the Regime should be more effective than it is. The lack of information on "results" and costs, which was also highlighted in the 10-year external evaluation of the Regime, is a significant deficiency that would be remedied to some extent through annual reporting by the proposed supervisory body. Regular, independent performance reviews of the Regime would ensure that "value for money" is being provided.

Therefore, the Committee recommends that:

The lack of information on "results" and costs is a significant deficiency.

3. **the federal government ensure that, every five years, an independent performance review of Canada's anti-money laundering and anti-terrorist financing regime, and its objectives, occurs. The review could be similar to the 10-year external review of the regime conducted in 2010, and could be undertaken by the Office of the Auditor General of Canada. The first independent performance review should occur no later than 2014.**

In the course of an examination of the regimes that exist in other countries, the Committee learned about approaches that are used when investigations and prosecutions occur. If adopted here, these approaches could improve the "results" of Canada's Regime.

For example, some regimes distribute funds forfeited through money laundering and terrorist financing investigations to law enforcement agencies. The agencies use these funds to support training in financial crimes, as well as to finance other anti-money laundering and anti-terrorist financing activities. In Canada, forfeited funds are paid into the Consolidated Revenue Fund. Canada's law enforcement agencies, like

their counterparts in some other countries, could benefit from additional funds.

Consequently, the Committee recommends that:

In Canada, forfeited funds are paid into the Consolidated Revenue Fund.

4. **the federal government consider the feasibility of establishing a fund, to be managed by the supervisory body recommended earlier, into which forfeited proceeds of money laundering and terrorist financing could be placed. These amounts could supplement resources allocated to investigating and prosecuting money laundering and terrorist financing activities. The government should ensure that implementation of this recommendation does not preclude victims from collecting damages awarded to them by a court of law in a suit brought under the *Justice for Victims of Terrorism Act*.**

The Committee learned that, in the United States, certain law enforcement investigators have expertise in financial crimes, which was developed through participation in anti-money laundering and anti-terrorist financing policing activities This type of expertise – particularly when it is augmented by ongoing training to ensure that expertise evolves alongside technological advancements – would improve the Regime's "results."

Expertise in financial crimes – particularly when it is augmented by ongoing training to ensure that expertise evolves alongside technological advancements – would improve the Regime's "results."

Thus, the Committee recommends that:

5. **the federal government ensure that the Financial Transactions and Reports Analysis Centre of Canada and the Royal Canadian Mounted Police employ specialists in financial crimes, and provide them with ongoing training to ensure that their skills evolve as technological advancements occur.**

CHAPTER FOUR – THE APPROPRIATE BALANCE BETWEEN THE SHARING OF INFORMATION AND THE PROTECTION OF PERSONAL INFORMATION

A. FINTRAC's Relationship with Law Enforcement, Intelligence, and Other Domestic and Foreign Departments and Agencies

The Committee was told that the privacy provisions of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* have been weakened since 2000 because of the expansion in FINTRAC's ability to share information with law enforcement, intelligence and other federal departments and agencies, as well as with foreign financial intelligence units with which it has a memorandum of understanding. The Committee was also informed that FINTRAC's ability to disclose and disseminate information is too restrictive, giving rise to requests that information be more accessible to reporting entities and to other governmental departments and agencies in order to increase the "results" of Canada's Regime. Furthermore, the Committee was advised that some foreign financial intelligence units provide access to reporting databases and that reporting entities should be permitted to share information with each other under certain circumstances.

The Committee recognizes that a balance is needed: on one hand, law enforcement and other agencies should be supported; on the other hand, individuals have the right to protection of their personal information.

The Committee recognizes that a balance is needed: on one hand, law enforcement and other departments and agencies should be supported; on the other hand, individuals have the right to protection of their personal information. It can be difficult to find and maintain this balance, but appropriate resources and measures must exist to ensure the protection of personal information that Canadians have come to expect while still providing law enforcement and other departments and agencies with the information that will assist in the investigation of money laundering and terrorist financing.

An understanding of the manner in which case disclosures are used by those who receive them could lead to improvements in the quality and timeliness of the information provided by FINTRAC.

An understanding of the manner in which case disclosures are used by those who receive them could lead to improvements in the quality and timeliness of the information provided by FINTRAC. From that perspective, those who receive and use case disclosures should provide FINTRAC with feedback about how case disclosures contribute to investigations and prosecutions, and whether improvements are needed so that the disclosures continue to be useful in investigations and prosecutions.

As a result, the Committee recommends that:

6. **the federal government require the Royal Canadian Mounted Police, the Canadian Security and Intelligence Service, the Canada Border Services Agency and the Canada Revenue Agency to provide quarterly feedback to the Financial Transactions and Reports Analysis Centre of Canada regarding the manner in which they use case disclosures and how those disclosures could be improved.**

FINTRAC's mandate is limited to disclosing financial information pertaining to money laundering and terrorist financing.

According to the Act, FINTRAC's mandate is limited to disclosing financial information pertaining to money laundering and terrorist financing. Unless money laundering or terrorist financing is suspected, FINTRAC does not provide case disclosures to law enforcement and intelligence agencies for crimes such as tax evasion. The Committee believes that expanding FINTRAC's mandate to allow the disclosure of information on other crimes would enhance FINTRAC's role in contributing to the investigation and prosecution of criminal activities.

Therefore, the Committee recommends that:

7. **the federal government permit the Financial Transactions and Reports Analysis Centre of Canada to provide case disclosures in relation to offences under the Criminal Code or other Canadian legislation.**

Another option to facilitate the sharing of, and increase the usefulness of, information involves providing selected federal departments and agencies with direct access to FINTRAC's database.

Another option to facilitate the sharing of, and increase the usefulness of, information involves providing selected federal departments and agencies with direct access to FINTRAC's database, as occurs in certain other countries. Given the priority placed on individual privacy in Canada, any such access should ensure the protection of personal information.

Consequently, the Committee recommends that:

8. **the federal government develop a mechanism by which the Royal Canadian Mounted Police, the Canadian Security and Intelligence Service, the Canada Border Services Agency and the Canada Revenue Agency could directly access the Financial Transactions and Reports Analysis Centre of Canada's database. The Privacy Commissioner of Canada should be involved in developing guidelines for access.**

B. FINTRAC's Relationship with Reporting Entities

The proper balance must exist between providing useful and adequate information to FINTRAC on one hand, and ensuring that the compliance

burden on reporting entities is not onerous in terms of time, money or other resources on the other hand. Although specific information about costs was not provided, the Committee is aware that reporting entities incur costs in complying with their client identification, customer due diligence, recordkeeping, reporting and other obligations under the Act. From that perspective, it is important that the reports submitted by them be as useful as possible, and be submitted as expeditiously as possible, in order to meet the goals of Canada's Regime.

In the 2010-2011 fiscal year, reporting entities submitted nearly 20 million reports to FINTRAC; many of these were likely submitted on an automated basis. Of those reports, 58,722 were suspicious transaction reports that require a greater investment of human resources. The Committee believes that "results" in relation to Canada's Regime must be considered in the context of the compliance costs incurred by reporting entities, with these costs minimized to the extent possible while ensuring that the Regime's objectives are met.

The Committee believes that "results" in relation to Canada's Regime must be considered in the context of the compliance costs incurred by reporting entities, with these costs minimized to the extent possible while ensuring that the Regime's objectives are met.

Consequently, the Committee recommends that:

9. **the federal government and the Financial Transactions and Reports Analysis Centre of Canada, in consultation with entities required to report under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and its regulations, annually review ways in which:**
    - **the compliance burden on reporting entities could be minimized; and**
    - **the utility of reports submitted by reporting entities could be optimized.**

Given the critical role that both FINTRAC and reporting entities play in the Regime and the shared goal of reducing money laundering and terrorist financing in Canada, FINTRAC should provide reporting entities with feedback and information that educates them about the importance of their contributions and that enhances their role. FINTRAC is well-placed to provide reporting entities with a range of support including sector specific feedback to enhance effectiveness and achieve better "results."

FINTRAC is well-placed to provide reporting entities with a range of support including sector specific feedback to enhance effectiveness and achieve better "results."

For these reasons, the Committee recommends that:

10. **the Financial Transactions and Reports Analysis Centre of Canada provide entities required to report under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act with:**
    - **on a quarterly basis and specific to each entity, feedback on the usefulness of its reports;**

- **on a quarterly basis and specific to each sector, information about trends in money laundering and terrorist financing activities; and**
- **tools, resources and other ongoing support designed to enhance the training of employees of reporting entities in relation to the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and its obligations.**

In the Committee's view, reports should – to the extent possible – be submitted to FINTRAC in "real time" in order to enhance the "results" of Canada's Regime.

In the Committee's view, reports should – to the extent possible – be submitted to FINTRAC in "real time" in order to enhance the "results" of Canada's Regime. For example, the Committee is aware that, in accordance with FINTRAC's Guidelines, reports in relation to electronic funds transfers are currently submitted in batch transfers within five working days of the transaction; similarly, other reports have deadlines for submission.

From that perspective, the Committee recommends that:

11. the Financial Transactions and Reports Analysis Centre of Canada review its guidelines in relation to the period in which reports must be submitted to it by entities required to report under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and its regulations. The goal of the review should be to ensure that, to the greatest extent possible, reports are submitted in "real time."

The relatively low number of money laundering and terrorist financing convictions in Canada could be due to difficulties in having witnesses testify in court.

In the course of examining the regimes in other countries, the Committee learned that – in some countries – witnesses play an important role in combatting money laundering and terrorist financing. The relatively low number of money laundering and terrorist financing convictions in Canada could be due to difficulties in having witnesses testify in court. The Committee believes that protecting those who assist law enforcement agencies – whether anonymous sources or witnesses who agree to testify at trial – may lead to improved "results."

For this reason, the Committee recommends that:

12. the federal government, notwithstanding the recently proposed changes to Canada's Witness Protection Program Act, ensure that the safety of witnesses and other persons who assist in the investigation and prosecution of money laundering and/or terrorist financing activities is protected.

With multinational financial institutions such as HSBC failing to comply with anti-money laundering and anti-terrorist financing requirements in their respective jurisdictions, the Committee believes that increased

support for whistle blowers, could lead to improved "results." The number of incidences of non-compliance by reporting entities could be improved in Canada if individuals were to notify FINTRAC about failures by reporting entities to comply with the Act, or about individuals and entities who may be complicit in money laundering and/or terrorist financing.

The number of incidences of non-compliance by reporting entities could be improved in Canada if individuals were to notify FINTRAC about failures by reporting entities to comply with the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, *or about individuals and entities who may be complicit in money laundering and/or terrorist financing.*

Thus, the Committee recommends that:

13. **the federal government establish a mechanism by which employees of entities required to report under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and its regulations, and other individuals, could anonymously notify the Financial Transactions and Reports Analysis Centre of Canada about:**
    - **failures to comply with the requirements of the Act; and**
    - **individuals or entities possibly complicit in money laundering and/or terrorist financing.**

CHAPTER FIVE – THE OPTIMAL SCOPE AND FOCUS

A. Risk-based and Threshold-based Reporting

Canada's anti-money laundering and anti-terrorist financing regime (the Regime) has both threshold-based and risk-based reporting requirements. For example, the current $10,000 threshold for large cash transactions does not require an assessment of risk; such an approach for this type of transaction may limit the extent to which criminals try to introduce illicit cash into the financial system through reporting entities. Conversely, with the latter, suspicious transaction reports might help to identify a specific or series of transactions that could be linked to money laundering and terrorist financing.

To the extent that is feasible, all decisions about the design elements of Canada's Regime should be assessed through the lens of the associated risk.

To the extent that is feasible, all decisions about the design elements of Canada's Regime should be assessed through the lens of the associated risk. These design elements include:

- the sectors that should report;
- the activities that should be reported;
- the information that should be included in reports;
- the extent to which, and manner in which, records should be kept by reporting entities and FINTRAC;
- the frequency and method of client identification and monitoring by reporting entities that should occur;
- the clients in respect of whom identification and monitoring should occur; and
- the information that should be shared by FINTRAC with reporting entities about their reports, as well as with law enforcement and other government agencies in relation to investigations and prosecutions.

An entirely risk-based approach is not appropriate for Canada: there is a need for both threshold-based and risk-based approaches.

The Committee recognizes that an entirely risk-based approach would enable efforts to be focused on clients, transactions and payment methods that are considered to pose the greatest risk for money laundering and terrorist financing. However, an entirely risk-based approach – which is typified by the regime in the United Kingdom – is not appropriate for Canada: there is a need for both threshold-based and risk-based approaches.

Accordingly, the Committee recommends that:

14. the federal government enhance Canada's existing anti-money laundering and anti-terrorist financing regime by placing additional emphasis on:

- **the strategic collection of information; and**
- **risk-based analysis and reporting.**

B. Reporting Entities

Consideration should be given to the sectors designated as reporting entities for purposes of Canada's Regime. In determining whether a particular sector should be designated, the circumstances in which cash transactions having a large dollar amount can occur should be an important consideration. From that perspective, in addition to the sectors that are currently designated as reporting entities, consideration should be given to vendors of electronic products, vehicles, large equipment, boats and art, all which could involve large cash transactions. As a payment method, cash presents risks that may not arise with other payment options.

As a payment method, cash presents risks that may not arise with other payment options.

Consequently, the Committee recommends that:

15. the federal government review, on an ongoing basis, the entities required to report under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and its regulations to ensure the inclusion of sectors where cash payments exceeding the current $10,000 threshold are made.

Both risk-based and threshold-based reports are appropriate, depending on the circumstances.

C. International Electronic Funds Transfers

As noted earlier, both risk-based and threshold-based reports are appropriate, depending on the circumstances. Regarding the latter, such reports may be particularly important in respect of international electronic funds transfers, as Canada could be one in a series of countries through which money laundering, terrorist financing and other financial crimes occur.

Some countries are considering removal of the $10,000 threshold for international electronic funds transfers, the result of which would be the submission of reports in respect of all such transfers. As FINTRAC received approximately 12 million reports in relation to international electronic funds transfers from reporting entities in the 2010-2011 fiscal year, the Committee is concerned that FINTRAC may have insufficient resources to collect and analyze more reports. The removal of such a

threshold would also have implications for reporting entities, which would face increased compliance costs; higher compliance costs could be particularly problematic for some small and medium-sized enterprises. Nevertheless, the Committee believes that money laundering and terrorist financing are global issues, and that international electronic funds transfers are an activity where international standards are required.

The Committee believes that money laundering and terrorist financing are global issues, and that international electronic funds transfers are an activity where international standards are required.

Therefore, the Committee recommends that:

16. the federal government eliminate the current $10,000 reporting threshold in relation to international electronic funds transfers.

D. Consideration of Technological Changes

One benefit of a parliamentary review requirement is the opportunity it gives legislators to ensure that legislation is amended as economies, societies and technologies evolve. During the current review of the Act, the Committee noted how technology has changed since the 2006 review. Technological changes have implications for the manner in which reporting entities can fulfil their obligations and people can undertake financial transactions.

Prepaid payment cards have emerged as a method of moving "dirty money" across international borders without involving financial institutions.

The development of electronic methods to launder money must be addressed through timely amendments to the Act and its regulations. In particular, prepaid payment cards, which cannot be seized under the Act by law enforcement or border agents because such cards are not defined as "monetary instruments", have emerged as a method of moving "dirty money" across international borders without involving financial institutions. Without the involvement of financial institutions, no report is required pursuant to the Act. FINTRAC's ability to detect emerging methods of money laundering and terrorist financing, some of which are related to advancements in technology, is enhanced both through ongoing review of Canada's Regime and the legislation that establishes it, and through continuous training of its employees.

Consequently, the Committee recommends that:

17. the federal government review annually, and update as required, the definition of "monetary instruments" in the Proceeds of Crime (Money Laundering) and Terrorist Financing Act in order to ensure that it reflects new payment methods and technological changes.

E. Public Awareness

At present, many people are unaware of the nature and scope of money laundering and terrorist financing in Canada, and of Canada's Regime.

Residents of all countries – whether individuals or businesses – can play a role in combatting money laundering and terrorist financing, which are global issues. In order for residents to play a role, they must be informed about the activities that constitute money laundering and terrorist financing, and about specific actions they can take in the event that they suspect or are made aware of these activities. At present, many people are unaware of the nature and scope of money laundering and terrorist financing in Canada, and of Canada's Regime. Recently, the Committee completed an examination of Bill C-28, An Act to amend the Financial Consumer Agency of Canada Act, which would create the position of Financial Literacy Leader within the Financial Consumer Agency of Canada. In that context, the Committee believes that the proposed Financial Literacy Leader may have a role to play in educating Canadians about money laundering and terrorist financing.

As a result, the Committee recommends that:

18. the federal government, in consultation with the proposed Financial Literacy Leader, develop a public awareness program about Canada's anti-money laundering and anti-terrorist financing regime, and about actions that individuals and businesses can take to combat money laundering and terrorist financing.

CHAPTER SIX – CONCLUSION

There is a lack of clear and compelling evidence that Canada's Regime is attaining "results" – whether measured by the detection and/or deterrence of money laundering and terrorist financing or by significant contributions to related investigations and prosecutions – that are commensurate with the time, monetary and other resources devoted to it.

In undertaking the statutory review required by section 72 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, the Committee heard testimony from federal, provincial and international departments and agencies, as well as the private sector, about the various elements of Canada's anti-money laundering and anti-terrorist financing regime (the Regime). In determining whether the legislation is having the intended effect, the Committee considered the Act's purpose and the context in which the legislation was initially enacted and subsequently amended.

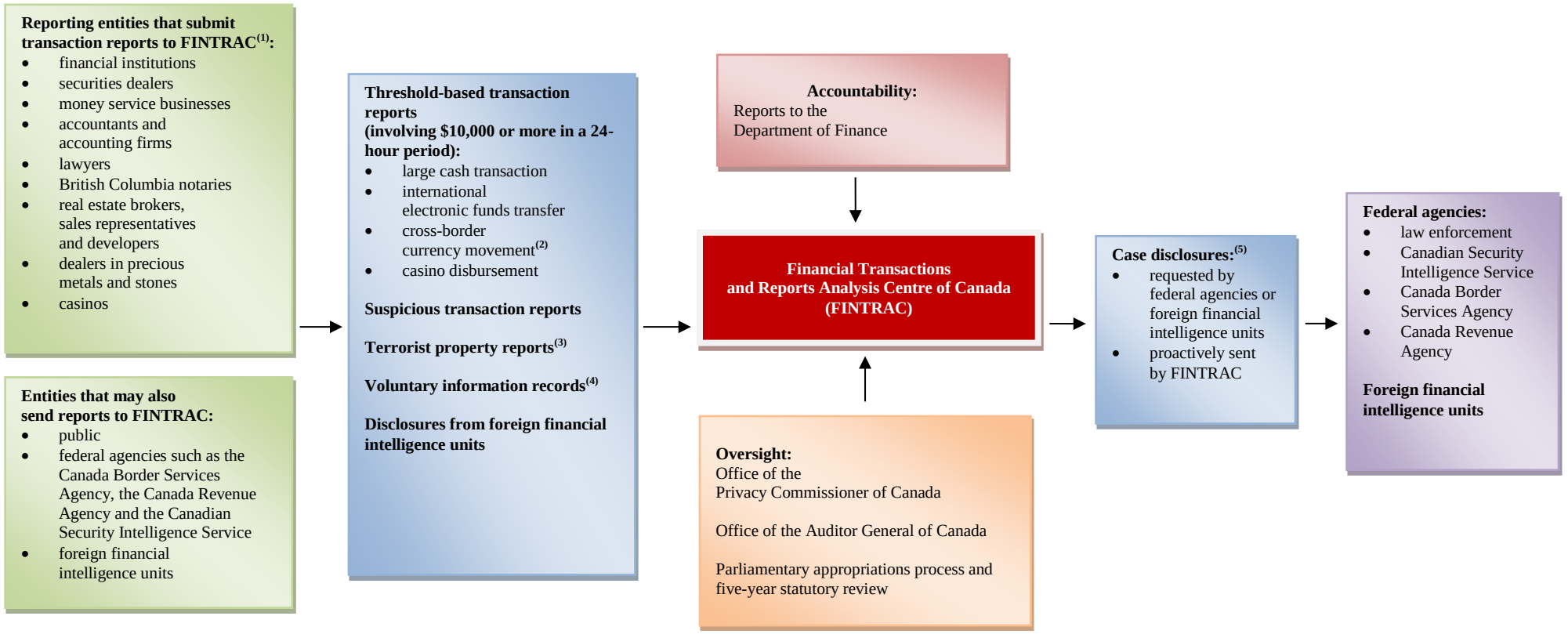
Having considered the testimony, the Committee concludes that there is a lack of clear and compelling evidence that Canada's Regime is attaining "results" – whether measured by the detection and/or deterrence of money laundering and terrorist financing or by significant contributions to related investigations and prosecutions – that are commensurate with the time, monetary and other resources devoted to it. In some sense, the approach of incremental legislative and regulatory changes that appears to have been used in the past has not been entirely successful. While elements of Canada's Regime that are working well must be retained, elements that are not having the desired "results" must be changed, and lessons that can be learned from the regimes in other countries must be embraced.

Believing that "value for money" should be an overarching goal, the Committee has made recommendations in three areas:

- the desired structure and performance Canada's Regime;
- the appropriate balance between the sharing of information and the protection of personal information in that Regime; and
- the optimal scope and focus for the Regime.

The Committee is confident that implementation of these recommendations will lead to the fundamental changes that are needed to improve the efficacy of Canada's anti-money laundering and anti-terrorist financing regime. The Committee looks forward to examining proposed legislative changes to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and to the next statutory review.

APPENDIX A – CANADA'S ANTI-MONEY LAUNDERING AND ANTI-TERRORIST FINANCING REGIME



Notes: (1) Reporting entities are also required to implement a compliance regime, maintain records of transactions and identify clients.

(2) Only the Canada Border Services Agency submits cross-border currency movement reports to FINTRAC.

(3) Terrorist property reports are submitted when any person has property in his/her possession or control that he/she knows or believes is owned or controlled by or on behalf of a terrorist group or a listed person.

(4) Voluntary information records can be submitted by members of the public or federal agencies.

(5) FINTRAC may disclose information if it has reasonable grounds to suspect that the information to be disclosed would be relevant to an investigation or prosecution of a money laundering or terrorist activity financing offence, or relevant to threats to the security of Canada.

(6) Regarding lawyers, due to an ongoing court challenge examining whether the application of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* to lawyers would contravene solicitor-client privilege, the provisions of the Act that apply to the legal profession are currently inoperative. Source: Financial Transactions and Reports Analysis Centre of Canada, *FINTRAC's Business Process*, 2011, http://www.fintrac.gc.ca/publications/brochure/2011-02/longdesc-eng.asp; Financial Transactions and Reports Analysis Centre of Canada, *Annual Report 2011*, 2011, http://www.fintrac.gc.ca/publications/ar/2011/ar2011-eng.pdf.

APPENDIX B – SUMMARY OF THE EVIDENCE

Strengthening Customer Identification and Due Diligence

A. The Act and Its Regulations, and the Department of Finance's Proposals

1. Client Identification Records

Paragraph 54(1)(a) of the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations requires financial entities and casinos to ascertain the identity of at least three authorized signers of each business account. They are not, however, required to keep a record of their identities or to identify the measures taken to confirm the identity of the signers. Proposal 1.1 in the Department of Finance's December 2011 consultation paper (the consultation paper) suggests that these reporting entities should be required to maintain records regarding the identities of the authorized signers.

2. Exemptions for Introduced Business

Pursuant to subsection 56(2) and paragraph 62(1)(b) of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (the Act), if a financial institution introduces its client to another financial institution, the second – or recipient – financial institution is exempt from some of the customer identification and due diligence requirements that would normally apply in respect of a new client. Proposal 1.2 in the consultation paper suggests that these exemptions should be reviewed, and that the division of responsibility regarding recordkeeping, client identification and due diligence in relation to the client introduced by one financial institution to another financial institution should be clarified.

3. Non-face-to-face Identification Requirements

In 2007, in Schedule 7 to the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations, the federal government introduced measures for accounts opened at financial institutions in situations where the client is not physically present or the identity of the client cannot be confirmed with a government-issued identification document. Bank statements from another financial institution have been used to confirm the identity of the account holder. Proposal 1.3 in the consultation paper suggests that clarity is needed about what procedures might be used to confirm the identity of the client in the instances discussed above.

4. Signing Authority

Proposal 1.4 in the consultation paper suggests that the requirement that reporting entities must maintain a record of their clients' signatures should be reviewed.

5. Politically Exposed Foreign Persons

Through the definition of "politically exposed foreign person" in subsection 9.3(3) of the Act, a distinction is implicitly made between clients who are politically exposed foreign persons (PEFPs) and other clients. PEFPs include: heads of state; senior politicians;

senior government, judicial or military officials; senior executives of state-owned enterprises; and political party officials. Due to their prominence and influence, these foreign officials are deemed to be a greater risk in terms of involvement in money laundering and/or terrorist financing activities. Proposal 1.5 in the consultation paper suggests that the definition of "politically exposed foreign person" should be expanded to include close associates of these foreign officials.

6. Politically Exposed Foreign Persons and Insurance Companies

Proposal 1.6 in the consultation paper suggests that insurance companies should be required to determine if a new client is a PEFP, and to follow all relevant PEFP requirements in the event that he/she is found to be such a person.

7. Existing Clients and Politically Exposed Foreign Persons

Under paragraph 54.2(b) and subsection 57.1(2) of the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations, financial entities and securities dealers are not required to determine if their existing low-risk account holders are PEFPs. Proposal 1.7 in the consultation paper suggests that reporting entities should be required to determine if all existing account holders are PEFPs.

8. Exemption for Listed Corporations

Pursuant to paragraph 62(2)(m) of the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations, reporting entities are not required to keep records in respect of public bodies or corporations with net assets of at least $75 million that are traded on a Canadian or other designated stock exchange, since – due to their public reporting requirements – these corporations are deemed to be a lower risk in terms of involvement in money laundering and/or terrorist financing activities. Proposal 1.8 in the consultation paper suggests that the threshold of $75 million should be eliminated.

9. Existence of a Corporation

The frequency with which reporting entities must confirm the existence of a corporation is not identified in the Act. Proposal 1.9 in the consultation paper suggests that reporting entities should be required to confirm annually the existence of their corporate clients. According to the proposal, this confirmation would occur by means of documents issued by the competent authority governing the relevant legislation under which the corporate client is incorporated.

10. Third Party

Pursuant to section 8 of the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations, a third party "provides instructions" to reporting entities, although some have interpreted the phrase to mean that the third party "carries out instructions." Proposal 1.10 in the consultation paper suggests that the term "third party" should be replaced by the term "instructing party."

B. What the Witnesses Said and Proposed

1. Client Identification

The Ontario Lottery and Gaming Corporation, Amex Bank of Canada and MasterCard supported changes to the existing requirements in relation to non-face-to-face identification, which they believe are complicated and have become less relevant over time. As well, in their view, the Act and its regulations have not been amended to recognize changes in digital identification and authentication methods. Amex Bank of Canada and the Ontario Lottery and Gaming Corporation advocated a more timely administrative approval process, rather than a legislative process, by which new identification methods might be used for the purposes of the Act's identification requirements. They believed that, with this change, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) would have to be more open to accepting electronic copies of identification and other documents.

In order to verify the identity of clients more easily, Amex Bank of Canada proposed that specific government databases could be used by reporting entities to confirm the identity of their clients, as is the case in Australia, the United Kingdom and the United States. Amex Bank of Canada also identified a number of examples of electronic documents that could be used to verify the identity of clients.

To encourage the use of a risk-based approach for client identification purposes, MasterCard suggested that a principled standard be considered for non-face-to-face identification rather than prescribing certain data sources that could be used to verify identification.

The Canadian Gaming Association and the Ontario Lottery and Gaming Corporation highlighted that the current regulations for non-face-to-face client identification limit the growth of the Canadian online gaming sector due to the requirements under the Act to provide certain identification documents to the reporting entity, and suggested that these regulations encourage Canadian online gamblers to use offshore gaming companies rather than those offered by provincial gaming operators.

With regard to client identification documents, the Canadian Real Estate Association asked that consideration be given to accepting expired documents for purposes of client identification, particularly for reporting entities with elderly clients.

Western Union emphasized that it has stricter client due diligence requirements than those set out in the Act; it requires identification from its clients when sending $1,000 or more or when receiving more than $300 as well as personal interviews when clients are sending more than $7,500. Western Union also has monitoring systems that analyze transactions occurring across all Western Union locations, with the result that Western Union submits a high number of suspicious transaction reports to FINTRAC.

2. Signing Authority

Amex Bank of Canada supported a review of the record of signing authority requirement, and advocated the adoption of digital identification methods and the elimination of written signature requirements.

3. Politically Exposed Foreign Persons

Mouvement Desjardins and the Investment Funds Institute of Canada asserted that the Department of Finance's proposals regarding client identification and recordkeeping requirements in relation to PEFPs would place an onerous compliance burden on insurance companies. The Investment Funds Institute of Canada stated that existing clients might be reluctant to provide additional personal information, while Mouvement Desjardins argued that expanding the PEFP requirements to existing clients would extend client identification and recordkeeping obligations to low-risk transactions and insurance products; in its view, only those transactions or insurance products that are high risk for money laundering or terrorist activities should be subject to client identification and recordkeeping obligations, and these transactions and products should be specified.

4. Exemption for Listed Corporations

The Investment Funds Institute of Canada and the Investment Industry Association of Canada supported the proposed recordkeeping exemption for listed corporations and the proposed removal of the $75 million threshold for net assets.

The Investment Industry Association of Canada urged consideration of extending the proposed exemption for listed companies to foreign companies that are listed on a foreign stock exchange. Given that Proposal 1.8 in the consultation paper recognizes that listed companies have extensive reporting requirements under Canadian securities law and thus are at low risk for money laundering or terrorist financing, the Investment Industry Association of Canada believed that a similar exemption should be given to foreign companies that are subject to similar securities regulation regimes.

The Investment Funds Institute of Canada stressed that its members would be concerned if changes to the current exemption that allows investment dealers to use the "allocated compliance model" for client identification, a process that minimizes the duplicative collection of personal client identification, were to occur.

Closing the Gaps in Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime

A. The Act and Its Regulations, and the Department of Finance's Proposals

1. International Electronic Funds Transfer Threshold

Paragraphs 12(1)(b) and (c) of the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations require reporting entities to disclose, to FINTRAC, electronic funds transfers of at least $10,000 originating in or destined for foreign jurisdictions.

Proposal 2.1 in the consultation paper suggests that this $10,000 threshold amount should be eliminated.

2. Prepaid Payment Cards

Some prepaid payment cards are issued by entities that are not required to report under the Act. Proposal 2.2 in the consultation paper suggests that customer identification and due diligence requirements should apply to entities that issue prepaid payment cards and other prepaid devices.

3. International Transactions and Prepaid Credit Cards

Proposal 2.3 in the consultation paper suggests that the Cross-Border Currency and Monetary Instruments Reporting Regulations should apply to cross-border transactions that occur on a prepaid payment card or other prepaid device.

4. Life Insurance Companies, Agents and Brokers

Subsection 19(1) of the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations requires reporting entities to disclose life insurance and annuity policies for which the client will be expected to make payments of at least $10,000. Other life insurance activities deemed to be low risk for money laundering are not required to be reported. Proposal 2.4 in the consultation paper suggests that the reporting requirements that currently exist in relation to life insurance and annuity payments of a certain amount should be extended to other insurance activities offered by insurance companies, agents and brokers, including account openings and loan products. As well, according to the proposal, the $10,000 threshold amount for reporting with respect to annuity and life insurance policies should be eliminated.

5. Reporting Obligations Below the Large Cash Transaction Threshold and Life Insurance

Section 17 of the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations requires life insurance companies, agents and brokers to disclose all transactions of at least $10,000. Proposal 2.5 in the consultation paper suggests that, unless the origin of transactions is known and could be deemed to be low risk, these reporting entities should be required to disclose transactions with a value below that threshold amount.

6. Large Cash Transaction Obligations

According to section 13 of the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations, reporting entities are required to disclose cumulative large cash transactions of at least $10,000 in a 24-hour period; however, if those funds are received by an agent or affiliate of the reporting entity, disclosure is not required. Proposal 2.6 in the consultation paper suggests that this exemption in relation to agents and affiliates should be eliminated.

7. Reporting Requirements and Dealers in Precious Metals and Stones

Section 39.1 of the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations requires reporting entities to disclose all precious metal and stone transactions that have a value of at least $10,000 and that meet various other criteria. Proposal 2.7 in the consultation paper suggests that an exemption should be created for the sale of precious metals and stones for manufacturing purposes unrelated to money laundering and terrorist financing.

8. Reporting Obligations for the Accountant Sector

Proposal 2.8 in the consultation paper suggests that an exemption with respect to reporting should be created for activities undertaken by accountants and accounting firms when providing trustee-in-bankruptcy services.

9. 24-Hour Rule

Subsection 3(1) of the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations requires reporting entities to disclose multiple transactions that total at least $10,000 in a 24-hour period. Proposal 2.9 in the consultation paper suggests that the language in the Regulations should be clarified so as not to exclude certain transactions that ought to be disclosed.

B. What the Witnesses Said and Proposed

1. International Electronic Funds Transfer Threshold

Capra International Inc. and KPMG Forensic supported elimination of the $10,000 international electronic funds transfer (EFT) threshold, believing that the result would be more information being sent to FINTRAC for analysis. Capra International Inc. thought that elimination of the threshold would be particularly beneficial in trying to deter terrorist financing, as it typically involves smaller amounts of money when compared to money laundering or other types of criminal activity. However, KPMG Forensic, Credit Union Central of Canada, the Office of the Privacy Commissioner of Canada and the Canadian Bankers Association expressed doubts about FINTRAC's ability to process and analyze so many additional reports in an effective manner.

The rationale given in the consultation paper for eliminating the international EFT threshold was to target terrorist financing and to be consistent with other jurisdictions around the world; however, the Canadian Security Intelligence Service (CSIS) stated that an increase in the number of reports being submitted to FINTRAC would not necessarily result in a proportional increase in the number of case disclosures being sent by FINTRAC to law enforcement and other government agencies. The Office of the Privacy Commissioner of Canada and the Canadian Bankers Association identified a need for further study to determine whether a threshold of $10,000 or some other amount should be the appropriate threshold for international EFT and/or large cash transaction reports.

While KPMG Forensic thought that a change in the international EFT threshold would not be overly problematic for reporting entities that have an automated reporting procedure for EFTs, other reporting entities – such as Credit Union Central of Canada, Mouvement Desjardins, the Canadian Association of Independent Life Brokerage Agencies, the Canadian Life and Health Insurance Association Inc., the Investment Industry Association of Canada and Western Union – indicated that elimination of the international EFT threshold would impose a significant compliance burden on reporting entities given the additional reports that would have to be submitted to FINTRAC. The Investment Industry Association of Canada argued that using a risk-based approach and relying on suspicious transaction reporting to examine smaller financial transactions would be more valuable to FINTRAC in targeting terrorist financing than would lowering the international EFT threshold.

2. Prepaid Payment Cards

According to the Royal Canadian Mounted Police (RCMP), new technologies to carry and transfer money are being examined by law enforcement agencies for their use in money laundering; in particular, store value cards, such as retail gift cards, and prepaid credit cards are increasing in prevalence. The Department of Finance indicated that customer due diligence and client identification should occur in relation to individuals buying prepaid payment cards. KPMG Forensic suggested that further study is needed regarding the type of prepaid payment card that should be included under the Act; for example, open loop prepaid payment cards, which are accepted at numerous retail locations, may be at a higher risk of being used for money laundering when compared to closed loop cards, which are accepted only at a particular retailer.

MasterCard highlighted that non-reloadable and reloadable prepaid credit cards have different levels of risk of being used for money laundering and terrorist financing.1 It noted that non-reloadable prepaid credit cards have lower value limits and are of lower risk than reloadable prepaid credit cards. Although MasterCard stated that the imposition of customer identification requirements on retailers and issuers of prepaid payment cards would create compliance burdens that would outweigh any anti-money laundering benefits, it suggested that the financial institutions that issue reloadable prepaid cards would be in the best position to perform any customer due diligence requirements. Similarly, Amex Bank of Canada requested that reporting entities not be required to undertake customer due diligence measures in respect of prepaid devices with a balance, or cumulative monthly transaction amount, of less than $3,000.

The Office of the Privacy Commissioner of Canada argued that the increased collection of personal information by the retail sector would be a significant undertaking with a high compliance burden, and suggested that measures that would not require the collection of personal information should be considered. The Office of the Privacy Commissioner of Canada and KPMG Forensic indicated that establishing a limit for the amount of money

[1] Non-reloadable cards are purchased at retailers, do not have a cash back option and have a maximum load limit at the time of purchase. Reloadable prepaid credit cards can be reloaded with additional funds and cash can be withdrawn from these cards at an automated teller machine; these cards have a greater maximum load limit and are available from financial institutions that issue the cards.

that could be loaded onto prepaid payment cards without client identification requirements being imposed would be a viable alternative to collecting personal information.

3. Precious Metals and Stones

The Canadian Jewellers Association asked that Proposal 2.7 be more specific with regard to the term "manufacturing," as the term has several different meanings that may not be consistent with the intention of the proposal.

4. Reporting Obligations for the Accounting Sector

The Canadian Institute of Chartered Accountants supported Proposal 2.8 and argued that the proposed exemption should be extended to activities undertaken by accountants when acting as a receiver, receiver-manager, interim receiver or monitor in an insolvency proceeding, since – in those circumstances – accountants are acting under the supervision of a court and not on behalf of a client. According to it, broadening the exemption would also provide consistency with interpretation notices provided by FINTRAC.

Improving Compliance, Monitoring and Enforcement

A. The Act and Its Regulations, and the Department of Finance's Proposals

1. Registration of Money Services Businesses

Proposal 3.1 in the consultation paper suggests that the information that money services businesses are required to disclose when they register with FINTRAC should be reduced.

2. Eligibility Requirements for Money Services Business Registration

Subsection 3(1) of the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations stipulates that individuals convicted of violating current legislation specified in section 11.11 of the Act are prohibited from registering as a money services business. Proposal 3.2 in the consultation paper suggests that individuals should also be prohibited from registering as a money services business if they have been convicted of violating acts that were later repealed or replaced.

3. Non-compliance with Reporting Obligations

According to section 73.15 of the Act, FINTRAC can impose a penalty on reporting entities that have failed to disclose a suspicious transaction, large cash transaction, electronic funds transfer to or from a foreign jurisdiction, or terrorist property report. Non-compliance proceedings against reporting entities that have not complied with the Act terminate after the penalty has been paid. Proposal 3.3 in the consultation paper suggests that FINTRAC should be permitted to require a reporting entity to file the report that it neglected to submit, even after a penalty has been paid, or to impose additional penalties on the reporting entity in the event that it continues to fail to provide FINTRAC with the report.

4. Reasonable Measures

The Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations require reporting entities to take reasonable measures to obtain various information when performing their due diligence role with respect to clients. They are not, however, required to record the reasonable measures that they have taken. Proposal 3.4 in the consultation paper suggests that reporting entities should be required to record the reasonable measures that they have taken in fulfilling their client identification and customer due diligence requirements.

5. Reporting

According to paragraph 73(1)(e.1) of the Act, modifications to the information on the reporting form used by reporting entities must be undertaken through the regulatory process and receive Governor in Council approval. Proposal 3.5 in the consultation paper suggests that the Minister of Finance should have the authority to modify the information on the reporting form.

6. Cross-Border Currency Reporting

Section 12 of the Act requires individuals and entities to report to the Canada Border Services Agency (CBSA) when they have imported or exported monetary instruments; this reporting must occur when the instruments have a value of at least $10,000. Proposal 3.6 in the consultation paper suggests that the CBSA's powers should be broadened so that it would have the authority to question individuals and entities about their compliance with the Act and to compel truthful responses.

B. What the Witnesses Said and Proposed

1. Non-compliance with Reporting Obligations

According to FINTRAC, having sound recordkeeping and client identification requirements as well as ensuring that reporting entities comply with these requirements are means by which to create an environment that is inhospitable to money laundering and terrorist financing. It also stated that the monetary penalties for non-compliance with the Act are applied sparingly, with only 15 penalties being assessed since the end of 2008, when it became possible to apply monetary penalties. As well, FINTRAC indicated that it will work with reporting entities to improve their compliance with the Act's requirements. KMPG Forensic said that, generally, reporting entities have a desire to comply with their obligations under the Act in order both to meet regulatory requirements and to be socially responsible.

The Public Prosecution Service of Canada provided statistics on the number of charges laid for non-compliance with the Act. During the 2005-2006 to 2009-2010 fiscal years, 89 non-compliance charges were laid, with 3 convictions and 31 guilty pleas; 68 of the 89 charges pertained to cross-border reporting violations. In the 2010-2011 fiscal year, 34 charges were laid for non-compliance with the Act, and all were related to cross-border reporting; there were no convictions and 13 guilty pleas.

Capra International Inc. noted that there is a lack of understanding of reporting obligations and how to identify the level of risk for a transaction. KMPG Forensic, the Canadian Life and Health Insurance Association Inc., C.D. Barcados Co. Ltd. and the Canadian Jewellers Association suggested that FINTRAC should provide more guidance and feedback before sending findings letters to the reporting entities. KPMG Forensic indicated that, as a result of not understanding their reporting requirements and a fear of monetary penalties for non-compliance, reporting entities tend to over-report rather than pose questions to FINTRAC regarding reporting requirements. The Office of the Privacy Commissioner of Canada also observed, in its last audit of FINTRAC in 2009, that reporting entities were submitting reports for transactions that did not meet the threshold of "reasonable grounds to suspect" that the transaction was related to money laundering or terrorist financing; these submissions were occurring because reporting entities feared being fined for non-compliance and they lacked information about what constitutes a suspicious transaction.

In the view of the Canadian Association of Independent Life Brokerage Agencies and the Canadian Life and Health Insurance Association Inc., FINTRAC should provide information on money laundering and terrorist financing trends in relation to particular industries; in this regard, the Canadian Life and Health Insurance Association Inc. advocated the creation, by FINTRAC, of a "threat assessment by sector" document similar to those provided by other countries' financial intelligence units. Similarly, C.D. Barcados Co. Ltd. and the Canadian Jewellers Association highlighted the need for information on money laundering trends in the precious metals and stones sector, and argued that FINTRAC should provide reporting entities with a sample compliance regime so that they could evaluate whether the measures that they have taken are sufficient to meet the compliance requirements of the Act.

The Canadian Real Estate Association suggested that, rather than imposing a fine on reporting entities that fail to provide FINTRAC with all of the information needed for a report, FINTRAC could require reporting entities to take reasonable measures to obtain the necessary information. Redwood Realty asserted that civil and criminal penalties for non-compliance with an administrative task could be seen to be excessive.

The Investment Industry Association of Canada asserted that, despite the challenges encountered by most reporting entities in trying to obtain feedback from FINTRAC, FINTRAC is open to hearing from the reporting entities and to learning more about the needs of the various industries. Capra International Inc. commented that FINTRAC is often constrained in its ability to provide feedback to reporting entities due to the Act's restrictions regarding the sharing of information as well as privacy legislation.

Strengthening the Sharing of Information in Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime

A. The Act and Its Regulations, and the Department of Finance's Proposals

1. Disclosure Information

According to subsection 55(7) of the Act, FINTRAC is able to disclose designated – rather than all – information to law enforcement and other government agencies. Proposal 4.1 in the consultation paper suggests that the designated information that FINTRAC is permitted to share with law enforcement and other government agencies should be expanded to include:

- the gender and occupation of the individual to whom the disclosure is related;
- the grounds for suspicion provided by international partners;
- the narrative from cross-border seizure reports;
- the actions that have been taken by reporting entities with respect to a suspicious transaction; and
- the "reasonable grounds to suspect" for which FINTRAC has decided to share this information.

2. Foreign Information Sharing

Section 58 of the Act permits FINTRAC to share designated information with law enforcement, government or foreign agencies that have powers and duties that are similar to those of FINTRAC. Proposal 4.2 in the consultation paper suggests that FINTRAC should be permitted to disclose the identity of the foreign entity or individual to foreign agencies when it would be relevant to do so.

3. Information Sharing and Registered Charities

The Canada Revenue Agency's Charities Directorate, which administers the registration of charities, receives information from government entities, such as CSIS, the RCMP and FINTRAC. Proposal 4.3 in the consultation paper suggests that the CBSA should be permitted to share information with the Charities Directorate when it is related to cross-border seizures associated with charities.

4. Disclosure of Information on Charities

Proposal 4.4 in the consultation paper suggests that the conditions under which FINTRAC discloses information to the Canada Revenue Agency (CRA) should be reviewed.

5. Disclosures to the Canada Border Services Agency

Under paragraph 55(3)(e) of the Act, FINTRAC is required to disclose, to the CBSA, information that is relevant to cases related to the importation of prohibited, controlled or regulated goods. Proposal 4.5 in the consultation paper suggests that this disclosure requirement should be expanded to include the exportation of these goods.

6. Disclosures for National Security

Proposal 4.6 in the consultation paper suggests that FINTRAC should be required to disclose information to the CBSA when there are grounds to suspect that there may be a threat to national security.

7. Disclosures to Police

Subsection 36(2) of the Act requires FINTRAC to disclose pertinent information to the police when there are reasonable grounds to suspect that the information is relevant to a money laundering or terrorist financing offence. Proposal 4.7 in the consultation paper suggests that this disclosure requirement should be extended to cases where a person may be in imminent danger of physical injury or death.

B. What the Witnesses Said and Proposed

1. Disclosure Information

Capra International Inc. stated that, under section 55 of the Act, FINTRAC can only disclose designated information to law enforcement and other government agencies, while FINTRAC mentioned that there is a disclosure threshold that must be met before information is provided to law enforcement and other government agencies; the disclosure threshold includes an examination of voluntary information reports from law enforcement and other government agencies or the public, suspicious transaction reports, newspaper articles and other media to determine whether the disclosure of information is warranted. FINTRAC indicated that, with regard to foreign requests for information, it has the discretion to determine whether it will disclose information, even if a memorandum of understanding exists between the financial intelligence units of the two countries; in 2010, FINTRAC provided 150 disclosures to, and received 50 disclosures from, foreign financial intelligence units.

The Canadian Bankers Association argued that FINTRAC should be permitted to disclose information to reporting entities and that, under certain circumstances, reporting entities should be allowed to disclose information to each other. An example provided by the Canadian Bankers Association of the restrictions placed on FINTRAC with regard to the disclosure of information is that FINTRAC cannot ask a reporting entity for additional information after receiving a suspicious transaction report. It highlighted that, under the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, the United States allows banks to share information under very rigid circumstances. While the Canadian Bankers Association acknowledged the need for the protection of personal information, it

advocated a balance between the protection of personal information on one hand and preventing criminals from using financial institutions and other reporting entities to launder funds or finance terrorism on the other hand.

In order to improve communication among the partners in Canada's anti-money laundering and anti-terrorist financing regime, Capra International Inc. argued that the Department of Finance should lead an interdepartmental working group with the partners to examine regime-related legislation and regulations with a view to removing any barriers that would decrease the efficiency of the regime.

2. Disclosure of Information on Charities

The Canadian Bar Association indicated that a more extensive review of the disclosure provisions in the Act as they pertain to charities should be conducted in order to address deficiencies in the collection and use of information against registered charities, and to ensure that the principles of procedural fairness and natural justice are observed.

Countermeasures

A. The Act and Its Regulations, and the Department of Finance's Proposals

1. Countermeasures

Proposal 5.1 in the consultation paper suggests that the Minister of Finance should require reporting entities to take countermeasures in relation to foreign states and foreign entities that are deemed to be high risk for facilitating money laundering or terrorist financing; the list of countermeasures would be an enhancement of the Act's existing requirements in relation to domestic transactions and domestic reporting requirements. For example, reporting entities would be required to identify clients, disclose the documents used to identify clients, take reasonable measures to identify the persons who control corporations and entities, ascertain the identity of clients of foreign financial institutions with whom the reporting entity has a relationship, and perform due diligence in relation to clients, among other requirements. Moreover, with respect to transactions, the reporting entity would be required to determine the purpose of specified transactions, monitor designated transactions, keep records of these transactions and report to FINTRAC, relevant transactions originating from or destined for foreign jurisdictions.

2. Foreign Entities

Proposal 5.2 in the consultation paper suggests that foreign entities should be classified in one of three categories:

- foreign entities that would be deemed to be reporting entities in Canada;
- entities incorporated, formed or operating in a foreign jurisdiction, including branches or subsidiaries of the entity; and
- entities not otherwise subject to the Act.

B. What the Witnesses Said and Proposed

1. Countermeasures

In the view of KPMG Forensic, FINTRAC should provide more guidance to reporting entities, including by providing ratings for countries to indicate the degree to which they present a risk of money laundering and/or terrorist financing. The Canadian Real Estate Association asserted that non-face-to-face identification methods should still be allowed under the proposed countermeasures, as relying on face-to-face identification measures would be impractical and would place a burden on reporting entities that would be too high. The Canadian Institute of Chartered Accountants said that the boundaries of the proposed countermeasures are unclear and urged further guidance on the proposed changes to the regulations. Lastly, Mouvement Desjardins supported the proposed changes in relation to countermeasures, as they would provide the federal government with the ability to implement countermeasures against foreign states and foreign entities quickly by providing information directly to reporting entities; however, the government would need to provide support to reporting entities to implement any of these measures.

Other Proposals

A. The Act and Its Regulations, and the Department of Finance's Proposals

1. Suspicious Activities

As indicated in subparagraph 3(a)(iii) of the Act, reporting entities are required to report suspicious transactions. Proposal 6.1 in the consultation paper suggests that reporting entities should be required to report activities that would give rise to suspicion of money laundering or terrorist financing.

2. Submitting Reports to FINTRAC

Subsection 12(5) of the Act requires the CBSA to submit, to FINTRAC, cross-border currency records in relation to monetary instruments having a value of at least $10,000; at present, the CBSA provides both electronic and physical records in this regard. Proposal 6.2 in the consultation paper suggests that the Act should be clarified in order to ensure that both physical and electronic records are provided.

3. Threshold for Non-compliance Disclosures

Subsection 65(1) of the Act stipulates that FINTRAC may disclose information to the police when there "is evidence of a contravention" of Part 1 of the Act. Proposal 6.3 in the consultation paper suggests that FINTRAC should be able to disclose information when disclosure "would be relevant to a contravention" of Part 1 of the Act.

4. Client Credit Files

Paragraphs 14(i) and 30(a) of the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations require reporting entities to retain records of their client credit

files when they do so as part of their normal operations. Proposal 6.4 in the consultation paper suggests that reporting entities should be required to create and retain a client credit file when it enters into a credit arrangement.

B. What the Witnesses Said and Proposed

1. Suspicious Activities

The Canadian Institute of Chartered Accountants argued that the wording of Proposal 6.1 is unclear, as it could be interpreted to include certain accounting activities, such as assurance services, that are currently not covered by the Act. In its view, clarity is needed. The Office of the Privacy Commissioner of Canada stated that this proposal could encompass activities that take place before a financial transaction actually occurs, which would increase the level of over-reporting to FINTRAC by reporting entities.

Technical Amendments

A. The Act and Its Regulations, and the Department of Finance's Proposals

1. Immigration and Refugee Protection Act

Proposal 7.1 in the consultation paper suggests that subsection 36(1.1) and paragraph 55(3)(d) of the Act should refer to section 91 of the Immigration and Refugee Protection Act in order to permit FINTRAC to recognize offences under section 91 for information-sharing purposes.

2. Financing of Terrorist Activities

Proposal 7.2 in the consultation paper suggests that, in order to require FINTRAC to inform the public about its activities in relation to terrorist financing, a reference to the financing of terrorist activities should be added to the Act.

Proposals in the Department of Finance's November 2011 Consultation Paper in Relation to the *Proceeds of Crime (money laundering) and terrorist financing regulations*

A. Introduction of "Business Relationships"

1. Department of Finance Proposal

Proposal 1.1 in the Department of Finance's November 2011 consultation paper suggests that the term "business relationship" should be added to the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations to define the ongoing relationship between a reporting entity and its clients. According to the proposal, the term would mean activities and transactions between a reporting entity and its clients, and reporting entities would be required to maintain a record of their business relationships. This proposal would support the notion that reporting entities must understand the ongoing

relationship that they have with a client, rather than conduct customer due diligence measures only when an account is opened or when a relationship commences.

2. What the Witnesses Said and Proposed

The Canadian Association of Independent Life Brokerage Agencies stated that business relationships of the type envisioned in Proposal 1.1 do not exist between its members and their clients. Moreover, according to it, its members may not have met the client or been privy to the discussions related to the transaction. Similarly, the Canadian Gaming Association argued that the concept of "business relationship," as it is described in the proposal, is not relevant to the gaming sector.

KPMG Forensic argued that the concept of a "business relationship," as described in Proposal 1.1, is unclear, and was concerned that the concept would be applied in unintended areas. It questioned whether the concept of a "business relationship" would apply to all transactions and clients, including low-risk clients and transactions. As an example, KPMG Forensic identified certain types of low-risk transactions, such as the exchange of mortgage-backed securities, that are exempted from the provisions of the anti-money laundering and anti-terrorist financing regime in the United States.

B. Customer Due Diligence in Respect of Suspicious Transactions that Are Otherwise Exempted from Customer Due Diligence Obligations

1. Department of Finance's Proposal

Proposal 2.1 in the Department of Finance's November 2011 consultation paper suggests that reporting entities should be required to determine the identity of clients who conduct transactions that give rise to suspicion of money laundering or terrorist financing; according to the proposal, there should be no exception to this requirement.

2. What the Witnesses Said and Propose

In the opinion of Western Union, adoption of Proposal 2.1 could lead to compliance duplication if both money services businesses and financial institutions are required to fulfil customer due diligence obligations.

C. Customer Due Diligence in Respect of Suspicious Attempted Transactions

1. Department of Finance's Proposal

Proposal 2.2 in the Department of Finance's November 2011 consultation paper suggests that reporting entities should be required to determine the identity of a person who attempts to conduct transactions that would give rise to suspicion of money laundering or terrorist financing.

2. What the Witnesses Said and Proposed

KPMG Forensic argued that the requirement to conduct customer due diligence for transactions and attempted transactions that would give rise to suspicion of money laundering or terrorist financing could contravene existing obligations in FINTRAC guidelines, which require reporting entities not to "tip off" clients about whom they intend to submit a suspicious transaction report.

D. Expand Customer Due Diligence Measures for Beneficial Ownership Information

1. Department of Finance's Proposal

Proposal 3.1 in the Department of Finance's November 2011 consultation paper suggests that reporting entities should be required to take reasonable measures to determine and record the beneficial ownership of their clients that are corporations, entities or trusts.

2. What the Witnesses Said and Proposed

KPMG Forensic noted that the determination of beneficial ownership is difficult and is not always possible. For example, according to it, public documentation may not exist to establish the beneficial ownership of foreign entities. It also felt that Proposal 3.1 is unnecessary, since the "reasonable measures" taken to determine the beneficial ownership of a corporation or other entity generally would involve the reporting entity asking the corporation or other entity to provide the identity of its beneficial owners.

E. Extend Ongoing Monitoring to All Risk Levels of Customers

1. Department of Finance's Proposal

Proposal 3.2 in the Department of Finance's November 2011 consultation paper suggests that reporting entities should be required to perform ongoing monitoring in relation to all clients, rather than only their high-risk clients.

2. What the Witnesses Said and Proposed

KPMG Forensic noted that enhanced customer due diligence measures and ongoing monitoring of clients should focus on the clients that pose the highest risk. It stated that, currently, reporting entities focus their monitoring efforts on the 5% to 10% of their clients who present the greatest risks; adoption of Proposal 3.2 would require reporting entities to focus on all of their clients.

Western Union suggested that adoption of Proposal 3.2 would negatively affect the risk-based approach of Canada's anti-money laundering and anti-terrorist financing regime by imposing costly and burdensome ongoing monitoring obligations on reporting entities. The Canadian Jewellers Association also argued that this and other proposals would impose a high compliance burden on dealers in precious metals and stones; consequently,

in its view, this proposal, among others, should not apply to dealers in precious metals and stones.

F. Conduct Ongoing Monitoring in Respect of Business Relationships

1. Department of Finance's Proposal

Proposal 3.3 in the Department of Finance's November 2011 consultation paper suggests that reporting entities should be required to conduct ongoing monitoring of the entire business relationship that they have with their clients.

2. What the Witnesses Said and Proposed

The Canadian Real Estate Association and Redwood Realty argued that ongoing monitoring of clients should not apply to the real estate sector, where the relationship with the client is generally limited to a single transaction. Similarly, the Canadian Jewellers Association felt that Proposal 3.3 should not apply to dealers in precious metals and stones. Western Union was concerned about the costs, processes and infrastructure required to perform ongoing monitoring.

G. Purpose and Nature of a Business Relationship

1. Department of Finance's Proposal

Proposal 3.4 in the Department of Finance's November 2011 consultation paper suggests that reporting entities should be required to maintain a record of the purpose and nature of their business relationships with their clients.

2. What the Witnesses Said and Proposed

KPMG Forensic suggested that the purpose of Proposal 3.4 is unclear, and argued that the proposal could be unnecessary. Furthermore, it stated that the nature of the relationship between a reporting entity and its client is not always easy to determine. The Canadian Jewellers Association suggested that this proposal should not apply to dealers in precious metals and stones.

H. Clarify and Expand the Application of Enhanced Customer Due Diligence Measures

1. Department of Finance's Proposal

Proposal 3.5 in the Department of Finance's November 2011 consultation paper suggests that reporting entities should be required to undertake enhanced due diligence measures in relation to high-risk clients, including with regard to the identification of clients, the maintenance of up-to-date client identification information and ongoing client monitoring.

2. What the Witnesses Said and Proposed

The Canadian Jewellers Association commented on the introduction of the concept of enhanced customer due diligence and its associated recordkeeping requirements. It noted that, while it understands the Department of Finance's position, the adoption of Proposal 3.5 could impose a significant compliance burden on dealers in precious metals and stones, depending on the manner in which the proposal is drafted in FINTRAC guidelines. As such, it believed that dealers in precious metals and stones should be exempt from this proposed measure.

Other Witness Views and Proposals

A. The Financial Transactions and Reports Analysis Centre of Canada's New Director

FINTRAC's new Director, who assumed office on 15 October 2012, said that demand for FINTRAC's products is high because of both threats to the safety and security of Canadians and FINTRAC's ability to trace monetary flows. He also noted that FINTRAC's contributions to Canada's anti-money laundering and anti-terrorist financing regime are often misconceived and must be considered in the context of the relative contributions of other federal departments and agencies that participate in the regime, and suggested that FINTRAC must constantly adapt and could potentially improve its reporting if the Act's reporting threshold in relation to international electronic funds transfers was reduced. He identified five key areas where action is required in order to strengthen Canada's anti-money laundering and anti-terrorist financing regime: deepen and strengthen FINTRAC's relationships with other federal departments and agencies that participate in the regime; better define risk factors to be monitored and establish risk profiles by sector; use the parliamentary review process to address some of the Act's limitations regarding the type of information that should be received and disclosed by FINTRAC; improve technological capabilities to facilitate electronic manipulation and sharing of information; and improve and constantly update the training of FINTRAC employees in order to ensure an ability to respond to new technologies as well as money laundering and terrorist financing techniques.

B. Funding for Canada's Anti-money Laundering and Anti-terrorist Financing Regime

Capra International Inc. recognized that the efficiency of Canada's anti-money laundering and anti-terrorist financing regime has increased since 2008, but stated that additional improvements are unlikely under current funding arrangements. In particular, it indicated that the regime-based funding directed to the RCMP is not sufficient for it to respond to FINTRAC's proactive disclosures. Moreover, Capra International Inc. noted that there is a discrepancy between funded and unfunded regime partners, and stated that funded partners have a stronger commitment to the regime; FINTRAC is the only fully funded partner. Lastly, it recognized that partially funded regime partners commit their own resources to anti-money laundering and anti-terrorist financing activities.

C. Statistics

Capra International Inc. identified the existence of difficulties in making links between and among reports received by FINTRAC, case disclosures made by FINTRAC to law enforcement agencies, actions taken by law enforcement agencies, charges laid and convictions won by the Public Prosecution Service of Canada.

The RCMP and CSIS indicated that the abilities and efficiency of FINTRAC have improved greatly over time, while the CRA noted that statistics in relation to Canada's anti-money laundering and anti-terrorist financing regime may not capture the criminal investigations that it has undertaken with the information received from FINTRAC.

Capra International Inc. indicated that data collection in relation to Canada's anti-money laundering and anti-terrorist financing regime occurs by each department or agency for its own purposes; consequently, these data are not harmonized. It argued that the federal government should create an interdepartmental working group to address this issue and to coordinate the collection of statistics among regime partners.

The Office of the Privacy Commissioner of Canada argued that better quantitative measures of the performance of Canada's anti-money laundering and anti-terrorist financing regime should be established. Moreover, it said that any amendments to the regime should be supported by data and evidence.

D. Risk-based Approach

American Express, KPMG Forensic, the Canadian Bankers Association, Mouvement Desjardins, Credit Union Central of Canada, MasterCard, Capra International Inc., the Canadian Life and Health Insurance Association Inc., the Canadian Jewellers Association and the Investment Industry Association of Canada either supported a risk-based approach or were concerned about the proposals in the Department of Finance's November and December 2011 consultation papers that would involve a departure from a risk-based approach. Furthermore, they recognized that reporting entities have limited resources and that their compliance efforts are best directed towards high-risk, rather than all, clients and transactions.

KPMG Forensic noted that the best practice globally in relation to an anti-money laundering and anti-terrorist financing regime is a risk-based approach, which is recommended by the Financial Action Task Force on Money Laundering (FATF) and is used in other countries, including the United States and the United Kingdom. It questioned the value of requiring reporting entities to allocate resources to the monitoring of relatively low-risk clients and transactions. Similarly, the Canadian Bankers Association stated that the purpose of using a risk-based approach is not to reduce reporting entity compliance costs, but rather to provide FINTRAC with better information. Further, it argued that reporting entities know their customers best and, as such, are able to determine which customers pose the greatest risks.

Capra International Inc. noted that a risk-based approach is used in government policy. It argued, for example, that since FINTRAC has performed a compliance examination on

only 0.3% of reporting entities to date, it must have used a risk-based approach in determining which reporting entities should be examined. The Canadian Life and Health Insurance Association Inc. supported a risk-based approach as a means of minimizing the compliance burden and of permitting reporting entities to allocate their resources more efficiently. Noting that insurance products are at a relatively low risk for money laundering, it suggested that reporting entities should be permitted to use simplified customer due diligence measures for relatively low-risk products, such as critical illness insurance and term insurance. Similarly, the Canadian Jewellers Association argued that dealers in precious metals and stones should receive a lower risk assessment than other sectors.

The Canadian Life and Health Insurance Association Inc. supported the recommendations in the FATF's October 2009 report, Risk-Based Approach: Guidance for the Life Insurance Sector, which identified different risks by type, including customer, product, service, transaction, delivery channel and country. In arguing for a risk-based approach, the Investment Industry Association of Canada indicated that each firm can establish its own risk-assessment regime based on the guidelines established by FINTRAC, which require reporting entities to assess risk in relation to product, transaction, client and jurisdiction. The Canadian Institute of Chartered Accountants suggested that the government should provide financial institutions with guidance about countries that pose a relatively higher risk of money laundering.

Lastly, the Investment Industry Association of Canada recognized that Canada's anti-money laundering and anti-terrorist financing regime already uses a risk-based approach, and suggested that the proposals in the Department of Finance's consultation papers deviate from that approach.

E. Compliance Burden

Credit Union Central of Canada spoke about the compliance burden imposed on reporting entities that are small businesses, such as credit unions. It noted that the current "one-size-fits-all" regulations mean that it is easier for large institutions to comply because of their size and ability to automate many of the requirements of Canada's anti-money laundering and anti-terrorist financing regime. Consequently, it suggested that the regime's regulatory requirements should be "filtered" through a "small business lens." Jewellers Vigilance Canada Inc. characterized the compliance burden imposed on small business dealers in precious metals and stones as "onerous."

The Canadian Jewellers Association, Jewellers Vigilance Canada Inc. and C.D. Barcados Co. Ltd. emphasized that the precious metals and stones sector consists primarily of small independent businesses that have not necessarily adopted technology, including email, which makes communication among dealers in precious metals and stones difficult. They suggested that the proposed requirements appear to target only low-risk transactions occurring with retail jewellers, rather than high-risk transactions that take place with transient dealers who purchase precious metals and stones from the public, for example. Jewellers Vigilance Canada Inc. argued that the existing compliance burden for small

independent jewellers is very high, as most jewellers do not deal with cash transactions exceeding $10,000 yet are required to maintain a compliance regime.

C.D. Barcados Co. Ltd. mentioned that the Canadian standards for jewellers go beyond FATF recommendations, which have a $15,000 cash transaction threshold, and argued that only those entities that would like to accept more than $15,000 in cash should be subject to the reporting requirements of Canada's anti-money laundering and anti-terrorist financing regime; entities that agree not to accept $15,000 or more in cash should not be subject to the regime. Similarly, the Canadian Jewellers Association suggested that dealers in precious metals and stones, and perhaps other reporting entities, should be exempt from the regime's reporting requirements if they agree not to receive cash exceeding a certain threshold amount. Moreover, it urged an increase in the large cash reporting threshold to $15,000, as recommended in the February 2012 FATF report.

The Investment Funds Institute of Canada supported the Department of Finance's proposals to improve efficiency, minimize the compliance burden and avoid duplication while meeting anti-money laundering objectives.

According to the Canadian Real Estate Association and Redwood Realty, most realtors are entrepreneurs and small businesses, with the majority conducting fewer than 10 transactions per year; consequently, the compliance burden under the Act is high for most realtors.

F. Protection of Personal Information

The Office of the Privacy Commissioner of Canada, which – under the Act – biennially reviews the measures taken by FINTRAC to protect the information that it collects, suggested that FINTRAC receives information beyond its legislative mandate. FINTRAC stated that it takes the privacy requirements of Canada's anti-money laundering and anti-terrorist financing regime seriously, and undertakes efforts to ensure that reporting entities do not send information that it does not want or need. Furthermore, it noted that information that is not needed is either returned to the reporting entity or destroyed.

The RCMP stated that it has compiled a database of information collected from FINTRAC disclosures. Following a review by the Office of the Privacy Commissioner of Canada, the RCMP determined that it did not need this information, which has since been deleted.

The Office of the Privacy Commissioner of Canada commented on what it believes is the gradual weakening of the privacy provisions of the Act since 2000, and noted that FINTRAC's ability to share information with other government entities has been expanded to include the Communications Security Establishment, the RCMP, CSIS, the CRA, the CBSA, and Citizenship and Immigration Canada. However, it also stated that its review of FINTRAC did not identify any inappropriate case disclosures made to law enforcement or other government agencies.

As well, the Office of the Privacy Commissioner of Canada argued that, in the event that FINTRAC's mandate is broadened, FINTRAC should be subject to permanent oversight

with respect to its information-protection measures because of the implications of an expanded mandate for the privacy of Canadians.

From its perspective as a recipient of information from FINTRAC, the CRA stated that the privacy requirements of Canada's anti-money laundering and anti-terrorist financing regime are restrictive. It noted that the decision to include tax evasion as a predicate offence under the regime had not materially changed the quantity of information shared by FINTRAC; therefore, there should not be any concern with respect to the protection of personal information. Moreover, the CRA indicated that it could not freely retrieve FINTRAC's database because of restricted access to the information.

KPMG Forensic was more concerned about the sharing of personal information than it was about privacy, and argued that more – rather than less – information is better for investigators. According to it, the financial intelligence units in other countries seem to have a greater ability to share personal information. It argued that financial institutions should be permitted to share personal information among themselves, with appropriate safeguards to address legitimate privacy concerns arising from that sharing.

The Canadian Bankers Association also suggested that financial institutions should be permitted to share personal information among themselves. It argued that, without an ability to share such information, a financial institution could terminate its relationship with a client believed to be involved in money laundering or terrorist financing, only to have that client obtain those services from another financial institution.

The Canadian Life and Health Insurance Association Inc. noted that the balance between privacy requirements on one hand and the ability to share personal information with law enforcement and FINTRAC on the other hand is problematic. It recognized that the privacy legislation in each jurisdiction impedes the cross-border flow of personal information between financial institutions and financial intelligence units. The Canadian Association of Independent Life Brokerage Agencies suggested that insurance policy contracts should contain a clause that informs the client that FINTRAC will have access to the personal information contained in the contract or application once the contract begins. The Canadian Bar Association argued that strong controls regarding the sharing of personal information are needed in order to protect the privacy of Canadians that is guaranteed in legislation and by the Canadian Charter of Rights and Freedoms.

With respect to data retention, FINTRAC indicated that it is required to retain personal information received from reporting entities for 10 years and must destroy that information after 15 years. The RCMP retains personal information related to proceeds of crime or money laundering investigations for eight years.

G. Access to Information

The Office of the Information Commissioner of Canada questioned both whether the personal information held by FINTRAC should be protected indefinitely and the circumstances under which the interests of the public outweigh the privacy provisions of Canada's anti-money laundering and anti-terrorist financing regime. It noted what it sees

as unnecessary access-to-information exemptions, both in the Act and in the Access to Information Act. In particular, it noted that exemptions exist in section 24 of the Access to Information Act and are listed in Schedule II of that Act for information submitted to and retained by FINTRAC under paragraphs 55(1)(a), (d) and (e) of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act.

According to the Office of the Information Commissioner of Canada, different partners in Canada's anti-money laundering and anti-terrorist financing regime are subject to different access-to-information requirements; some of the documentation held by FINTRAC is subject to the exemption in section 24 of the Access to Information Act, while other types of information held by FINTRAC, and information held by CSIS and the RCMP, are subject to the general access-to-information provisions of the Access to Information Act. It suggested that the section 24 exemption in the Access to Information Act in respect of paragraphs 55(1)(a), (d) and (e) of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act should be removed. According to it, those exemptions could be incorporated directly into the Access to Information Act in order to eliminate duplication and confusion.

From the perspective of the Office of the Information Commissioner of Canada, the balance between the public's right to know on one hand and the protection of personal information on the other hand has been lost, as information referred to in paragraphs 55(1)(a), (d) and (e) of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act is – in effect – permanently protected from public disclosure due to section 24 of the Access to Information Act. It argued that access to personal information should be denied in only specific and limited circumstances.

H. Reporting Entities and Other Sectors to Be Included in the Regime

1. Reporting Entities

a. Insurance Companies

The insurance sector has been recognized by the FATF as a sector that should be covered by anti-money laundering and anti-terrorist financing legislation. The Canadian Association of Independent Life Brokerage Agencies and the Canadian Life and Health Insurance Association Inc. do not disagree with the FATF, and asserted that the insurance sector is at low risk of money laundering or terrorist activity financing, as insurance companies do not accept cash and only certain investment policies offered by insurers could pose a risk of being used to launder money. The Canadian Life and Health Insurance Association Inc. indicated that neither the RCMP nor the Sûreté du Québec could identify any situations in Canada where insurance proceeds were used to launder money.

With regard to the current reporting requirements for the insurance sector, the Canadian Association of Independent Life Brokerage Agencies commented that managing general agents, who are intermediaries between insurance advisors and insurance companies, have the same reporting and client identification obligations as advisors, even though

they do not meet with clients. Regarding managing general agents, it argued that these obligations are difficult and that compliance with them is costly; consequently, in its view, any future expansion of these obligations would be a challenge for managing general agents.

b. Casinos

The Ontario Lottery and Gaming Corporation and the Canadian Gaming Association highlighted that casinos and gaming in Canada are regulated by the provinces/territories as well as by FINTRAC. The Ontario Lottery and Gaming Corporation noted that, although casinos in Canada may be operated by private companies, they are owned and regulated by provincial/territorial Crown agencies. Similarly to FINTRAC, provincial gaming legislation also regulates client identification and transactions in casinos; for example, in Ontario, casinos are required to track cash transactions that exceed $2,500.

In the view of the Canadian Gaming Association, the federal government and FINTRAC should recognize that money laundering in casinos can occur only in the event of a payout and that casinos must report to FINTRAC whenever there are payouts of $10,000 or more.

c. Lawyers and Law Firms

The Department of Finance indicated that lawyers are involved in a variety of financial transactions on behalf of their clients; as a result, there is a risk of money laundering in the legal profession. In particular, according to the Department, transactions that take place through lawyers' trust accounts as well as trust accounts opened by a lawyer for a specific client could hide the identity of clients and their associated financial transactions.

The Federation of Law Societies of Canada explained that provincial/territorial law societies have implemented rules to cover any perceived gaps in Canada's anti-money laundering and anti-terrorist financing regime, in particular with a "no cash" rule that prevents lawyers from accepting cash exceeding $7,500 for financial transactions and other rules in relation to client identification. It indicated that the federal government has not found the client identification rules to be sufficient to combat money laundering in the legal profession, and requires lawyers to submit reports to FINTRAC for financial transactions.

The Federation of Law Societies of Canada and the Canadian Bar Association described how the Act has been applied to the legal profession since obligations for lawyers and law firms were enacted in 2001. They indicated that the 2001 provisions that required lawyers to submit suspicious transaction reports were repealed by the federal government in 2006 and that, since 2008, lawyers and law firms have been required to verify client identification as well as to keep records of when they receive or pay funds exceeding $3,000 on behalf of another person or entity, or if the transaction occurs through a trust fund. They noted, however, that these provisions are currently inoperative due to ongoing litigation examining whether the Act's obligations contravene solicitor-client privilege,

and highlighted the September 2011 British Columbia Supreme Court decision that the Act infringes on the solicitor-client relationship; in the Court's view, the rules set out by provincial/territorial law societies are sufficient for client identification and verification purposes. Finally, they commented that, as the federal Crown has appealed this decision, a temporary injunction will continue to exempt lawyers and law firms from the application of the Act and its regulations.

In response to concerns that lawyers and law firms may be targets for money laundering, the Canadian Bar Association noted that lawyers are subject to stringent codes of conduct administered by the law societies and that they are subject to the Criminal Code in the same manner as all other Canadian citizens. It also commented that trust accounts are audited regularly by law societies and that client identification rules require lawyers to verify a client's identity for all non-face-to-face transactions, including international transactions through trust accounts. The Federation of Law Societies and the Canadian Bar Association shared their view that regulation of money laundering in the legal profession should be administered by the law societies rather than by FINTRAC.

2. Other Sectors to Be Included in the Regime

Amex Bank of Canada argued that businesses that accept cash and have less oversight pose a particular risk for money laundering. MasterCard identified cash and cross-border movements of cash as a means by which money is laundered. Similarly, the Canadian Institute of Chartered Accountants stated that "bulk cash" smuggling to foreign jurisdictions with fewer controls was a method of laundering money. KPMG Forensic noted that it is not unusual for the police to discover large amounts of cash during a raid. As well, the Canadian Institute of Chartered Accountants identified trade-based money laundering, which results from the sale or purchase of imports and exports at artificially inflated or deflated prices, as another approach taken by money launderers.

The Canadian Bankers Association stated that, in its view, all sectors that should be included in Canada's anti-money laundering and anti-terrorist financing regime are covered at this time. However, it also noted that it is possible to purchase a new car, such as a Maserati, with $150,000 in cash.

The Canadian Jewellers Association and the Canadian Institute of Chartered Accountants identified retailers that accept large amounts of cash, such as vendors of electronics, cars and boats, as businesses that are exempt from reporting obligations in Canada. The Canadian Jewellers Association, C.D. Barcados Co. Ltd. and Jewellers Vigilance Canada Inc. indicated that auction houses, which can accept cash as payment and are also excluded from Canada's anti-money laundering and anti-terrorist financing regime, should be covered. Jewellers Vigilance Canada Inc. commented that, similarly, art dealers are not covered. The Canadian Jewellers Association argued that all sectors and industries should be subject to reporting requirements.

C.D. Barcados Co. Ltd. noted that while dealers in precious metals and stones are covered by Canada's anti-money laundering and anti-terrorist financing regime, the "we buy your gold" businesses are difficult to monitor because they may only be open

temporarily and may not have a fixed address. The Canadian Jewellers Association requested that this type of business be covered by the regulations to the Act. The Canadian Real Estate Association and the Department of Finance identified private real estate sales as a potential area where large cash transactions could occur without any reporting obligations. The Department recognized, however, that a deposit at a financial institution following a private real estate transaction would likely result in a report to FINTRAC.

Imperial Tobacco asked that an in-depth study be conducted on contraband tobacco products and their links to organized crime, money laundering and terrorist financing. In particular, it requested that the government take measures to ensure the integrity of the Canada–United States border in relation to the smuggling of contraband tobacco, impose mandatory jail sentences for repeat offenders in relation to contraband tobacco, create an RCMP anti-contraband tobacco force, enforce the law equally for all tobacco manufacturers and retailers, not raise tobacco taxes, deploy a contraband tobacco public awareness campaign and create a joint Quebec-Ontario-federal government working group to coordinate efforts in the fight against illicit tobacco sales.

The Canadian Bank Machine Association indicated that it does not support the House of Commons Standing Committee on Justice and Human Rights' recommendation, contained in its report The State of Organized Crime, that non-bank automated bank machine (ABM) operators be required to report to FINTRAC in respect of cash transactions of $7,500 or more. The Canadian Bank Machine Association noted that, while non-bank ABM operators do not submit reports to FINTRAC, they do follow Interac's anti-money laundering regulations that set out criteria for potential purchasers of ABMs and that require owners of ABMs to deposit funds from ABMs into Canadian bank accounts. Furthermore, the Canadian Bank Machine Association emphasized that non-bank ABM operators do not have control over withdrawals from ABMs and thus do not play a role in preventing criminal activity that may be linked to cash withdrawals from ABMs.

The Canadian Automobile Dealers Association stated that large cash transactions relating to the purchase of new vehicles are rare and that more than 90% of such purchases are financed. It also indicated that 85% of its members report that cash transactions exceeding $10,000 represent less than 2% of their total sales. According to the Canadian Automobile Dealers Association, when a dealer deposits more than $10,000 in cash at a financial institution in relation to a single transaction, the dealer must provide information about the purchaser of the vehicle. Furthermore, it noted that – in order to meet requirements for licencing, warranty registration and vehicle insurance – dealers collect information about the driver of the vehicle, including his/her licence number, address, social insurance number and insurance company. It suggested that it would be difficult to launder large amounts of cash through automobile dealerships without detection, and speculated that home construction and renovations as well as unregulated used car brokers are more likely targets for money launderers. It observed that its members are greatly affected by vehicle theft by criminals involved in organized crime, with vehicle thefts valued at up to $1 billion annually for the resale of parts and exportation. It also said that any new regulations in relation to combating money

laundering should be consistent with the goals of the federal Red Tape Reduction Commission and noted that its members are willing to work with the federal government regarding proposed reporting requirements.

The Ontario Motor Vehicle Industry Council (OMVIC) stated that automotive dealerships facilitate money laundering with relative ease and, therefore, are highly desired by organized crime. Although the OMVIC agreed that large cash transactions are rare in the automotive sector, it argued that automobiles often act as a high-value alternative to cash, and are exchanged in mass quantities between automobile dealers and across borders as a means of payment for contraband items, such as drugs. It also observed that, in some cases, the automobiles may not exist; the criminals may fabricate documents, such as false invoices bearing serial numbers and forged identification of individuals, as "proof" of a large automotive purchase or sale as a means to transfer funds. The OMVIC also indicated that a significant portion of its resources are spent in combatting money laundering in the automotive dealership sector.

Heffel Fine Art Auctioneers stated that it is extremely rare for a piece of art to be purchased with cash at an auction house; thus, it does not believe that auction houses are targets for money launderers. That said, it suggested that someone buying a piece of art from a private dealer with cash who then sells it through an auction house could be laundering money. It also noted that very few art dealers in the secondary market sell art that is valued at more than $10,000 per piece; nevertheless, there are more opportunities for money laundering with art dealers than with auction houses. It also said that, as an alternative to cash, the transportation of pieces of art across borders to be resold could involve money laundering. It remarked that, in recent years, Heffel Fine Art Auctioneers' auctions – which have had annual sales valued at between $30 million and $50 million – have involved less than $10,000 in cash. It commented on the suggestion by dealers in precious metals and stones that auctions provide opportunities for money laundering due the anonymity of buyers and sellers, stating that while the identities of buyers and sellers are not made publicly available, auction houses both confirm the identity of sellers and ask for identification and banking information from buyers participating in live or online auctions. Finally, it indicated that most art in Canada is purchased by buyers directly, rather than through agents.

Boating Ontario stated that cash transactions for boat purchases represent less than 2% of total sales, that 65% to 75% of such purchases are financed, and that its members are required to provide financial institutions with information about the identity of purchasers when cash deposits exceeding $10,000 for a single transaction are made. It also indicated that its members confirm the ownership of boats and trailers for the secondary market sales of boats. Moreover, Boating Ontario noted that sales of recreational boats have decreased since the onset of the global financial and economic crisis, and that the boating manufacturing sector is being negatively affected by the relative value of the Canadian dollar. That said, its members are willing to work with the federal government regarding potential reporting requirements related to Canada's anti-money laundering and anti-terrorist financing regime.

I. Public Education

Capra International Inc. argued that the Department of Finance should conduct a survey to determine the level of public awareness about money laundering, terrorist financing and Canada's anti-money laundering and anti-terrorist financing regime. The Canadian Jewellers Association urged the creation of marketing materials to explain to clients the need for customer identification and other information requirements. It also requested that FINTRAC's money laundering typologies specifically address the laundering of money in the precious metals and stones sector, and that FINTRAC provide materials describing a sample compliance regime for small, medium and large dealers in precious metals and stones.

J. Amendments to the Act and Its Regulations

The Canadian Life and Health Insurance Association Inc. supported regular updates to the legislation that establishes Canada's anti-money laundering and anti-terrorist financing regime, especially since FATF recommendations were released in February 2012.

Recognizing that, in January 2012, FINTRAC began a compliance assessment in relation to dealers in precious metals and stones, the Canadian Jewellers Association felt that amendments to Canada's anti-money laundering and anti-terrorist financing regime that would affect these dealers should not be made until the assessment is complete.

In the view of the Canadian Bar Association, amendments to the Act and its regulations should be drafted with precision, as numerous reporting entities are not confident that they understand their obligations. It also felt that imprecise legislation can lead to an arbitrary interpretation of the law.

K. Deterrence

According to the Department of Finance, the existence of an anti-money laundering and anti-terrorist financing regime in Canada is a strong deterrent to such activities and increases confidence in Canada's financial system. Moreover, it indicated that the regime's compliance obligations require financial institutions to implement systems that combat fraud and manage risk.

The Canadian Bankers Association argued that the effectiveness of Canada's anti-money laundering and anti-terrorist financing regime should be measured by the degree of difficulty encountered in, and the costs associated with, laundering money, recognizing that criminals will find a way to launder money.

Capra International Inc. noted that while immediate outcomes can be measured, deterrence effects must be inferred. The Office of the Privacy Commissioner of Canada was critical of the government's view that Canada's anti-money laundering and anti-terrorist financing regime is working and is a deterrent to money laundering. It questioned whether more sophisticated methods, such as comparative and quantitative analysis, could be used to measure deterrence.

L. Terrorism and Terrorist Lists

The Office of the Privacy Commissioner of Canada stated that, since the beginning of Canada's anti-money laundering and anti-terrorist financing regime, one person has received a six-month sentence for participating in the financing of the Tamil Tigers.

Public Safety Canada indicated that Canada has three complementary terrorist listing regimes implemented under the United Nations Resolutions on the Suppression of Terrorism, the United Nations Al-Qaida and Taliban Regulations, and Canada's Criminal Code, in accordance with which Public Safety Canada has responsibility for the terrorist list pursuant to section 83.06 of the Code; there are currently 44 persons or entities on that list. The Department of Foreign Affairs and International Trade takes the lead role with respect to lists and regulations under the United Nations Act, while the Office of the Superintendent of Financial Institutions notifies financial institutions of the sanctions imposed on entities.

According to Public Safety Canada, when a person or entity is placed on a terrorist list, financial institutions are required to freeze the assets of that person or entity, and persons in Canada and Canadians abroad are prohibited from knowingly dealing with the assets of that person or entity. Furthermore, Public Safety Canada indicated that persons in Canada and Canadians abroad are required to notify CSIS or the RCMP of property in their possession that belongs to a terrorist group, and that reporting entities must submit terrorist property reports to FINTRAC.

With respect to anti-terrorist financing, the Canadian Life and Health Insurance Association Inc. argued that a single government entity should maintain a useful, up-to-date and cost-efficient consolidated list of terrorist groups.

M. Freezing of Assets and Property

According to Public Safety Canada, in Canada, there is currently about $200,000 in frozen assets belonging to persons or entities on a terrorist list.

According to the Department of Foreign Affairs and International Trade, on 23 March 2011, the Governor in Council introduced regulations under the Freezing Assets of Corrupt Foreign Officials Act to freeze the assets and property of politically exposed foreign persons at the request of the Government of Egypt and the Government of Tunisia. It indicated that, to date, 268 persons – 123 in respect of Tunisia and 145 in respect of Egypt – have been listed in the regulations and that, in total, the Government of Canada has frozen residential property valued at $2.55 million and accounts containing $122,000. As well, the Department indicated that the assets of persons from Libya have also been frozen based on decisions made by the United Nations Security Council pursuant to the United Nations Act; at one time, more than $2 billion in assets belonging to persons and entities from Libya were frozen.

N. Disclosures, Criminal Investigations and Prosecutions

With respect to law enforcement agencies, KPMG Forensic noted that, according to Capra International Inc.'s 10-year review of Canada's anti-money laundering and anti-terrorist financing regime, about 80% of the case disclosures sent by FINTRAC to the RCMP were associated with ongoing cases, while proactive case disclosures made up 20% of all FINTRAC disclosures. It also indicated that the RCMP may not have the resources to investigate proactive case disclosures. KPMG Forensic recognized that there are many intangible benefits to the current regime, as FINTRAC disclosures can assist open investigations by providing additional information about suspects and their activities as well as by identifying as-yet-unknown associates. To address the problem of allegedly inadequate law enforcement resources, KPMG Forensic suggested that the federal government should provide additional resources to the RCMP's Integrated Proceeds of Crime units to enable the proactive disclosures received from FINTRAC to be addressed.

The RCMP stated that, in 2010, it had initiated investigations based on 93 proactive disclosures from FINTRAC. Of those 93 investigations, 69 have been concluded, 23 are still under investigation, and no investigation has resulted in charges being laid.

The Department of Finance warned against using prosecutions to measure the success of Canada's anti-money laundering and anti-terrorist financing regime. In particular, it stated that there is not a one-for-one link between FINTRAC disclosures to law enforcement agencies and successful prosecutions, and noted that information may also be associated with plea bargains and other beneficial results, including the deterrence of money laundering.

The Public Prosecution Service of Canada explained that it does not gather evidence, but it receives evidence that it uses to determine if the evidence is sufficient to lay charges.

As well, the Public Prosecution Service of Canada provided data on charges laid and their outcomes – including convictions and guilty pleas – associated with proceeds of crime, money laundering and terrorist financing. Over the 2005-2006 to 2009-2010 fiscal years, 425 money laundering charges were laid, with 11 convictions and 77 guilty pleas; as well, 32,149 charges of possession of property obtained through criminal activity were laid, with 385 convictions and 2,519 guilty pleas. Over that period, five terrorist financing charges were laid, with one conviction. In the 2010-2011 fiscal year, 46 money laundering charges were laid, with 4 convictions and 8 guilty pleas; 6,733 charges of possession of property obtained through criminal activity were laid, with 61 convictions and 578 guilty pleas. Finally, in that fiscal year, one terrorist financing charge was laid, with one guilty plea.

It recognized that it has no information about the role played by FINTRAC disclosures in criminal investigations or whether those investigations result in the laying of charges or other outcomes.

O. Charities

According to Public Safety Canada, it and its partner organizations work with the CRA to prevent abuse of the charity registration system. The CRA's Charities Directorate indicated that it reviews the list of registered charitable organizations to ensure that registered charities are not a source of terrorist financing.

According to the CRA, in 2006, amendments to the Act permitted FINTRAC to share information with the CRA regarding charities involved in terrorist financing. It also indicated that equivalent amendments were made to the Income Tax Act to permit the CRA to share information with FINTRAC and other government entities in relation to suspected terrorist financing.

P. Tax Evasion

According to the Department of Finance, with the July 2010 addition of tax evasion to the list of predicate offences under Canada's anti-money laundering and anti-terrorist financing regime, and subject to certain initial tests such as suspicion of money laundering, FINTRAC may disclose information to the CRA on suspected tax evasion. In discussing the 2010 changes, the Office of the Privacy Commissioner of Canada stated that it understood the rationale for these changes to the Act, since money laundering and tax evasion offences are often related.

According to the CRA, it received 147 proactive disclosures from FINTRAC in 2011; these disclosures resulted in 115 audits and $27 million in reassessed federal taxes. Moreover, the CRA commented that, over the last five years, it has received 800 proactive disclosures from FINTRAC, which has resulted in 500 audits and about $81 million in reassessed federal taxes. While these audits are civil assessments, the CRA noted that it also engages in criminal investigations for more serious matters; in any given year, it conducts approximately 150 criminal investigations. Moreover, the CRA said that, since the changes to Canada's anti-money laundering and anti-terrorist financing regime in July 2010, it has sent a voluntary information record to FINTRAC with each of those investigations. Finally, the CRA commented that, in 2011, charges were laid against 204 taxpayers for offences under the Criminal Code.

Q. International Comparison

According to the United Kingdom Financial Intelligence Unit (UKFIU), which is part of the Serious Organized Crime Agency and reports to the Home Office, it – like FINTRAC – is a member of the FATF and of the Egmont Group; as well, it must also meet the obligations set out in European Union Money Laundering Directives.

The UKFIU noted that its primary role is to manage suspicious activity reports (SARs) submitted by reporting entities; approximately 250,000 SARs were submitted to the UKFIU in 2011. It also indicated that it receives consent reports, which allow businesses to avail themselves of a defence against money laundering charges by seeking the consent of the UKFIU to undertake an activity that could be illegal and subject to criminal charges. Regarding the collection of information, the UKFIU highlighted its use

of a risk-based approach rather than an approach that involves threshold-based transactions.

Moreover, according to the UKFIU, SARS are stored on the ELMER database – which is accessible by law enforcement and authorized government agencies – for a period of six years, after which they are deleted. The UKFIU admitted that it is difficult to evaluate the success of the United Kingdom's anti-money laundering and anti-terrorist financing regime, as statistics that pertain to prosecutions or the amount of money seized by law enforcement agencies are not correlated with information obtained from the ELMER database; however, any money that is seized is given to law enforcement agencies and, consequently, those involved in the regime have an incentive to act in a manner that leads to success in the fight against money laundering and terrorist financing.

Finally, the UKFIU indicated that reporting entities want more feedback with regard to SARs and advancements in the technology that support the United Kingdom's anti-money laundering and anti-terrorist financing regime.

APPENDIX C – CAPRA INTERNATIONAL INC. RECOMMENDATIONS

The [Anti-Money Laundering and Anti-Terrorist Financing] Regime should be continued as a horizontal initiative with at least the same level of resourcing provided as currently exists. In addition, [the Department of] Finance, in consultation with the Regime partners, should conduct a review and provide recommendations regarding the funding allocations for the Regime partners that include a detailed assessment of the appropriateness and use by the partners of the current funding levels relative to their responsibilities for anti-money laundering and anti-terrorist financing (AML/ATF) activities.

[The Department of] Finance should lead an Interdepartmental Working Group with representation from Regime partners to determine future steps for continuing to improve the Regime's compliance with international commitments and to examine the following key issues:

a. regime-related legislation and regulations (Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and related enabling legislation of Regime partners) that may be constraining information sharing with the aim of identifying possible solutions that may require either legislative/regulatory amendments or operational changes to remove barriers to effective and efficient Regime operations;

b. concerns raised by reporting entities, as cited in this evaluation report, with a view to addressing their issues, as appropriate, regarding how requirements under the PCMLTFA are being complied with;

c. the inconsistencies identified in the Regime performance data and statistics to facilitate the Regime's ability to accurately report on its achievement; and

d. whether updates are required to the Regime's management and accountability framework and Logic Model, particularly in relation to the Regime roles and responsibilities of [the Office of the Superintendent of Financial Institutions], [the Department of] Justice (as it now exists after the creation of the Public Prosecution Service of Canada), and the Royal Canadian Mounted Police – Money Laundering unit, and in relation to the current expected outcomes that do not include reference to measures of the number of Money Laundering/Terrorist Financing charges laid and the number of convictions obtained.

[The Department of] Finance should consider conducting a public opinion survey to determine the level of public awareness of the Money Laundering/Terrorist Financing threat and of the AML/ATF actions of the Regime. This survey would provide a baseline of information to be used in future evaluations, and to assess the extent of public acceptance of the Regime.

APPENDIX D – WITNESSES

Organization	Name, Title	Date of Appearance	Committee Issue No.
Department of Finance	Allan Prochazka, Senior Analyst, Financial Sector Division	2012-02-02	9
Department of Finance	Diane Lafleur, General Director, Financial Sector Policy Branch	2012-02-02	9
Department of Finance	Annik Bordeleau, Senior Project Leader, Financial Crimes - Domestic, Financial Sector Division	2012-02-02	9
Department of Finance	Leah Anderson, Director, Financial Sector Division	2012-02-02	9
Canada Border Services Agency	Maria Romeo, Director, Emerging Border Programs Division, Border Programs Directorate, Programs Branch	2012-02-08	10
Canadian Security Intelligence Service	Allison Merrick, Director General DDEX (Discovery and Data Exploitation)	2012-02-08	10
Public Safety Canada	Michael MacDonald, Director General, National Security Operations Directorate	2012-02-08	10
Department of Public Safety	Yves Legeurrier, Director, Serious and Organized Crime Division	2012-02-08	10
Royal Canadian Mounted Police	Superintendent Jeff Adam, Proceeds of Crime Director	2012-02-08	10
Financial Transactions and Reports Analysis Centre of Canada	Barry MacKillop, Deputy Director, Financial Analysis and Disclosure	2012-02-09	10
Financial Transactions and Reports Analysis Centre of Canada	Chantal Jalbert, Assistant Director, Regional Operations and Compliance	2012-02-09	10
Financial Transactions and Reports Analysis Centre of Canada	Paul Dubrule, General Counsel	2012-02-09	10

Organization	Name, Title	Date of Appearance	Committee Issue No.
Financial Transactions and Reports Analysis Centre of Canada	Darlene Boileau, Deputy Director, Strategic Policy and Public Affairs	2012-02-09	10
Office of the Superintendent of Financial Institutions Canada	Alain Prévost, General Counsel in the Legal Services Division	2012-02-15	11
Office of the Superintendent of Financial Institutions Canada	Nicolas Burbidge, Senior Director of the Anti-Money Laundering and Compliance Division	2012-02-15	11
Public Prosecution Service of Canada	Simon William, Senior Counsel	2012-02-16	11
Office of the Information Commissioner of Canada	Suzanne Legault, Commissioner	2012-02-16	11
Public Prosecution Service of Canada	George Dolhai, Acting Deputy Director of Public Prosecutions and Senior General Counsel	2012-02-16	11
Canada Revenue Agency	Claude St-Pierre, Director General, Enforcement and Disclosures Directorate, Compliance Programs Branch	2012-02-29	12
Canada Revenue Agency	Alison Rutherford, Acting Director, Review and Analysis Division, Charities Directorate, Legislative Policy and Regulatory Affairs Branch	2012-02-29	12
Canada Revenue Agency	Stephanie Henderson, Manager, Special Enforcement Program, Enforcement and Disclosures Directorate, Compliance Programs Branch	2012-02-29	12
Canada Revenue Agency	Cathy Hawara, Director General, Charities Directorate, Legislative Policy and Regulatory Affairs Branch	2012-02-29	12

Organization	Name, Title	Date of Appearance	Committee Issue No.
Foreign Affairs and International Trade Canada	Sabine Nolke, Director General, Non-Proliferation and Security Threat Reduction	2012-02-29	12
Foreign Affairs and International Trade Canada	Michael Walma, Director, International Crime and Terrorism Division	2012-02-29	12
Office of the Privacy Commissioner of Canada	Jennifer Stoddart, Privacy Commissioner	2012-03-01	12
Office of the Privacy Commissioner of Canada	Mike Fagan, Manager, Audit and Review	2012-03-01	12
Office of the Privacy Commissioner of Canada	Carman Baggaley, Senior International Research and Policy Analyst	2012-03-01	12
KPMG Forensic	Susana Johnson, Head, Anti-Money Laundering Services	2012-03-07	13
Canadian Bankers Association	Bill Randle, Assistant General Counsel	2012-03-08	13
Credit Union Central of Canada	Marc-André Pigeon, Director, Financial Services Sector	2012-03-08	13
Credit Union Central of Canada	Evelyne Olivier, Internal Audit and Administration Officer, Winnipeg Police Credit Union	2012-03-08	13
Canadian Bankers Association	Stephen Harvey, Vice President, Chief Anti-money Laundering Officer, CIBC	2012-03-08	13
Mouvement Desjardins	Karine Bolduc, Certified Management Accountant and Director, Compliance and Anti-Money Laundering	2012-03-08	13
Capra International Inc.	Waldo Rochow, Evaluator	2012-03-14	14
Capra International Inc.	Gunter Rochow, President	2012-03-14	14
Capra International Inc.	Rick Reynolds, Evaluator	2012-03-14	14
Capra International Inc.	Michel Laurendeau, Senior Evaluator	2012-03-14	14

Organization	Name, Title	Date of Appearance	Committee Issue No.
Capra International Inc.	Ralph Kellett, Chief, Evaluation Practice	2012-03-14	14
Capra International Inc.	Eric Culley, Evaluator	2012-03-14	14
Canadian Life and Health Insurance Association Inc.	Frank Swedlove, President	2012-03-15	14
Ontario Lottery and Gaming Corporation	Derek Ramm, Director, Anti-Money Laundering Programs, Legal, Regulatory and Compliance	2012-03-15	14
Canadian Gaming Association	Paul Burns, Vice President	2012-03-15	14
Canadian Association of Independent Life Brokerage Agencies	Allan Bulloch, Chair, Legislative Committee	2012-03-15	14
Canadian Life and Health Insurance Association Inc.	Jean-Pierre Bernier, Special Advisor to the President, Risk Management	2012-03-15	14
Canadian Jewellers Association	David Ritter, President and CEO	2012-03-28	15
Jewellers Vigilance Canada Inc.	Phyllis Richard, Executive Director	2012-03-28	15
The Investment Funds Institute of Canada	Ralf Hensel, General Counsel, Corporate Secretary, Director, Policy - Manager Issues	2012-03-28	15
C.D. Barcados Co. Ltd.	Alexander Barcados, President	2012-03-28	15
Investment Industry Association of Canada	Amanda L. Archibald, Vice-President, Compliance and AROP, Raymond James Ltd.	2012-03-28	15
Investment Industry Association of Canada	Michelle Alexander, Director, Policy and Corporate Secretary	2012-03-28	15
Canadian Real Estate Association	Gary Simonsen, Chief Executive Officer	2012-03-29	15
Canadian Real Estate Association	David Salvatore, Director, External Relations	2012-03-29	15

Organization	Name, Title	Date of Appearance	Committee Issue No.
Western Union Financial Services (Canada), Inc.	Derek McMillan, Director, Compliance (International)	2012-03-29	15
MasterCard Canada Inc.	Richard McLaughlin, Senior Vice-President, Global Products and Solutions	2012-03-29	15
Canadian Institute of Chartered Accountants	Matthew McGuire, Chair, Anti-Money Laundering Committee	2012-03-29	15
Amex Bank of Canada	Wilf Gutzin, Vice-President and Senior Counsel	2012-03-29	15
Amex Bank of Canada	Scott Driscoll, Vice President, Chief Compliance Officer and Chief Anti-Money Laundering Officer	2012-03-29	15
Canada Regional Counsel, MasterCard Canada Inc.	Andrea Cotroneo, Vice-President	2012-03-29	15
Federation of Law Societies of Canada	Frederica Wilson, Senior Director, Regulatory and Public Affairs	2012-04-04	16
Canadian Bar Association	Ronald A. Skolrood, Member, CBA Proceeds of Crime Working Group	2012-04-04	16
Canadian Bar Association	Gaylene Schellenberg, Lawyer, Legislation and Law Reform	2012-04-04	16
Federation of Law Societies of Canada	John J.L. Hunter, Q.C., President	2012-04-04	16
Serious Organised Crime Agency	Alan Hislop, Head, United Kingdom Financial Intelligence Unit	2012-04-26	16
Imperial Tobacco Canada	Pénéla Guy, Director, Regulatory and Government Affairs	2012-05-02	17
Canadian Bank Machine Association	Chris Chandler, President	2012-10-17	24
Boating Ontario Association	Jeff Wilcox, Governor	2012-11-29	26

Organization	Name, Title	Date of Appearance	Committee Issue No.
Canadian Automobile Dealers Association	Richard C. Gauthier, President and Chief Executive Officer	2012-11-29	26
Heffel Fine Art Auctioneers	Andrew Gibbs, Ottawa Representative	2012-11-29	26
Financial Transactions and Reports Analysis Centre of Canada	Gérald Cossette, Director	2012-12-06	28

APPENDIX E – OTHER BRIEFS SUBMITTED TO THE COMMITTEE

ORGANIZATION	NAME
Art Dealers Association	Elizabeth Edwards
Department of the Treasury Financial Crimes Enforcement Network, United States	Bess J. Michael
Ontario Motor Vehicle Industry Council	Carey Smith
Anti-Money Laundering and Counter Terrorism Financing	Denis Meunier

Appendix B:

Canada, Department of Finance, *Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada 2015* (Ottawa: Department of Finance, 2015).

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

2015

Department of Finance Canada
Ministère des Finances Canada

Table of Contents

Foreword by the Minister of Finance 5

Executive Summary 7

Introduction 9

Chapter 1: Risk Mitigation 11

Chapter 2: Overview of the Methodology to Assess Inherent Money Laundering and Terrorist Financing Risks in Canada 15

Chapter 3: Assessment of Money Laundering Threats 18

Chapter 4: Assessment of Terrorist Financing Threats 27

Chapter 5: Assessment of Inherent Money Laundering and Terrorist Financing Vulnerabilities 31

Chapter 6: Results of the Assessment of Inherent Money Laundering and Terrorist Financing Risks 42

Next Steps 66

Annex: Key Consequences of Money Laundering and Terrorist Financing 67

Glossary 68

List of Key Acronyms and Abbreviations 71

Foreword by the Minister of Finance

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

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

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

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

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

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

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

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

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

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

And we continue to strengthen our own link within it.

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

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

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

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

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

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

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

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

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

Executive Summary

Canada has a robust and comprehensive anti-money laundering and anti-terrorist financing (AML/ATF) regime, which promotes the integrity of the financial system and the safety and security of Canadians. It supports combating transnational organized crime and is a key element of Canada's counter-terrorism strategy.

The Government of Canada has conducted an assessment to identify inherent money laundering and terrorist financing (ML/TF) risks in Canada. This report also includes a process to update this assessment over time. The report provides an overview of the risks of money laundering and terrorist financing before the application of any mitigation measures. Those measures include a range of legislative, regulatory and operational actions that prevent, detect and disrupt money laundering and terrorist financing.

Canada has a comprehensive AML/ATF regime that provides a coordinated approach to mitigating the inherent risks identified in this assessment and combating money laundering and terrorist financing more broadly. The AML/ATF regime is operated by 11 federal regime partners, eight of which receive dedicated funding totalling approximately $70 million annually.[1] The inherent risks identified are being addressed through a strong regime that focuses on policy coordination, both domestically and internationally; the prevention and detection of money laundering and terrorist financing in Canada; disruption activities, including investigation, prosecution and the seizure of illicit assets; and the implementation of measures to ensure the ongoing improvement of the AML/ATF regime.

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

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

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

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

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

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

The inherent ML/TF vulnerabilities are presented for 27 economic sectors and financial products. The assessment indicates that there are many sectors and products that are highly vulnerable to money laundering and terrorist financing. Of the assessed areas, domestic banks, corporations (especially private for-profit corporations), certain types of money services businesses and express trusts were rated the most vulnerable, or very high. The vulnerability was rated high for 16 sectors and products, medium for five sectors and products and low for one sector. Many of the sectors and products are highly accessible to individuals in Canada and internationally and are associated with a high volume, velocity and frequency of transactions. Many conduct a significant amount of transactional business with high-risk clients and are exposed to high-risk jurisdictions that have weak AML/ATF regimes and significant ML/TF threats. There are also opportunities in many sectors to undertake transactions with varying degrees of anonymity and to structure transactions in a complex manner.

By connecting the threats with the inherently vulnerable sectors or products, the assessment revealed that a variety of them are exposed to very high inherent ML risks involving threat actors (e.g., OCGs and third-party money launderers) laundering illicit proceeds generated from 10 main types of profit-oriented crimes. The assessment also identified five very high inherent TF risk scenarios that involve five different sectors that have been assessed to be very highly vulnerable to terrorist financing, combined with one high TF threat group of actors.

This risk assessment is an analysis of Canada's current situation and represents a key step forward in providing the basis for the AML/ATF regime to promote a greater shared understanding of inherent ML/TF risks in Canada on an ongoing basis. The assessment will help to continue to enhance Canada's AML/ATF regime, further strengthening the comprehensive approach it already takes to risk mitigation and control domestically, including with the private sector and with international partners.

Introduction

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

The Government of Canada is committed to combating money laundering and terrorist financing, while respecting the Constitutional division of powers, the *Canadian Charter of Rights and Freedoms* and the privacy rights of Canadians. The Government of Canada has put in place a robust and comprehensive anti-money laundering and anti-terrorist financing (AML/ATF) regime. The regime is operated by 11 federal departments and agencies, each responsible for certain elements of it, as well as other departments and agencies that support the regime's efforts, coordinated by the Department of Finance Canada.[2] Provincial and municipal law enforcement bodies and provincial financial sector and other regulators are also involved in combating these illicit activities. Within the private sector, there are almost 31,000 Canadian financial institutions and designated non-financial businesses and professions (DNFBPs)[3] with reporting obligations under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA), known as reporting entities, that play a critical frontline role in efforts to prevent and detect money laundering and terrorist financing.

The regime's understanding of ML/TF risks plays a key role in its ability to effectively combat these illicit activities. That understanding helps to support the policy-making process to more effectively address vulnerabilities and other potential gaps in the regime. It helps to inform operational decisions about priority setting and resource allocation to combat threats and to focus on those that have the greatest economic, social and political consequences. It also plays a central role in how the private sector applies its risk-based approaches and mitigates its risks. Overall, the regime's understanding of risks helps to ensure that it is focused on adequately mitigating the risks of greatest concern to Canada.

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

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

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

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

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

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

Chapter 1: Risk Mitigation

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

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

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

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

(i) Policy and Coordination

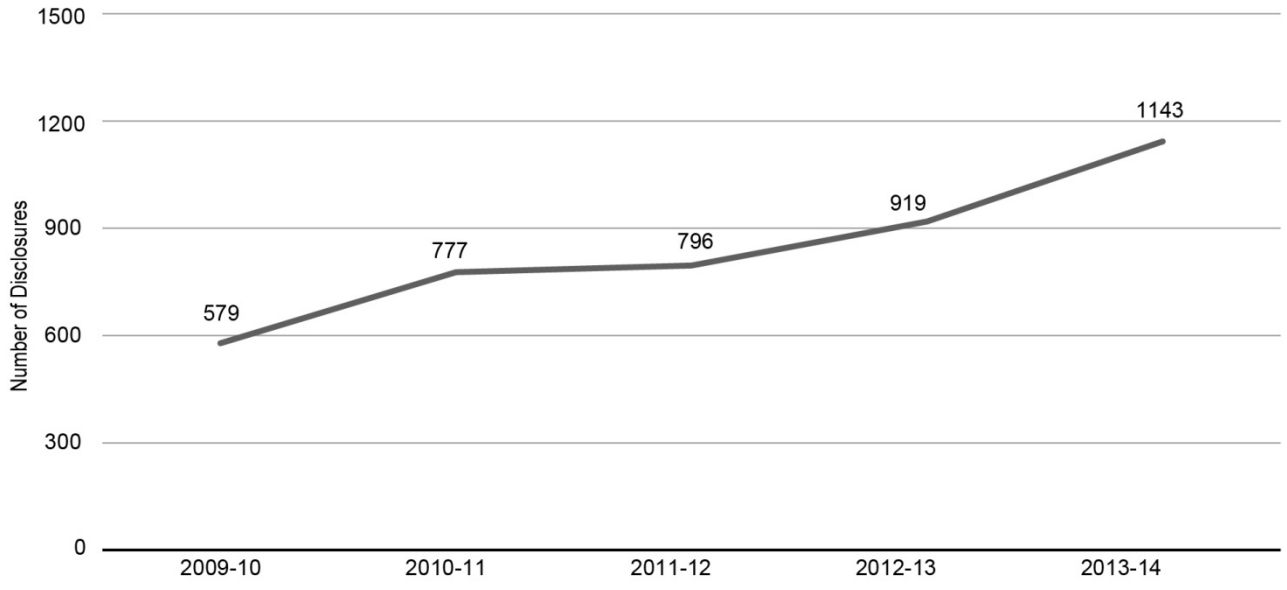
The first pillar consists of the regime's policy and legislative framework as well as its domestic and international coordination, which is led by the Department of Finance Canada. The PCMLTFA is the legislation that establishes Canada's AML/ATF framework, supported by other key statutes, including the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

The PCMLTFA requires prescribed financial institutions and DNFBPs, known as reporting entities, to identify their clients, keep records and establish and administer an internal AML/ATF compliance program. The PCMLTFA creates a mandatory reporting system for suspicious financial transactions, large cross-border currency transfers and other prescribed transactions. It also creates obligations for the reporting entities to identify ML/TF risks and to put in place measures to mitigate those risks, including through ongoing monitoring of transactions and enhanced customer due diligence measures.

The PCMLTFA also establishes an information sharing regime where, under prescribed conditions respecting individuals' privacy, information submitted by the reporting entities is analyzed by FINTRAC and the results disseminated to regime partners and the general public. The information disseminated under the PCMLTFA can be intelligence used to support domestic and international partners in the investigation and prosecution of ML/TF related offences. The information can also be in the form of trend and typology reports used to educate the public, including the reporting entities, on ML/TF issues.

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

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



Given the number of regime participants and the complexity of the issues, the effective regime-wide coordination of strategic, policy and operational matters is important. In addition, given that many serious forms of money laundering and terrorist financing often have international dimensions, Canada's cooperation internationally is also a key component. International cooperation is a core practice of the regime, and for many partners it is conducted on a routine basis, in particular in supporting investigations and prosecutions of money laundering and terrorist financing, including through formal mutual legal assistance led by the Department of Justice Canada.

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

Canada recognizes that protecting the integrity of the international financial system from money laundering and terrorist financing requires playing a strong international role to broadly increase legal, institutional and operational capacity globally. Canada's international AML/ATF initiatives are advanced through the leadership role that it plays in the Financial Action Task Force (FATF), the G-7, the G-20, the Egmont Group of Financial Intelligence Units and, most recently, the counter-financing work stream of the Anti-Islamic State of Iraq and the Levant (ISIL) Coalition.[6]

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

(ii) Prevention and Detection

The second pillar provides strong measures to prevent individuals from placing illicit proceeds or terrorist-related funds into the financial system, while having correspondingly strong measures to detect the placement and movement of such funds. At the centre of this prevention and detection approach are the reporting entities, specifically the financial institutions and DNFBPs, that are the gatekeepers of the financial system in implementing the various measures under the PCMLTFA, and the regulators, principally FINTRAC and OSFI, which supervise them.

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

(iii) Disruption

The final pillar deals with the disruption of money laundering and terrorist financing. Regime partners, such as CSIS, the CBSA and the RCMP, supported by FINTRAC's intelligence gathering and analysis activities, undertake financial investigations in relation to money laundering, terrorist financing and other profit-oriented crimes. The CRA also plays an important role in investigating tax evasion and its associated money laundering, and in detecting charities that are at risk and ensuring that they are not being abused to finance terrorism. The PPSC ensures that crimes are prosecuted to the fullest extent of the law.

The restraint and confiscation of proceeds of crime is also an important law enforcement component of the regime. PWGSC manages all seized and restrained property for criminal cases prosecuted by the Government of Canada. The CBSA enforces the Cross-Border Currency Reporting Program, and transmits information from reports and seizures to FINTRAC.

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

The regime also has a robust terrorist listing process to freeze terrorist assets, pursuant to the *Criminal Code* and the *Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism*, which is led by Public Safety Canada and DFATD, respectively. Canada currently has 90 terrorist-related listings under this process.[7]

Oversight and Enhancements

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

The Parliament of Canada undertakes a comprehensive review of the PCMLTFA every five years and the Office of the Privacy Commissioner of Canada is required to conduct a privacy audit of FINTRAC every two years. Among other periodic reports,[8] reviews and audits, the regime's performance is statutorily mandated to be reviewed every five years. Internationally, Canada's regime is assessed by the FATF against its global AML/ATF standards and is subject to the FATF's follow-up process.

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

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

Implementation

The Government of Canada expects that this report will be used by financial institutions and other reporting entities to contribute to their understanding of how and where they may be most vulnerable and exposed to inherent ML/TF risks. FINTRAC and OSFI will include relevant information related to inherent risks in their respective guidance documentation to assist financial institutions and other reporting entities in integrating such information in their own risk assessment methodology and processes so that they can effectively implement controls to mitigate ML/TF risks. Members of the oversight of the regime will also use the results of the risk assessment to inform policy and operations as part of the ongoing efforts to combat money laundering and terrorist financing.

[7] As of December 31, 2014.

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

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

Overview

The Government of Canada has developed an assessment to identify and understand inherent ML/TF risks in Canada, and their relative importance, through a rigorous and systematic analysis of qualitative and quantitative data and expert opinion about money laundering and terrorist financing. The assessment provides the basis to think critically and systematically about ML/TF risks on an ongoing basis, and to promote a common understanding of these risks. This chapter provides an overview of the risk assessment methodology.

Scope of the Methodology

The methodology assesses the inherent ML/TF risks, which are the fundamental risks in Canada that are the subject of the broad suite of government and private sector controls and activities to effectively mitigate those risks. Understanding Canada's risk context and the main characteristics that expose sectors and products to inherent ML/TF risks in Canada is important in being able to identify and apply measures to effectively mitigate them.

The basis of the risk assessment is that risk is a function of three components: threats, inherent vulnerabilities and consequences. Furthermore, risk is viewed as a function of the likelihood of threat actors exploiting inherent vulnerabilities to launder illicit proceeds or fund terrorism and the consequences should this occur.

Key Definitions

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

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

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

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

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

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

Assessing the ML/TF Threats and Inherent Vulnerabilities

During a series of workshops, experts from Canada's AML/ATF regime used their expertise and knowledge to assess the ML/TF threats and inherent vulnerabilities of sectors and products using the rating criteria set out in the methodology. In addition, the experts harnessed the regime's store of information, data and analysis to rate each threat and vulnerability. Experts provided ratings of low, medium, high or very high using the defined rating criteria to assess the range of threats and inherent vulnerabilities. The individual ratings were then aggregated to arrive at an overall rating.

The ML threat in Canada was assessed for 21 criminal activities that are most associated with generating proceeds of crime in Canada as well as the threat from third-party money laundering. The ML threat was rated for each criminal activity against four rating criteria: the extent of the threat actors' knowledge, skills and expertise to conduct money laundering; the extent of the threat actors' network, resources and overall capability to conduct money laundering; the scope and complexity of the ML activity; and the magnitude of the proceeds of crime being generated annually from the criminal activity. The ML threat rating results are presented in Chapter 3.

The TF threat in Canada was assessed for 10 terrorist groups as well as for foreign fighters, defined as those who travel abroad to support and fight alongside terrorist groups. The TF threat of these groups was assessed against six rating criteria: the extent of the threat actors' knowledge, skills and expertise to conduct terrorist financing; the extent of the threat actors' network, resources and overall capability to perform TF operations; the scope and global reach of their TF operations; the estimated value of their fundraising activities annually in Canada; the extent of the diversification of their methods to collect, aggregate, transfer and use funds; and the extent to which the funds may be used against Canadian domestic and international interests. The TF threat rating results are presented in Chapter 4.

The assessment considered the inherent features of Canada that may be exploited by threat actors for illicit purposes (e.g., geography, economy, demographics). Against this, the inherent ML/TF vulnerabilities were assessed for 27 economic sectors and products. The areas were assessed against five rating criteria: the inherent characteristics of the assessed areas (size, complexity, accessibility and integration); the nature and extent of the vulnerable products and services; the business relationship with its clients; geographic reach (extent of activity with high-risk jurisdictions and locations of concern); and the degree of anonymity and complexity afforded by the delivery channels. Canada's inherent features and sector and product vulnerability assessment results are presented in Chapter 5.

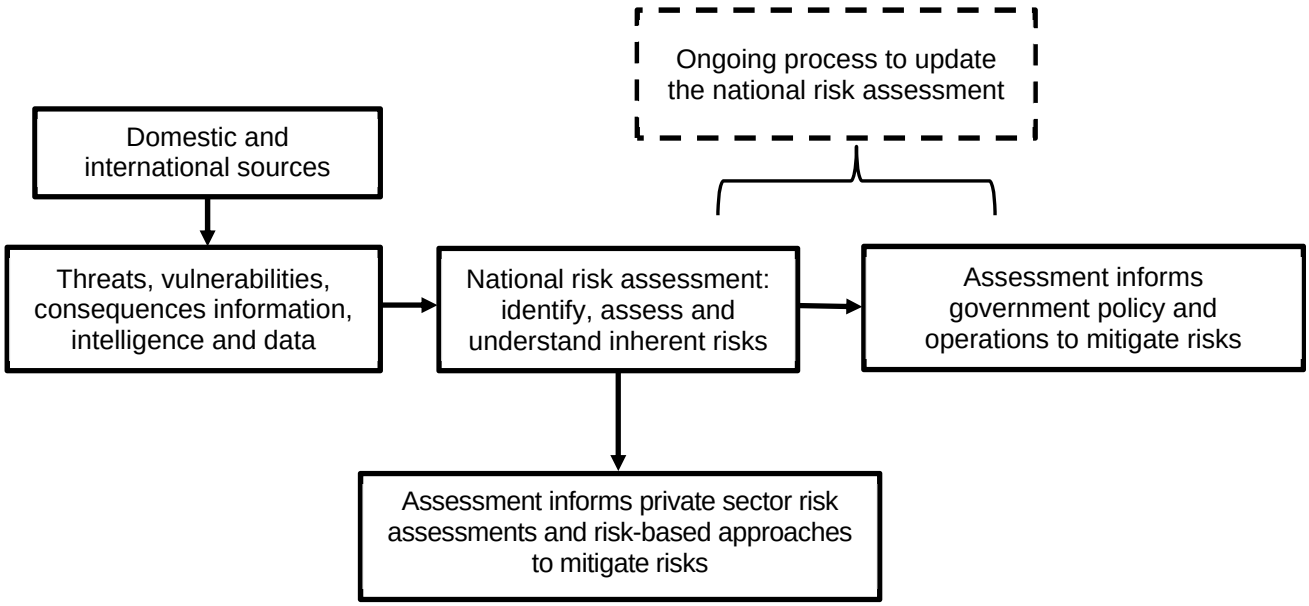
Assessing the Inherent ML/TF Risks

The inherent ML/TF risks were assessed based on the likelihood of money laundering or terrorist financing occurring while considering the consequences of such events. The likelihood of the money laundering or terrorist financing was assessed by matching the ML/TF threats with the inherently vulnerable sectors and products through the ML/TF methods and techniques that are used by threat actors to exploit these sectors and products. Inherent ML/TF risk scenarios were created from these judgements and used to plot the inherent risk results by sector, product or service in a number of illustrative charts. This presentation allows one to compare the different levels of exposure of various sectors and products to inherent ML/TF risks in Canada.[9] The results are presented in Chapter 6.

Risk Assessment and Mitigation Framework

The inherent risk assessment and its methodology should be viewed as one core element of a larger framework to support an ongoing process to identify, assess and mitigate ML/TF risks in Canada. This framework is summarized below in Chart 2.

Chart 2
Canada's ML/TF Risk Assessment Framework



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

Chapter 3: Assessment of Money Laundering Threats

Overview

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

Threat actors who perpetrate profit-oriented crime in Canada range from unsophisticated, criminally inclined individuals, including petty criminals and street gang members, to criminalized professionals[10] and organized crime groups (OCGs).[11] According to the Criminal Intelligence Service Canada, there are over 650 OCGs operating in Canada. Of these threat actors, transnational OCGs are the most threatening both in terms of generating the most proceeds of crime and in the intensity of efforts to launder the proceeds. The most powerful transnational OCGs in Canada, consisting of factions with ties to Italy and Asia, and certain Outlaw Motorcycle Gangs, are involved in multiple lines of profit-oriented crime and have the infrastructure and network to launder large amounts of proceeds of crime on an ongoing basis through multiple sectors using a diverse set of methods to avoid detection and disruption. These OCGs have strong networks and strategic relationships with other criminal organizations domestically and internationally (e.g., Mexican and Columbian drug cartels).

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

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

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

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

Discussion of the Money Laundering Threat Assessment Results

Experts assessed the ML threat for 21 profit-oriented crimes and third-party money laundering using the following criteria:

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

As presented in Table 1, eight profit-oriented crimes and third-party money laundering were rated as a very high ML threat, eight were rated high, four were rated medium and one was rated low.

Table 1
Overall Money Laundering Threat Rating Results

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

Very High Money Laundering Threats

ML Threat from Capital Markets Fraud: Securities fraud, including investment misrepresentation and other forms of capital markets fraud-related misconduct, such as illegal insider trading and market manipulation, occurs in Canada. Over one-quarter of Canadians believe that they have been approached with a possible fraudulent investment opportunity.[12] Although it is challenging to be definitive on the actual amount of reported losses, capital markets fraud is a rich source of proceeds of crime. For instance, in 2009, two Canadians were arrested and charged with fraud, theft and money laundering for orchestrating a Ponzi-style investment fraud that resulted in defrauding about 2,000 investors of between $100 million and $200 million. Most of the large-scale securities frauds in Canada have been perpetrated by criminalized professionals, who have (or purport to have) professional credentials and financial expertise. Perpetrating capital markets fraud, especially the larger, more elaborate national and international schemes (such as Ponzi schemes), requires significant knowledge and expertise and, often, access to a network of witting or unwitting facilitators to help orchestrate and perpetrate the fraud. Alongside the sophisticated fraudulent schemes, there are sophisticated ML schemes designed to integrate and legitimize the fraud-related proceeds into the financial system. ML schemes in this context would involve a range of sectors and methods, including shell or front companies, electronic funds transfers (EFTs), structuring and/or smurfing deposits[13] and nominees[14].

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

---

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

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

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

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

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

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

[15] Money mules are those who facilitate fraud and ML schemes, often unknowingly (e.g., moving money through international EFTs on behalf of criminals). They are often located in different jurisdictions from where the crimes are committed and they tend to exhibit very low levels of sophistication and capability and are essentially directed to undertake certain actions to launder the funds.

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

ML Threat from Mortgage Fraud: Mortgage fraud occurs across Canada, but it is most prevalent in large urban areas in Quebec, Ontario, Alberta and British Columbia. Mortgage fraud schemes are often undertaken to facilitate another criminal activity (e.g., illicit drug production and distribution, money laundering) or directly for profit. OCGs conduct the vast majority of mortgage fraud in Canada. To carry out this crime, OCGs are believed to rely on the assistance of witting or unwitting professionals in the real estate sector, including agents, brokers, appraisers and lawyers. OCGs frequently use straw buyers to orchestrate the mortgage fraud. OCGs conducting mortgage fraud schemes are, for the most part, suspected to be highly sophisticated and capable in terms of the associated ML activity. Professional money launderers have been used to launder mortgage fraud-related proceeds. It is suspected that criminally inclined real estate professionals, notably real estate lawyers, are used to facilitate money laundering. OCGs involved in mortgage fraud appear to launder funds through banks, MSBs, legitimate businesses and trust accounts. Victims of mortgage fraud, which can include Canadian homeowners and lending institutions, can incur significant financial losses.

ML Threat from Third-Party Money Laundering: Large-scale and sophisticated ML operations in Canada, notably those connected to transnational OCGs, frequently involve third-party money launderers, namely professional money launderers, nominees or money mules. Of the three, professional money launderers pose the greatest threat both in terms of laundering domestically generated proceeds of crime as well as laundering foreign-generated proceeds through Canada (and through its financial institutions). Professional money launderers specialize in laundering proceeds of crime and generally offer their services to criminals for a fee. These individuals are in the business of laundering large sums of money and by their very nature have the sophistication and capability to support complex, sustainable and long-term ML operations. As a group, they use many different methods and techniques, sometimes within the same scheme, to launder money that is challenging to detect. The professional money launderers are of principal concern since they are often the masterminds behind large-scale ML schemes and are frequently used by the most powerful transnational OCGs in Canada. Nominees and money mules are less of a threat, but nonetheless important because they may be critical in carrying out or facilitating ML schemes, both large and small.

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

ML Threat from Tobacco Smuggling and Trafficking: The largest quantity of illicit tobacco found in Canada originates from the manufacturing operations based on Aboriginal reserves that straddle Quebec, Ontario and New York State. Given the profitable nature of the illicit tobacco trade, there is significant organized crime involvement in the smuggling and trafficking of illicit tobacco across the Canada-U.S. border. The OCGs involved in the illicit tobacco trade are some of the most sophisticated and threatening in Canada. These OCGs have the sophistication and capability to use a variety of sectors and methods (e.g., commingling, structuring, smurfing and refining) to launder the large amount of cash proceeds that are generated from the illicit tobacco smuggling and trafficking. In addition to the proceeds of crime generated from the reserve-manufactured illicit tobacco trade, proceeds of crime are generated from counterfeit cigarettes imported from overseas (primarily from China); cigarettes produced legally in Canada, the United States or abroad, and sold tax-free; and "fine cut" tobacco imported illegally, mostly by Canadian-based manufacturers.

High Money Laundering Threats

ML Threat from Currency Counterfeiting: The large-scale production of Canadian counterfeit currency is primarily undertaken by OCGs. OCGs generally conduct currency counterfeiting alongside other profit-oriented criminal activities. OCGs that produce and distribute high-quality counterfeit currency are suspected to exhibit a high level of sophistication and capability in terms of the methods used to launder the proceeds arising from currency counterfeiting. They appear to have the network and infrastructure in place to successfully launder, through a number of sectors, predominantly cash proceeds arising not only from currency counterfeiting but also from their other criminal activities.

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

ML Threat from Human Trafficking: Canada is primarily a destination country for human trafficking, and domestic human trafficking for sexual exploitation is the most common form of human trafficking in Canada.[17] Sex trafficking is largely perpetrated by criminally inclined individuals, who recruit and traffic domestically and, to a lesser extent, OCGs, some of which only recruit and traffic domestically, while others recruit and traffic domestically and internationally. Criminally inclined individuals are not believed to exhibit any real levels of sophistication or capability in terms of laundering their sex trafficking-related proceeds. It is suspected that most of their activity would centre on laundering mostly cash proceeds for immediate personal use, leveraging a very limited or non-existent network, and using a limited number of sectors and methods. The OCGs that conduct sex trafficking and generate significant proceeds are suspected to use established ML infrastructure to launder the proceeds. Some OCGs, although less sophisticated in terms of money laundering, are nonetheless more capable because they may have access to venues to facilitate money laundering (e.g., strip clubs and massage parlors) as well as victims that can be used as nominees for deposits and wire transfers.

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

ML Threat from Identity Theft and Fraud ("Identity Crime"): Identity crime is prevalent in Canada and it is a concern given that stolen identities are often used to support the conduct of other criminal activities. The OCGs conducting identity crime are well-established and resilient, and have well-developed domestic and international networks. They are also associated with drug trafficking, human smuggling and counterfeiting currency. It is suspected that these OCGs use multiple methods and sectors to launder the funds. Identity crime itself can support money laundering by providing individuals with fake credentials to subvert customer due diligence safeguards. In 2014, Canadians reported over $10 million in losses to identity crime.[18] It is important to note that identity crime also facilitates the conduct of other criminal activities that generate significant proceeds of crime.

ML Threat from Illegal Gambling: Illegal gambling in Canada consists of private betting or gaming houses, unregulated video gaming and lottery machines, and unregulated online gambling. Organized crime is the major provider of illegal gambling opportunities in Canada, although there are some smaller operators. The illegal gambling market appears to be small in terms of the numbers of threat actors involved, but it is suspected to be highly profitable for those involved in it. OCGs conduct these activities in a sophisticated manner. For traditional bookmaking betting activities, OCGs use pyramid-style schemes to protect more senior members of the pyramid. Bookmakers will only accept cash to benefit from its anonymity. For online gambling, OCGs have based the network servers to run illegal gambling sites in jurisdictions where online gambling is legal. It is assumed that the OCGs operating in this space have the capability to use a variety of sectors and methods to launder the proceeds of crime. The main forms of illegal gambling proceeds are cash and possibly high value goods (in instances where gamblers may have run out of cash).

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

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

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

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

ML Threat from Pollution Crime: Pollution crime in Canada comes in a variety of forms and is principally undertaken by OCGs, companies and individuals. Of the forms taken, there is particular concern that OCGs have infiltrated the waste management sector, as owning waste management companies can be an effective vehicle to generate illicit profits, by dumping waste illegally, and to launder proceeds from other criminal activities. OCGs may also be involved in the trafficking of electronic waste and in the importation of counterfeit products that do not meet Canada's environmental standards (e.g., counterfeit engines). Finally, some private and public companies may be using deceptive practices to undermine emissions schemes and may be dumping or using third parties to dump waste illegally. Given the sophisticated nature of activities and operations, it is assumed that there is a great degree of sophistication, capability and scope in terms of being able to launder the proceeds arising from pollution-related crime. In the case of waste management, the OCGs appear to demonstrate a very high degree of sophistication and capability to operate waste management businesses in a manner that generates illegal profit and is used for money laundering.

ML Threat from Robbery and Theft: Smaller-scale thefts and robberies are most frequently carried out by opportunistic individuals and petty thieves, while larger-scale thefts and robberies are more frequently associated with OCGs, which are heavily involved in motor vehicle, heavy equipment and cargo theft. The most sophisticated and capable tend to be the OCGs that have well-established auto theft networks in Canada, which are used to supply foreign markets with stolen Canadian vehicles. The OCGs that have established auto theft networks in Canada are also suspected to be highly sophisticated and capable from a ML perspective. It is believed that these OCGs use a range of trade-based fraud and related ML techniques to disguise the illicit origin of the automobiles as well as a range of methods to move the proceeds back into Canada, including bulk cash smuggling and EFTs. Front companies, shell companies and nominees may be used to obscure the flow of funds back to Canada arising from the illicit sales in other countries. Professional money launderers may be utilized to mastermind ML schemes given the large amounts of proceeds generated by these networks and the challenges of laundering proceeds that are generated across multiple jurisdictions.

Medium Money Laundering Threats

ML Threat from Firearms Smuggling and Trafficking: The illicit firearms market in Canada appears to be dominated by unsophisticated, criminally inclined individuals and OCGs (primarily street gangs operating in metropolitan areas) as well as a small number of sophisticated OCGs. Very few OCGs are involved in the trafficking or smuggling of firearms for the purpose of achieving large profits. Instead, OCGs mainly use firearms to strengthen their position within other criminal markets, such as the illicit drugs market. While the majority of guns recovered in crime in Canada are believed to be domestically sourced, a majority of successfully traced handguns are smuggled into Canada from abroad, mostly from the United States. OCGs may sell illicit firearms to other OCGs and criminally inclined individuals, although it is unclear how important these OCGs are in terms of acting as a general supply hub for illicit firearms in Canada. These OCGs may use their established ML infrastructure to launder the proceeds arising from their firearms trafficking activities, which generally focus on exploiting a number of different sectors using a variety of methods.

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

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

ML Threat from Tax Evasion / Tax Fraud (hereafter referred to as tax evasion): Tax evasion is carried out in many different forms in Canada, with the ultimate objective of underpaying or evading the payment of taxes owing or to unlawfully claim refunds or credits. Tax evasion is frequently carried out by opportunistic individuals, commonly using relatively unsophisticated techniques to evade taxes, such as falsifying or fabricating documentation to misrepresent their tax situation. To facilitate tax evasion, unscrupulous tax preparers have been known to provide counsel on how to evade taxes or obtain fraudulent refunds using a variety of different techniques. Tax evasion is also conducted by professional criminals, including OCGs, who may orchestrate tax evasion schemes (e.g., duty or tax refund fraud). Since tax evasion generally involves ordinary individuals using tax evasion techniques of low sophistication, the ensuing money laundering is also believed to be unsophisticated. In cases of large (or multiple) refunds that have been generated by sophisticated tax evasion schemes, more sophisticated ML techniques may be observed.

Low Money Laundering Threats

ML Threat from Wildlife Crime: There is an established illicit market for certain types of Canadian species, including narwhal tusks, polar bear hides, peregrine falcon eggs and wild ginseng. Black market prices for certain Canadian species are high and have risen significantly over the last five years. Wildlife crime in Canada appears to be largely conducted by opportunistic, criminally inclined individuals. Individuals conducting wildlife crime are suspected to exhibit low levels of sophistication, capability and scope in terms of laundering wildlife crime-related proceeds. The proceeds tend to be fairly modest (with some exceptions) and the laundering activity appears to be focused on immediately placing or integrating the proceeds for personal use, and limited to one sector.

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

Chapter 4: Assessment of Terrorist Financing Threats

Overview

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

Canada has listed 54 terrorist entities under its *Criminal Code* and 36 terrorist entities under the *Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism.* [23] The majority of these entities are based in foreign countries, mainly in Africa, Asia and the Middle East.[24] Members or supporters/sympathizers of some of these listed entities have been present in Canada at one point or another. Their activities have often focused on providing financial or material support to terrorist entities based in foreign countries. Although their focus has been more on terrorist financing and less on conducting terrorist attacks in Canada, Canada is not immune to such attacks and, over the years, a few attacks have been carried out while others have been thwarted. Canadian interests[25] have also been affected by terrorism-related incidents that have occurred abroad.

Not all 90 listed terrorist entities pose a TF threat to Canada since not all of these entities have financing or support networks in Canada. Consequently, an entity posing a terrorist threat to Canada does not necessarily pose a TF threat to Canada, or if so, the level of threat may not be the same. On the one hand, some terrorist groups and associated individuals pose a significant terrorist attack threat to Canada at home and abroad, while the TF threat in Canada is lower. On the other hand, some entities pose a very high or high TF threat but a lower terrorist attack threat to Canada.[26]

A number of TF methods have been used in Canada and have involved both financial and material support for terrorism, including the payment of travel expenses and the procurement of goods.[27] The transfer of suspected terrorist funds to international locations has been conducted through a number of methods including the use of MSBs, banks and non-profit organizations (NPOs) as well as smuggling bulk cash across borders. Based on open source and other available reporting on the potential for Canadians to send money or goods abroad to fund terrorism, the following countries were assessed to be the most likely locations where such funds or goods would be received: Afghanistan, Egypt, India, Lebanon, Pakistan, Palestinian Territories, Somalia, Sri Lanka, Syria, Turkey, United Arab Emirates and Yemen.

---

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

23 As at December 31, 2014.

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

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

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

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

Discussion of the Terrorist Financing Threat Assessment Results

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

Table 2
Terrorist Financing Threat Groups of Actors

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

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

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

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

Al Qaeda Core and Affiliated Groups

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

Al Shabaab

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

Foreign Fighters/Extremist Travellers

More attention has been given in recent years by Canada and other countries to individuals referred to as "foreign fighters" or "extremist travellers" who have travelled to other countries to participate in terrorism-related activities. As of early 2014, the Government of Canada was aware of more than 130 individuals with Canadian connections who were abroad and who were suspected of terrorism-related activities, which included involvement in training, fundraising, promoting radical views and planning terrorist violence. These foreign fighters are frequently self-funded or have raised funds from friends and family, and have participated or currently participate in conflicts such as those in Afghanistan, Iraq, Somalia and Syria. Foreign fighters may deplete and close bank accounts and max out credit cards prior to travelling abroad. A number of those individuals remain abroad, some have returned to Canada and others are presumed dead.[29] Foreign fighters returning to Canada[30] may encourage and recruit aspiring violent extremists in Canada, may engage in fundraising activities, or may even plan and carry out terrorist attacks in Canada.

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

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

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

Hamas

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

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

Hizballah

Hizballah, a populist Lebanon-based terrorist organization seeking to represent the Shi'a people and Shi'a Islamism, is highly disciplined and sophisticated, with extensive paramilitary, terrorist and criminal fundraising capabilities. It has a global network of support that spans the Americas, Europe, the Middle East and Africa. Hizballah has an established fundraising network in Canada.

Khalistani Extremist Groups

Khalistani extremist groups, such as Babbar Khalsa International and the International Sikh Youth Federation, are suspected of raising funds for the Khalistan cause in a number of countries, particularly in countries that have large Sikh diaspora populations. There appears to be a global network but it is unclear how strong it is and the motivations surrounding the support. These groups used to have an extensive fundraising network in Canada, but it now appears to be fractured and diffuse.

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

Overview

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

While being mindful of the contextual vulnerabilities of Canada, experts assessed the inherent ML/TF vulnerabilities of 27 economic sectors and financial products, using the following five rating criteria:

1) *Inherent Characteristics:* the extent of the sector's economic significance, complexity of operating structure, integration with other sectors and scope and accessibility of operations.

2) *Nature of Products and Services:* the nature and extent of the vulnerable products and services and the volume, velocity and frequency of client transactions associated with these products and services.

3) *Nature of the Business Relationships:* the extent of transactional versus ongoing business, direct versus indirect business relationships and exposure to high-risk clients and businesses.

4) *Geographic Reach*: the exposure to high-risk jurisdictions and locations of concern.

5) *Nature of the Delivery Channels*: the extent to which the delivery of products and services can be conducted with anonymity (face-to-face, non-face-to-face, use of third parties) and complexity (e.g., multiple intermediaries with few immediate controls).

The assessment indicates that there are a significant number of economic sectors and financial products that are inherently vulnerable to money laundering and terrorist financing. Of the 27 rated areas, the overall ML/TF vulnerability was rated "very high" for five sectors and products, "high" for 16 sectors and products, "medium" for five sectors and products and "low" for one sector (see Table 3). Inherent vulnerabilities and risks are, however, the subject of mitigation and control measures provided by the AML/ATF regime, including through preventive measures and effective supervision.

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

Corporations (and company services providers), express trusts, lawyers[31] and NPOs, although not subject to reporting obligations under the PCMLTFA, were formally included as part of this assessment since it was determined to be necessary to assess their ML/TF vulnerabilities given their importance and widespread use within Canada. Other sectors and products that are not currently covered under the PCMLTFA will continue to be assessed for ML/TF risks. These include, but are not limited to, cheque cashing businesses, closed-loop pre-paid access,[32] factoring companies,[33] financing and leasing companies, ship-based casinos, unregulated mortgage lenders and white-label automated teller machine providers.

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

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

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

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

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

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

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

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

Inherent Vulnerabilities of Canada

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

Governance/Legal Framework

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

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

Geography

Canada is the second-largest country[34] in the world with a land area of 9.9 million square kilometres. Canada has a total of over 200,000 kilometres of coastlines spanning the Pacific Ocean to the west, the Arctic Ocean to the north and the Atlantic Ocean to the east. Canada shares the longest international border in the world, at over 8,800 kilometres, with the United States to the south and northwest (Alaska). This makes Canada vulnerable to criminal activities conducted across Canada, as well as by land, air or marine modes of transportation through its borders. Detection of criminal activities may be challenging in light of the geographic expanse of Canada.

Economy and Financial System

Canada was the 15th largest economy in the world at the end of 2013 (based upon a ranking of real gross domestic product (GDP), with a value of 1,518.4 billion current international dollars).[35] In the same year, 70 per cent of the economy was devoted to services, while manufacturing and primary sectors accounted for the remaining 30 per cent.[36]

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

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

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

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

Since 2006, the size of Canada's underground economy (i.e., economic activity that is not reported for tax purposes) expressed as a percentage of GDP is estimated to have dropped to 2.3 per cent[41] from 2.9 per cent in 1992. A recent Organisation for Economic Co-operation and Development (OECD) study provides an international perspective on relative adjustments for the non-observed economy (NOE) across countries, and suggests that Canada has one of the smaller NOE adjustments, below a number of European Union economies.[42]

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

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

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

---

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

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

39 Ibid.

40 Ibid.

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

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

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

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

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

46 Ibid.

47 Ibid.

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

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

50 Ibid.

51 Ibid.

There are approximately 31,000 financial institutions and DNFBPs (e.g., casinos, MSBs, securities dealers, real estate agents and developers) that are subject to the PCMLTFA, offering products and services that involve financial transactions that can be vulnerable to illicit activity. Table 4 provides an appreciation of the relative size of the various assessed sectors and products.[52]

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

Table 4
Statistics on Assessed Sectors and Products

Sector or Product	Number of Known Entities	Notes
Domestic Systemically Important Banks	6	Banks hold over 60 per cent of the financial sector's assets; the six largest domestic banks, the D-SIBs, hold 93 per cent of these assets.
Other Domestic Banks[53]	22	
Foreign Bank Subsidiaries[54]	24	
Foreign Bank Branches[55]	29 (26 full service and 3 lending)	
Life Insurance Companies	73 federal and 18 provincially regulated[56]	Assets held on behalf of Canadian policyholders and annuitants totalled over $646 billion (end of 2013).
Independent Life Insurance Agents and Brokers	154,000 agents and 45,000 brokers (est.)	
Trust and Loan Companies	63 federally regulated trust companies and loan companies and 14 provincially regulated[57]	Trust and loan companies account for four per cent of the financial sector's assets, or over $320 billion (mid-2013). The six largest Canadian banks own 95 per cent of these trust and loan companies.[58]
Securities Dealers	3,487[59]	The D-SIBs own six of the securities dealers, accounting for 75 per cent of the sector's transaction volume. This sector also includes financial advisors and investment counsellors.
Credit Unions and Caisses Populaires (CUCPs)	696 CUCPs,[60] six Cooperative Credit Associations and one Cooperative Retail Association that are federally regulated	CUCPs hold over $320 billion in assets (November 2014).
Money Services Businesses (MSBs)	850 registered MSBs[61]	The MSB sector handles billions of dollars in transactions each year. It is estimated that MSBs registered with FINTRAC handle approximately $39 billion a year.

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

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

[54] Ibid.

[55] Ibid.

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

[57] Ibid.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[74] Based on internal research.

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

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

Demographics

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

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

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

Discussion of the Results of the Inherent Vulnerabilities Assessment

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

The vulnerability of credit unions and caisses populaires (CUCPs), foreign bank branches and subsidiaries, and trust and loan companies were rated high. These institutions are significant in terms of their size and scope and are accessible to a broad range of clients. Foreign bank branches are believed to be less accessible to retail clients, with a larger proportion of their business focused on corporate clients (given the $150,000 minimum deposit threshold). All of these institutions offer a range of vulnerable products and services and undertake a mix of transactional, ongoing and third-party business. These vulnerable products and services are available to a client base of which a significant amount consists of high-risk clients. Foreign bank subsidiaries often target specific diaspora communities in Canada as well as foreign individuals, which may make them more vulnerable to foreign politically exposed persons (PEPs) and clients with connections to high-risk jurisdictions. CUCPs operate in more remote Canadian locations that, in

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

some instances,[78] may attract high crime and corruption activities as well as transient workers sending remittances back to their home countries, which may be at high risk of ML/TF. Finally, most of these institutions provide services through face-to-face and non-face-to-face delivery channels, provided online or over the telephone, which lend themselves to varying degrees of anonymity. There are, however, some foreign subsidiaries that offer banking services exclusively in a non-face-to-face environment. In contrast, CUCPs tend to focus more on fostering face-to-face interactions through branch locations, which makes the business relationship less anonymous.

ML/TF Vulnerabilities of the Money Services Businesses Sector (Medium to Very High): Although the MSB sector is broadly vulnerable, the degree of vulnerability is not uniform largely because of the variation in terms of size and business models found among the MSBs across the sector. Of those assessed, there are two types of MSBs that are most vulnerable. The first consists of the national full-service MSBs that have the most dominant presence in Canada. These MSBs conduct a large amount of transactional business of products and services (i.e., wire transfers, currency exchange and monetary instruments) that have been found to be vulnerable to money laundering and terrorist financing. These products and services are widely accessible and it is assessed that PEPs, clientele in vulnerable businesses or occupations, and clientele whose activities are conducted in locations of concern comprise a significant portion of the clientele profile. The second type of highly vulnerable MSB consists of the small, predominantly family-owned MSBs located across Canada that provide wire transfer services largely through informal networks. These MSBs are vulnerable because they can allow high-risk clients to wire funds to high-risk jurisdictions through their informal networks. In addition, because they tend to be small, low-profile businesses, they may be vulnerable to being exploited for illicit purposes.

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

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

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

TF Vulnerabilities of Registered Charities (High):[79] The registered charities of greatest concern are those engaged in "service" activities that operate in close proximity to an active terrorist threat. This encompasses registered charities that operate both in high-risk jurisdictions, including in areas of conflict with an active terrorist threat, as well those that operate domestically, but within a population that is actively targeted by a terrorist movement for support and cover. The assessment indicates that these service-oriented organizations offer a number of vulnerable products and services, including funds, gifts-in-kind, and educational and social services. They may be involved in transactional and indirect relationships. A large number of the financial transactions conducted by registered charities may be performed via delivery channels involving a high degree of anonymity and involving some level of complexity, such as when multiple intermediaries are involved. Individuals may make anonymous donations to registered charities. While the transfer of funds from one organization to another is not likely to be anonymous, the significant use of cash may make the original source of funds difficult to determine. It may also be difficult to know how the funds or resources will be used once transferred to partner organizations or third parties, including agents.

ML/TF Vulnerabilities of Brick and Mortar Casinos (High): Brick and mortar casinos conduct a large amount of business across Canada, most of which is highly transactional and cash-intensive. Casinos provide a limited number of vulnerable products and services, but the volume of transactions that is undertaken with these products and services is viewed as important. The casino's business relationship with clientele is mostly transactional but there are some ongoing relationships. The casino's clientele would include PEPs and non-residents (e.g., tourists) and clientele in vulnerable businesses and professions. Some casinos offer clients the ability to transfer funds electronically, meaning that funds could be sent to high-risk jurisdictions. Clients can conduct gaming activity in casinos relatively anonymously, although casinos are monitored and some activities require face-to-face interaction with casino staff. Despite this monitoring, there is no customer identification or verification of the source of funds.

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

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

The geographic reach of these online casinos is very limited, confined to users based in the province offering the service. All transactions are conducted online through non-face-to-face interactions and can involve intermediaries. Non-face-to-face users must register to use the site and must provide a method of payment (e.g., credit or debit card). Although this reduces the anonymity of the accountholder, it still makes it difficult to determine who is in control of the account.

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

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

ML/TF Vulnerabilities of the Securities Sector (High): The securities sector is significant in Canada and accepts large volumes of funds for investment purposes, usually through wire transfers from bank accounts. The securities sector offers a range of products and services that are vulnerable, including brokerage accounts, a variety of investment products and wire transfers, constituting a significant portion of the sector's operations. Clients include individuals, corporate entities, pension funds and institutional accounts, both domestic and foreign. The sector has a combination of transactional and ongoing account relationships. The client profile includes non-residents, high-net-worth clients, and PEPs in Canada and abroad. Operations are not restricted to domestic transactions; the sector has international reach and involves business with high-risk jurisdictions on an ongoing basis. Most of the securities transactions involve face-to-face interactions; however, online brokerages, whose presence has been growing, are providing the opportunity for greater anonymity in this area. The nature of the delivery channels can be complex, as it can involve representation by third parties, including lawyers.

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

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

ML/TF Vulnerabilities of Virtual Currencies (High): The virtual currency sector is significant in terms of assets and volume of transactions and it employs a variety of complex business/delivery models, involving a range of participants, some of which are evolving rapidly. The sector provides one type of vulnerable product—virtual currency—but it provides a number of different forms of virtual currency, each of which exhibit varying degrees of vulnerability. Convertible virtual currencies, which constitute an important part of the sector, are the most vulnerable, largely because of the increased anonymity that they can provide as well as their ease of access and high degree of transferability. Virtual currency providers appear to have largely transactional relationships with their clients in addition to some more ongoing relationships. Given some recent cases, criminal elements would appear to be attracted to the level of anonymity provided by convertible virtual currencies. Virtual currencies, notably convertible decentralized virtual currencies, can provide a high degree of anonymity and complexity. They can be traded on the internet and some virtual currencies may permit anonymous funding (funding using cash, prepaid cards, or third-party funding through virtual exchangers that do not properly identify the funding source). The anonymity and complexity can pose significant challenges for law enforcement to determine the beneficial ownership of the virtual currency involved in criminal activities.

ML/TF Vulnerabilities of Open-Loop Prepaid Access (High): The use of prepaid access is prevalent in Canada but it represents a small portion of the payment methods used domestically. Open-loop products, which are offered across Canada, can be loaded with cash and can be used as a payment method almost anywhere credit and debit cards are accepted. These products can be used to withdraw cash and to undertake person-to-person transfers in Canada and abroad. The business relationship with clients is transactional and cards are issued to individuals physically present in Canada. Given the nature of the product, clients can be high-risk, including those in vulnerable occupations and businesses. Some open-loop cards can be purchased and loaded relatively anonymously while others that are reloadable and have higher loading limits require proof of identification. In some cases, however, the verification may be done online, in a non-face-to-face setting.

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

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

Inherent Money Laundering Risks

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

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

Bulk cash smuggling or the use of cash couriers, within Canada and across the Canadian border, is a ML method that is frequently used, including by professional money launderers, as the first step in the ML process and does not involve any sector, product or service. Trade-based money laundering[84] is another technique used by professional money launderers and OCGs that poses many detection and investigative challenges since it often involves many players and sectors including different types of corporations, deposit-taking financial institutions, MSBs and brokers that are generally located in various jurisdictions.

Charts 3 to 9 provide a graphic representation of all inherent ML risk scenarios involving the exploitation by ML threat actors of various sectors and products or services, and Table 5 lists all the types of criminal offences that generate illicit proceeds that can then be laundered. The numbers 1 to 9 on the horizontal axis of Charts 3 to 9 should be cross-referenced with Table 5.

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

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

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

[83] The 10 profit-oriented crimes generating the most proceeds and posing a high to very high threat are: human smuggling, payment card fraud, tobacco smuggling and trafficking, mass marketing fraud, mortgage fraud, capital markets fraud, illicit drug trafficking, counterfeiting and piracy, corruption and bribery, and commercial trade fraud.

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

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

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

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

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

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

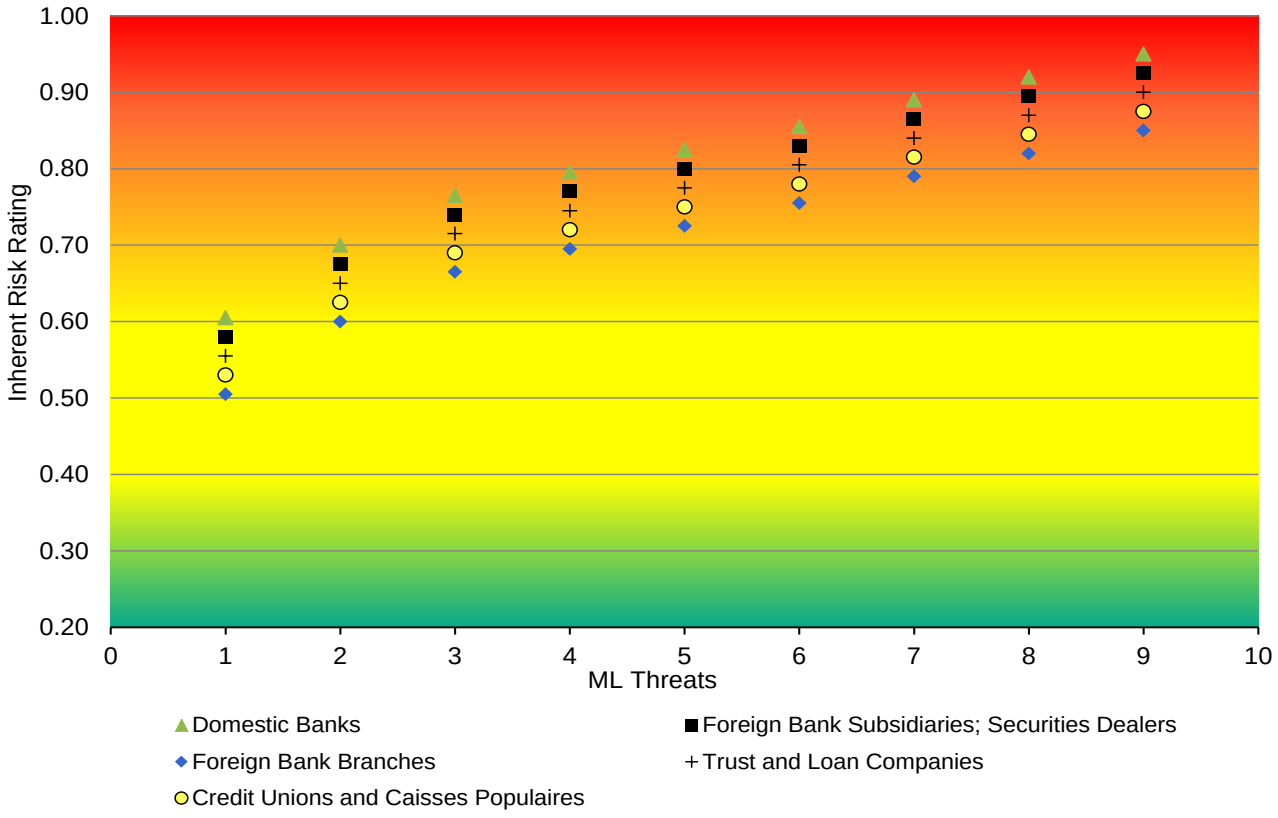
Deposit-Taking Financial Institutions

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

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

Chart 3

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



Deposit-taking financial institutions are well known to be used for the placement and layering stages of money laundering, for example, through the use of personal and business deposit accounts; domestic wire transfers and international EFTs; currency exchanges; and monetary instruments such as bank drafts, money orders and cheques (i.e., personal and travellers). The main ML methods and techniques used to exploit these products and services include the following:

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

Typical Inherent ML Risk Scenario Involving Deposit-Taking Financial Institutions

Members of an OCG involved in drug trafficking, counterfeiting, tobacco smuggling and human trafficking generate, on a weekly basis, large amounts of cash and also receive international EFTs for some of their criminal activities. Given the large amount of illicit proceeds they generate, they have hired a professional money launderer who is coordinating a number of ML activities with the assistance of nominees and smurfs. Money pick-ups are organized and sometimes involve foreign travel; hence the illicit cash is often smuggled into Canada. The same individuals or others are instructed to, over a number of days, deposit cash, using ATMs (during the day or at night), under the $10,000 reporting threshold into various personal and business accounts held at multiple deposit-taking financial institutions. Some are then instructed to purchase bank drafts or issue cheques in the name of identified nominees who then deposit them into other accounts. Funds are then transferred to other individuals or businesses through domestic wire transfers or international EFTs, the latter in instances when individuals or businesses located in foreign countries are part of the ML schemes. At the direction of the professional money launderer, some individuals are also responsible for conducting currency exchanges and refining activities before depositing cash into personal or business accounts, or just handing over the resulting cash to the professional money launderer or other identified individual(s).

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

Securities Dealers

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

- Deposits of physical certificates (little information is available to the broker to confirm the source of the funds used to purchase the shares or how the client obtained them);
- Securities traded over the counter are exchanged directly between entities rather than through an organized stock exchange such as the Toronto Stock Exchange;
- Early redemption of securities;
- Requesting proceeds of securities sale in the form of negotiable instruments;
- Transfers of funds between accounts held at multiple institutions;
- Frequent changes of ownership; and
- Use of off-book transactions, registered representatives, offshore accounts and nominees.

Inherent ML Risk Scenario Involving Stock Manipulation

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

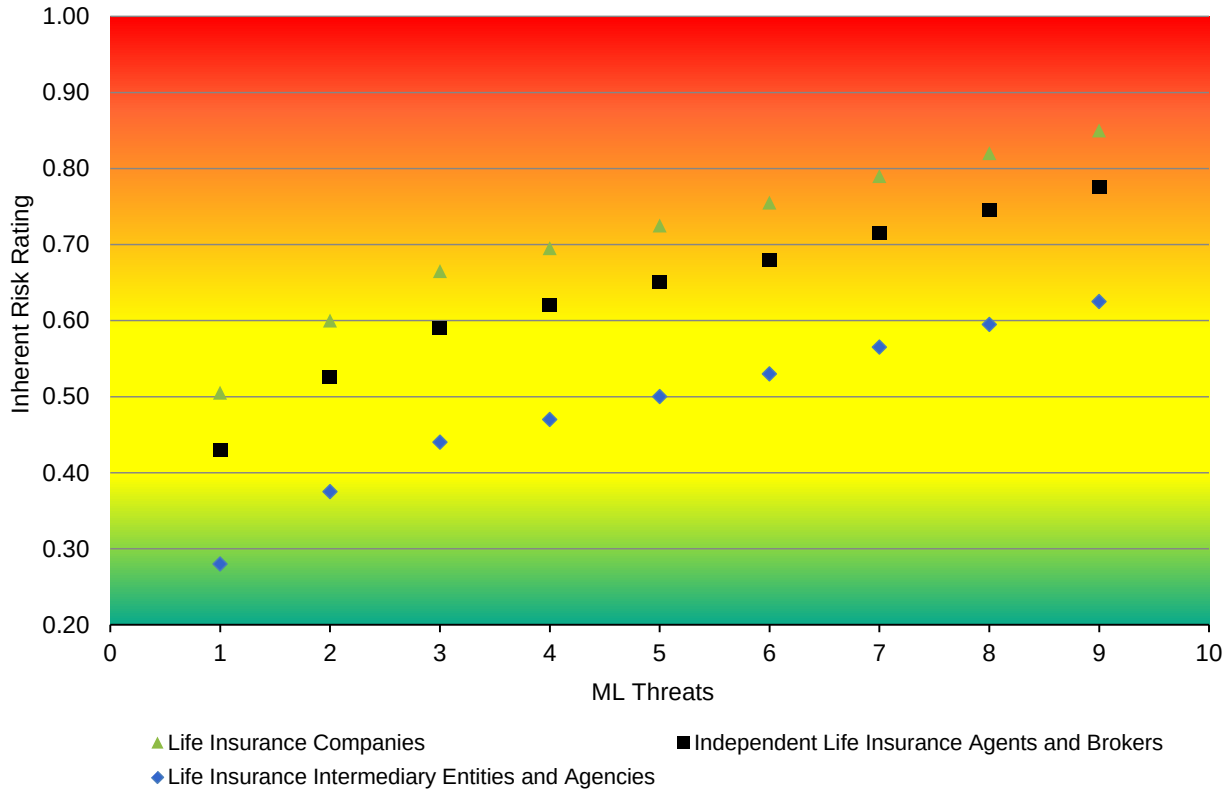
Inherent ML Risk Scenario Involving Over-the-Counter Securities

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

Life Insurance

As illustrated on Chart 4, ML risk scenarios involving life insurance companies and/or individual agents/brokers are rated medium to high. Given that life insurance intermediary entities and agencies mainly provide administrative support to advisors and allow commission pooling opportunities and access to insurance company products, and do not generally deal directly with clients, they are exposed to low to medium inherent money laundering risk scenarios.

Chart 4
Inherent ML Risks in the Life Insurance Sector by Type of ML Threats



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

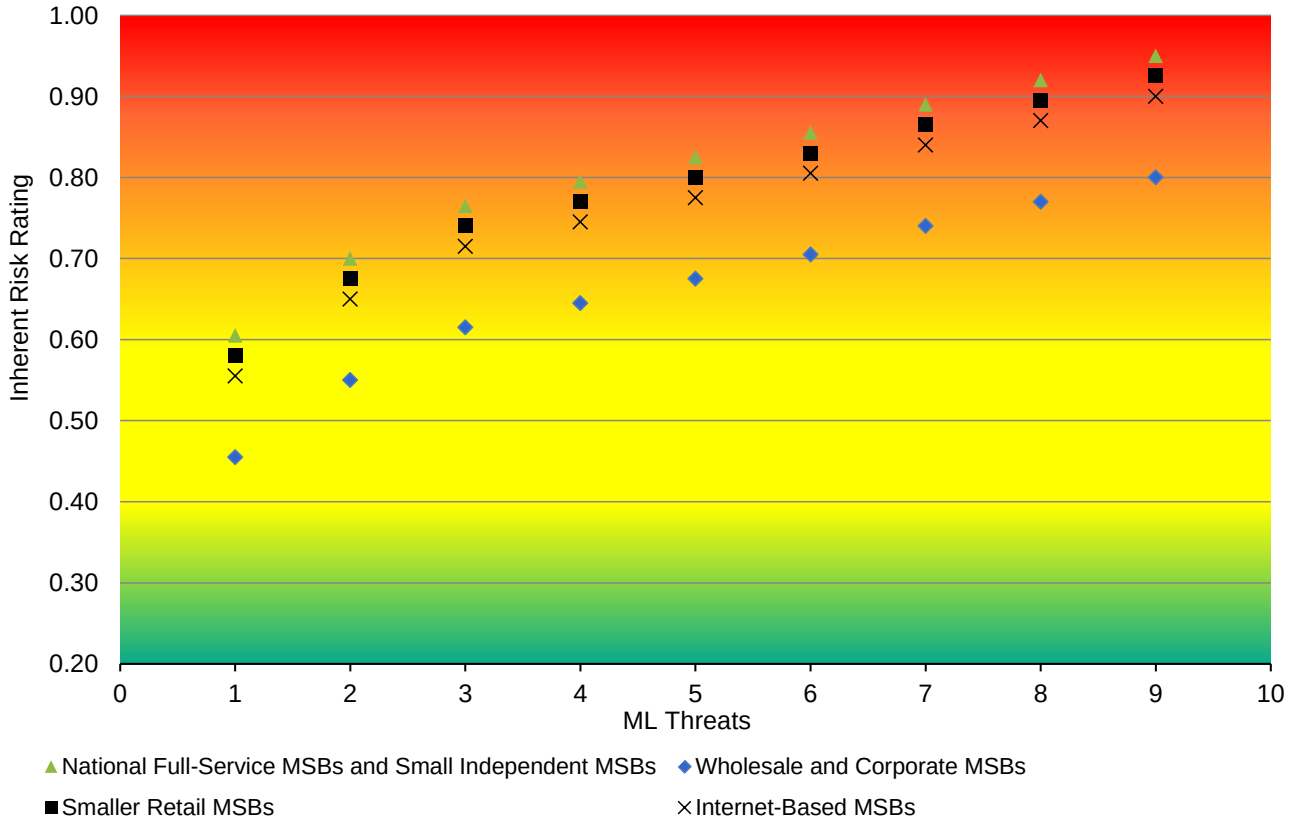
- Early redemption/surrendering of life insurance products with single premium payments and/or high cash values;
- Premium payments made by third parties;
- Use of offshore policies and professional advisors;
- Direct co-option of life insurance industry representatives by criminal elements (e.g., through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

Money Services Businesses

The majority of ML risk scenarios illustrated in Chart 5 and involving all types of MSBs, with the exception of wholesale and corporate MSBs, are rated high to very high. Inherent risk scenarios associated with wholesale and corporate MSBs mainly fall into the medium to high range, since they offer a more limited number of products and services, predominantly EFTs and bank drafts, to a smaller clientele segment (i.e., corporations).

Chart 5

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



MSB products and services that are the most often used for money laundering and terrorist financing are international EFTs, currency exchanges and negotiable instruments (e.g., money orders). Cash transactions in this sector are very common and can therefore be used in the ML placement stage. Other products and services such as EFTs, money orders and travellers cheques can also be used in the layering stage of money laundering. Five main ML methods/techniques have been identified for the MSB sector and are further described in the following ML risk scenarios:

- Structuring or attempting to circumvent MSB record-keeping requirements;
- Attempting to circumvent MSB client identification requirements;
- Smurfing, using nominees and/or other proxies;
- Exploiting negotiable instruments; and
- Refining.

Inherent ML Risk Scenario Involving Monetary Instruments and Structuring

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

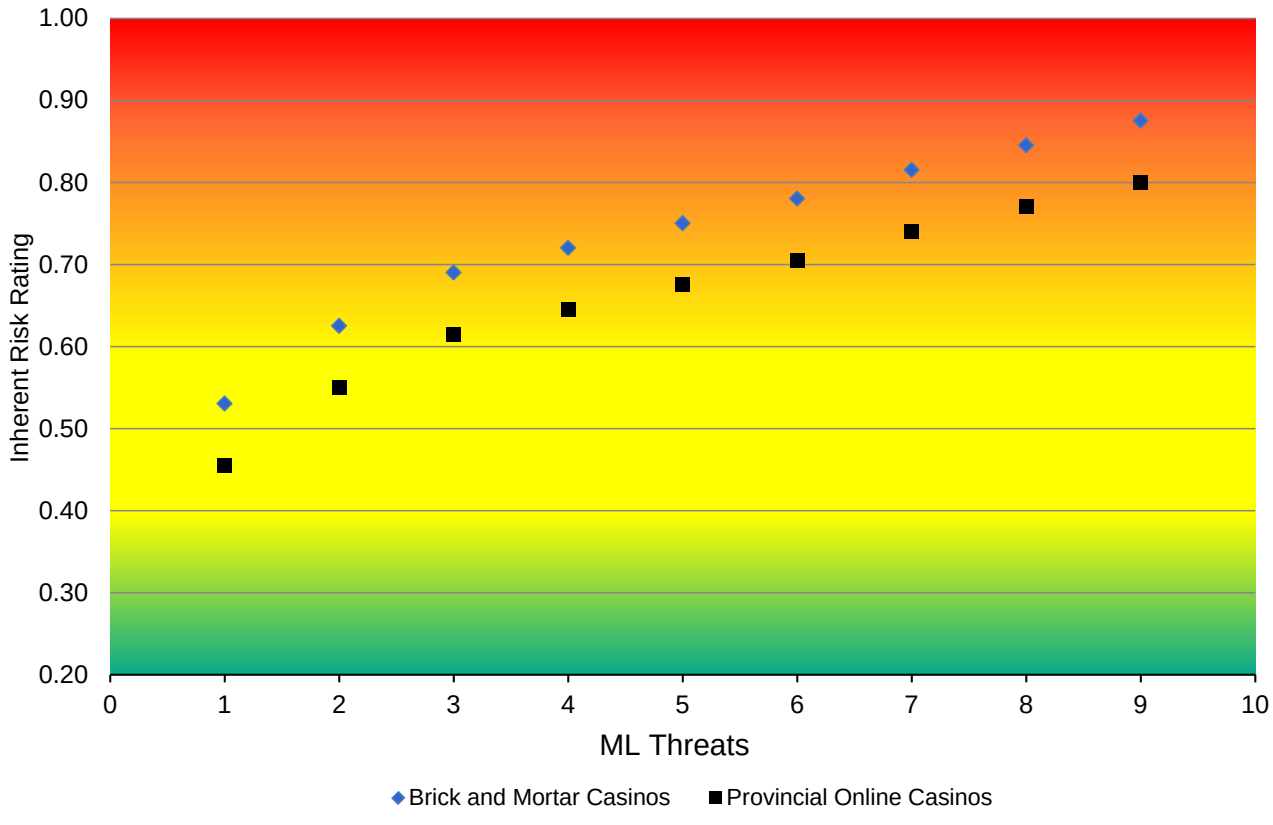
Inherent ML Risk Scenario Involving Monetary Instruments and an Attempt to Circumvent Client Identification Requirements

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

Casinos

Chart 6 illustrates the different level of ML risk scenarios involving brick and mortar and provincially regulated online casinos. Given the larger number of products and services offered to clients such as cash purchases of chips, slot machines accepting cash, currency exchanges, self-service ticket redemption machines and so on, brick and mortar casinos are exposed to higher inherent ML risk scenarios than provincially regulated online casinos.

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



Brick and Mortar Casinos

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

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

Typical Inherent ML Risk Scenario Involving Brick and Mortar Casinos

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

- Exchanges of small denomination bills for larger denomination bills at the cashier window in amounts under the reporting threshold;
- Exchanges of a large amount of small denomination bills for casino tickets, and later for large denomination bills;
- Frequent or repeated exchanges at the cashier window of a large amount of foreign currency (most often US dollars) for Canadian currency, with minimal or no gaming activity;
- Cash purchases of casino chips in amounts below the reporting threshold;
- Use of multiple cashiers to cash out casino chips in amounts below the reporting threshold;
- Passing of cash, casino chips or other casino value instrument between related OCG members prior to entering the casino, either on the casino floor, at the gaming table or prior to cashing out;
- Deposits of cash, cheque/bank draft to a front money account, followed by the purchase of casino chips, then redemption of the chips for a casino cheque, or withdrawal of all or part of the funds, with minimal or no gaming observed;
- Deposits of small denomination bills to a front money account, followed by withdrawals of the funds in higher denomination bills;
- Cash deposits by a third party to a customer's front money account;
- Credit card purchases of casino chips with minimal or no gaming and then by cash out with a casino cheque, while illicit cash was used to pay the credit card balance; and
- Casino chip purchases, using illicit cash/bank draft, payable to customers engaged in minimal or no game play and then redemption of the chips for a casino cheque.

Provincially Regulated Online Casinos

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

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

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

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

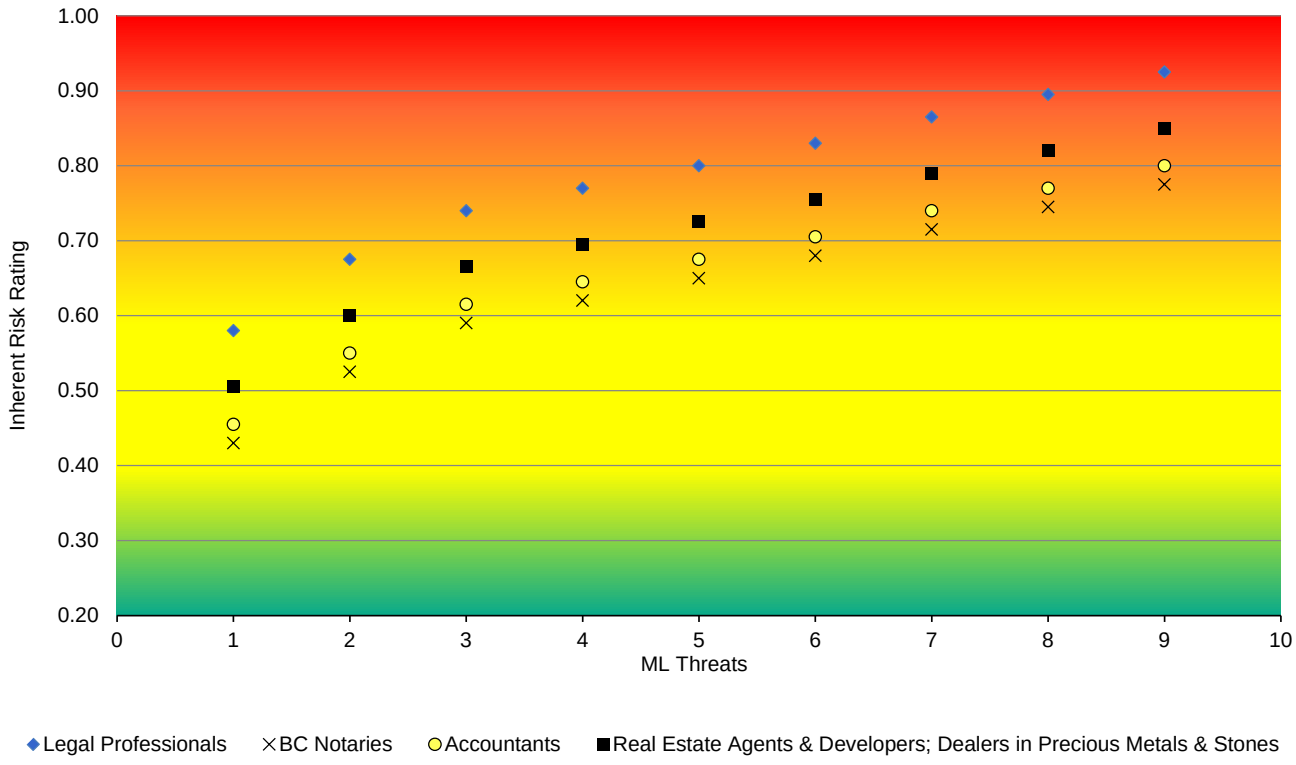
Inherent ML Risk Scenario Involving Third-Party Funding

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

Non-Financial Businesses and Professions

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

Chart 7
Inherent ML Risks Related to Non-Financial Businesses and Professions by Type of ML Threats



Legal Professionals and BC Notaries

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

Legal professionals and BC notaries may be used as intermediaries to put distance between criminal activities and the proceeds generated by those activities, and therefore to hide the source and true beneficial owners of such funds, often through complex corporate or trust structures formed with the assistance of legal professionals. This assistance also adds a veil of legitimacy to the movement of funds and other business operations.

Real Estate Sector

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

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

The associated ML techniques most often observed are as follows:

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

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

Other ML methods and techniques that allow illicit cash into the financial system include cash purchases or large cash down payments, and cash payments especially in the construction, renovation and upgrading of real estate assets. Finally, illicit foreign funds can also be used to purchase Canadian real estate properties.[88]

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

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

Dealers in Precious Metals and Stones

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

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

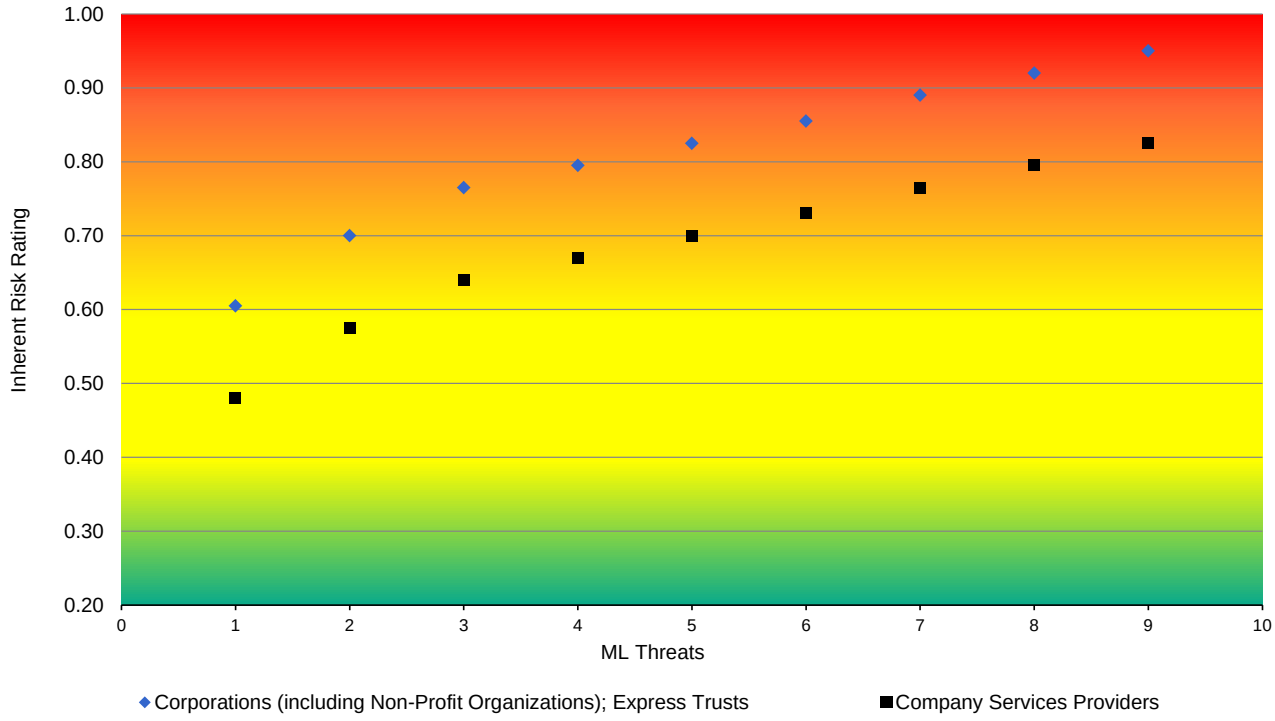
The main ML methods identified are as follows:

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

Corporations, Express Trusts and Company Services Providers

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

Chart 8
Inherent ML Risks Related to Corporations, Express Trusts and Company Services Providers by Type of ML Threats



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

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

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

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

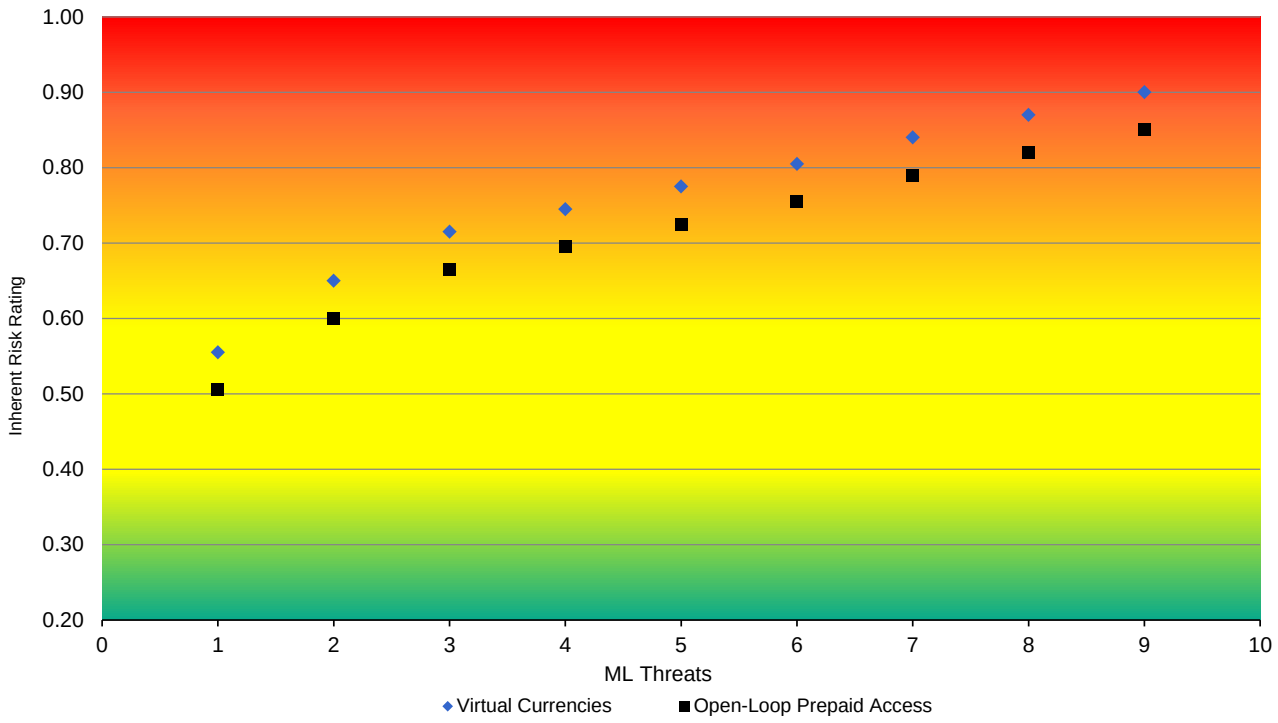
There are only a few CSPs in Canada but they are also exposed to high inherent ML risks, in particular when they are involved in managing corporations for their clients. The limited number of CSPs in Canada is likely due to the fact that provincial or federal incorporation can be done online through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

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

Selected Products Holding Monetary Value

Chart 9 illustrates the level of ML risks associated with virtual currencies and open-loop prepaid access products and services. Virtual currencies, in particular convertible ones, are mostly used in high to very high ML risk scenarios and can be used in all three stages of money laundering. Open-loop prepaid access products are also mainly used in high ML risk scenarios.

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



Virtual Currencies

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

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

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

Prepaid Access Products

Because they can be reloaded with cash and can be used in the same places that regular credit cards are accepted, open-loop prepaid access products can be used for money laundering, particularly in instances when the allowed loading limit is high. There have been specific incidents where prepaid access products, mainly open-loop ones, were suspected of being used in ML schemes in Canada:

- In 2009, law enforcement officials investigated a case which involved over 40 suspects believed to have loaded prepaid cards in another country and then used them to withdraw approximately $350,000 from ATMs in Canada.
- A Canadian Internet payment services provider and its foreign subsidiaries were suspected of laundering the proceeds of fraud. Three open-loop prepaid card providers in Canada and the U.S. were used. Funds were sent from foreign countries to the Canadian Internet payment services provider's bank accounts. The money was then loaded onto prepaid cards for layering in other countries.
- In addition, the U.S. Secret Service has observed significant cross-border movement of the proceeds of white-collar crimes and drug crimes from the United States into Western Canada through prepaid cards.

Inherent Terrorist Financing Risks

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

Table 6
Terrorist Financing Threat Groups of Actors

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

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

On the other hand, a total of 93 high TF risk scenarios were identified that involve, to varying degrees, all 19 sectors and products represented in Charts 10 to 13, and that were assessed to have a medium to very high vulnerability to terrorist financing. Seven different groups of TF threat actors rated low, medium and high have or could exploit all or some of those sectors, as further explained in the following pages.

The majority of the TF risk scenarios included in Charts 10 to 13 were rated lower than for money laundering, and with the exception of the risk scenarios referred to above and rated high or very high, most of them were rated medium.

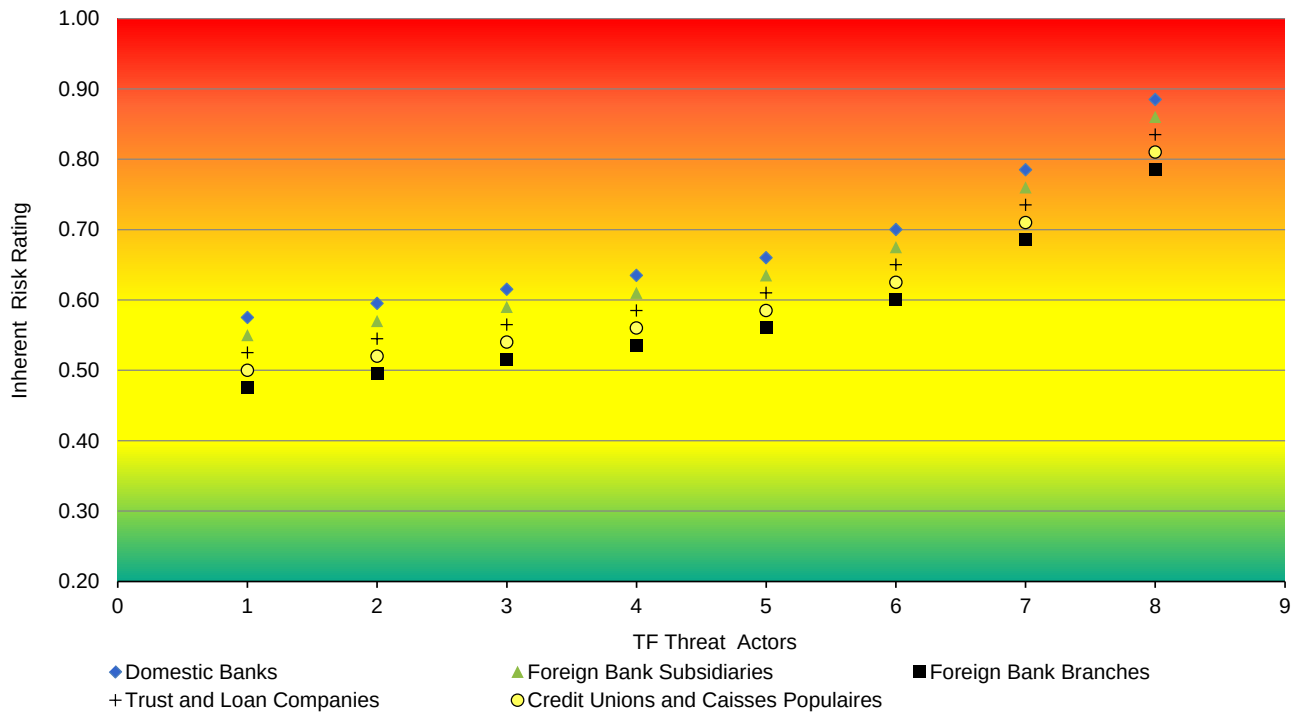
Each number (i.e., 1-8) on the horizontal axis of Charts 10 to 13 represents one group of TF threat actors associated with the different assessed terrorist groups.

Deposit-Taking Financial Institutions

Deposit-taking financial institutions included in Chart 10 are mainly used in the transmission, as well as sometimes in the aggregation, of funds suspected to be ultimately destined for terrorist groups or individuals, the majority of which are active in foreign countries. As for money laundering, but to support different goals, TF risk scenarios described below and rated medium to very high, generally involve the use of domestic wire transfers, international EFTs, monetary instruments such as bank drafts, money orders and cheques (e.g., personal, travellers), personal and business accounts, currency exchanges, trust accounts as well as loan/mortgage and credit card services.

Chart 10

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



Inherent TF Risk Scenarios Involving Deposit-Taking Financial Institutions

The majority of TF actors associated with the assessed terrorist groups are suspected of using international EFTs as one TF transmission method to send funds overseas,[90] often in high-risk jurisdictions. Individuals associated with some of those groups may also use domestic wire transfers to move funds within Canada and/or aggregate collected funds (e.g., cash or web-based[91] donations) into one or a few bank accounts (personal or business) before sending the funds overseas. This also means that cash deposits, sometimes conducted by third parties or nominees, may occur when cash donations are obtained through door-to-door solicitation or the use of donation boxes. Cash withdrawals may also occur when, for example, they need funds to pay for their airplane tickets and/or for their terrorist-related expenses. Other TF methods involve the use of monetary instruments and commingling of illicit funds[92] with legitimate business revenue in Canada.

Other inherent TF risk scenarios may involve the use of fraudulent loans to raise funds, while email money transfers may be used for the transmission of funds. Credit card fraud, including bust-out schemes[93] and card skimming, have been used by some TF actors. Business accounts and, in some instances, trust accounts, are also suspected of being used to hide the true source or beneficial owner of funds destined for terrorist activity. Finally, some TF risk scenarios may involve trade-based schemes or the use of businesses as fronts, and therefore would involve the domestic or international movement of funds into and out of business accounts.

Money Services Businesses

As for deposit-taking financial institutions, the products and services offered by MSBs such as currency exchanges, domestic wire transfers, international EFTs and money orders are often used in TF risk scenarios (rated medium to very high) involving the majority of TF actors associated with the assessed terrorist groups. Although all types of MSBs illustrated in Chart 11 can be exploited for TF activities, it is suspected that national full-service, small independent and smaller retail MSBs are most often used. This is mainly due to the fact that national full-service MSBs operate globally and offer money transfer services to multiple foreign jurisdictions, while smaller retail MSBs offering currency exchanges, domestic wire transfers and international EFT services are typically agents of national full-service MSBs. Operators of small independent MSBs may have ethno-cultural or familial links to some foreign jurisdictions and possibly links to informal money value transfer operators (e.g., hawalas). Some of the jurisdictions where funds are sent to or received from may be considered high-risk due to ongoing conflicts and/or the presence of terrorist organizations or other factors.

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

---

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

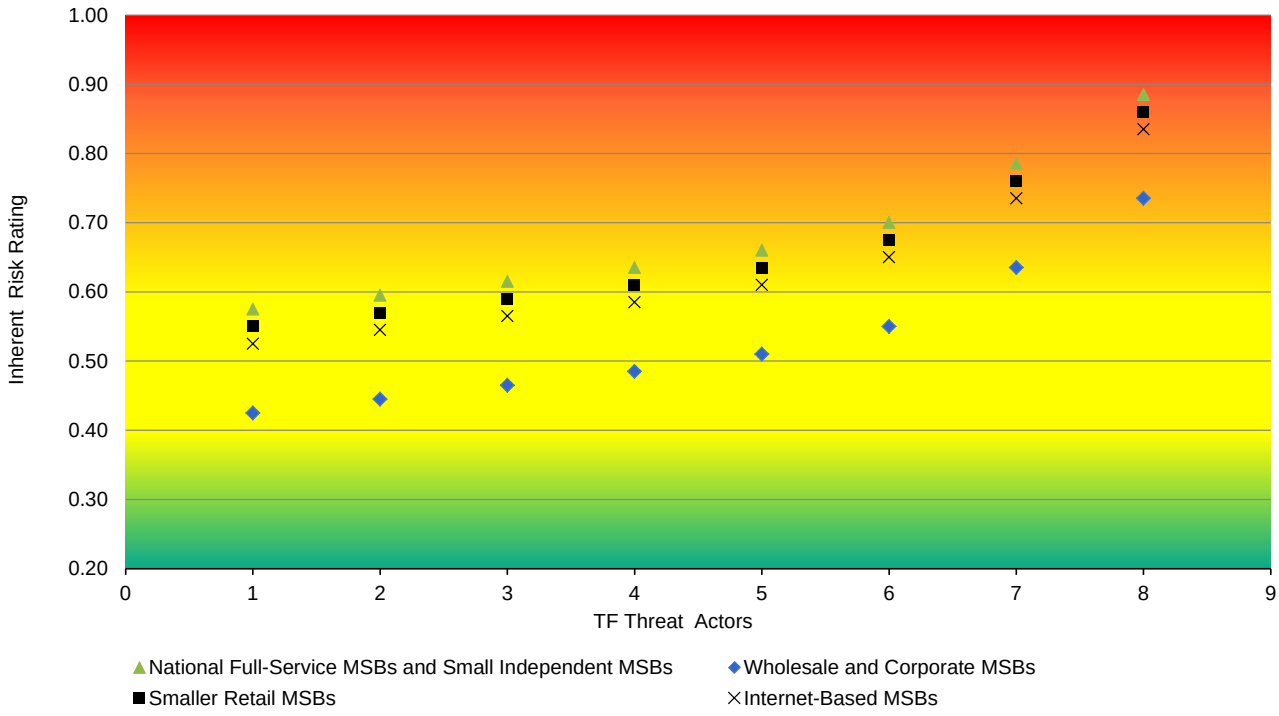
[91] Some TF actors are suspected of having used or are still using websites or social media tools (e.g., Facebook, Twitter) to raise funds, and such activity sometimes involves crowd funding (i.e., multiple donors contributing funds for the same cause or the same individual). Mobile payment systems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

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

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

Chart 11

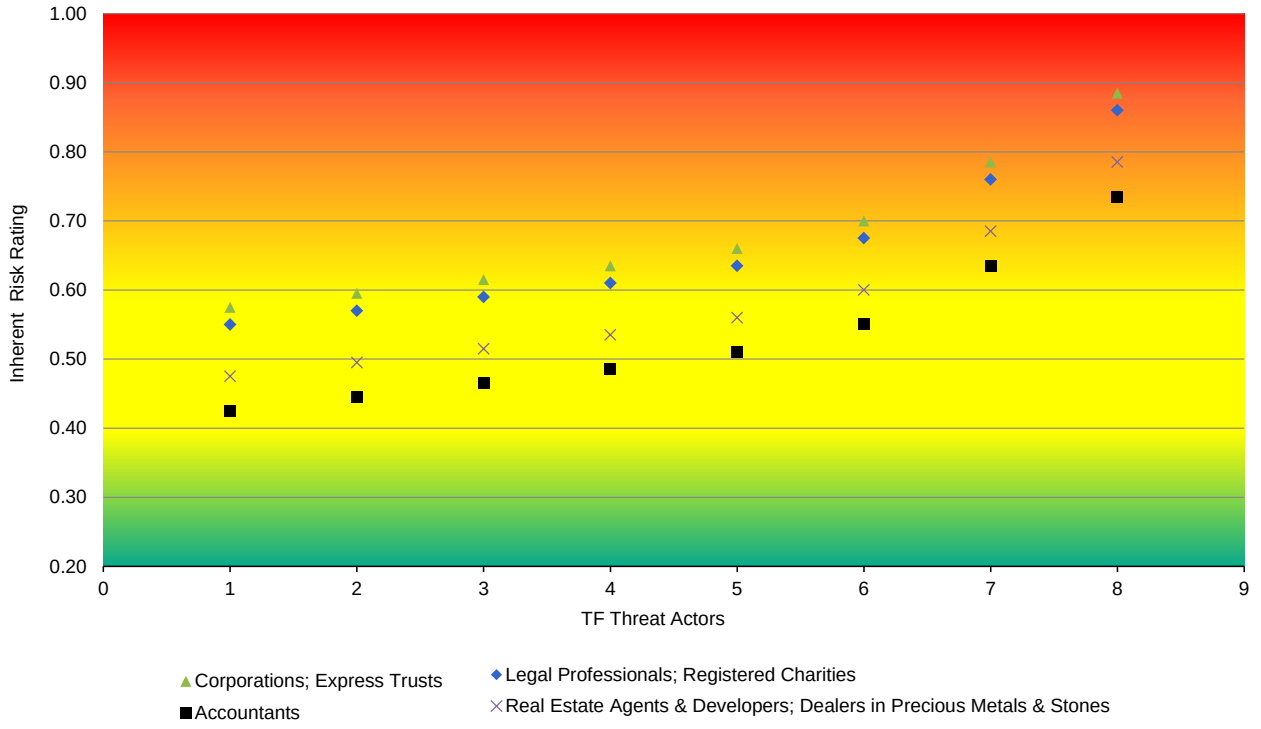
Inherent TF Risks in the Money Services Businesses Sector by TF Threat Actors



Express Trusts and Non-Financial Businesses and Professions

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

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



Corporations

Corporations, particularly private ones, are used in TF risk scenarios as fronts to move funds destined for terrorist groups or individuals, or to commingle illicit funds with legitimate business revenue or to use in trade-based schemes. Generally, corporations involved in TF schemes have been from the food, import/export, shipping/freight, automobile, general contracting/labour, real estate, travel, telecommunications, textile and trading industries. In addition, in the broader context of terrorist resourcing, the procurement of goods is also considered a form of terrorist financing and could involve various types of corporations. Most TF actors associated with the assessed terrorist groups use businesses in some TF schemes.

Legal Professionals and Accountants

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

Registered Charities

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

Inherent TF Risk Scenarios Involving Charities

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

- Diversion of funds—an organization, or an individual acting on behalf of an organization, diverts funds to a known or suspected terrorist entity;
- Affiliation with terrorist entity—an organization, or an individual acting on behalf of an organization, maintains operational affiliation with a terrorist organization or supporter of terrorism, putting it at risk of abuse for purposes including general logistical support to the terrorist entity;
- Abuse of programming—organization-funded programs meant to support legitimate humanitarian purposes are manipulated at the point of delivery to support terrorism;
- Support of recruitment—organization-funded programs or facilities are used to create an environment which supports and/or promotes terrorism recruitment-related activities; and
- False representation and sham organizations—under the guise of charitable activity, an organization or individual raises funds, promotes causes and/or carries out other activities in support of terrorism.

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

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

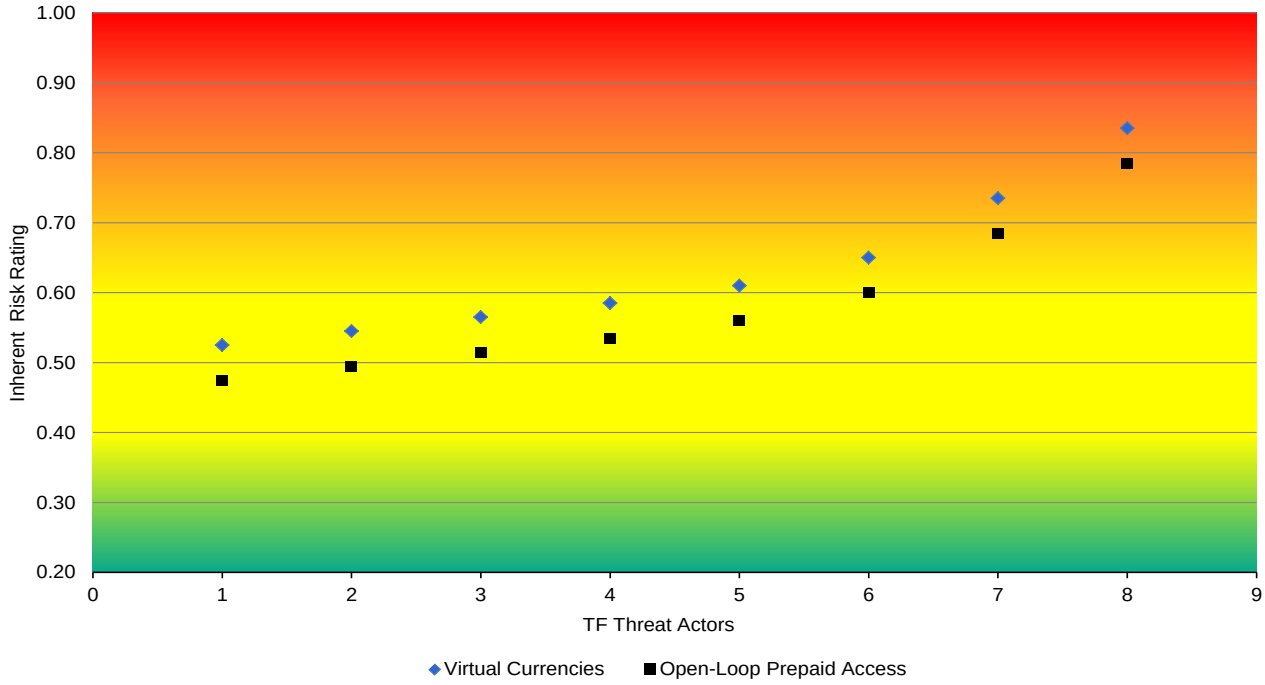
Dealers in Precious Metals and Stones

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

Virtual Currencies and Open-Loop Pre-Paid Access

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

Chart 13
Inherent TF Risks Related to Products Holding Monetary Value by TF Threat Actors



Next Steps

This risk assessment is an analysis of Canada's current situation and represents a key step forward in providing the basis for the AML/ATF regime to promote a greater shared understanding of inherent ML/TF risks in Canada. The assessment will help to continue to enhance Canada's AML/ATF regime, further strengthening the comprehensive approach it already takes to risk mitigation and control domestically, including with the private sector and with international partners.

The Government of Canada expects that this report will also be used by financial institutions and other reporting entities to contribute to their understanding of how and where they may be most vulnerable and exposed to inherent ML/TF risks. FINTRAC and OSFI will include relevant information related to inherent risks in their respective guidance documentation to assist financial institutions and other reporting entities in integrating such information in their own risk assessment methodology and processes so that they can effectively implement controls to mitigate ML/TF risks. Members of the oversight of the regime will also use the results of the risk assessment to inform policy and operations as part of the ongoing efforts to combat money laundering and terrorist financing.

Annex: Key Consequences of Money Laundering and Terrorist Financing

Social Consequences

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

Economic Consequences

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

Political Consequences

- Eroding of public institutions and the rule of law
- Greater perceived attractiveness for illicit ML/TF activities ("safe haven")
- Loss of credibility and influence internationally
- Lower government revenues
- Negative public perception in the government's ability to deal with ML/TF activity (weak on crime)

Glossary

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

List of Key Acronyms and Abbreviations

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

Terrorist Groups

AQ	Al Qaeda
AQAP	Al Qaeda in the Arabian Peninsula
AQIM	Al Qaeda in the Islamic Maghreb
AS	Al Shabaab
Hamas	Harakat al-Muqawama al-Islamiyya
ISIS	Islamic State in Iraq and Syria
LTTE	Liberation Tigers of Tamil Eelam
JN	Jabhat Al-Nusra

Appendix C:

Canada, Parliament, House of Commons, Standing Committee on Finance, *Confronting Money Laundering and Terrorist Financing: Moving Canada Forward, Report of the Standing Committee on Finance* 42nd Parl, 1st Sess (November 2018) (Chair: Wayne Easter).

HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

CONFRONTING MONEY LAUNDERING AND TERRORIST FINANCING: MOVING CANADA FORWARD

Report of the Standing Committee on Finance

The Honourable Wayne Easter, Chair

NOVEMBER 2018
42nd PARLIAMENT, 1st SESSION

Appendix C

CONFRONTING MONEY LAUNDERING AND TERRORIST FINANCING: MOVING CANADA FORWARD

Report of the Standing Committee on Finance

Hon. Wayne Easter
Chair

NOVEMBER 2018

42nd PARLIAMENT, 1st SESSION

NOTICE TO READER

Reports from committee presented to the House of Commons

Presenting a report to the House is the way a committee makes public its findings and recommendations on a particular topic. Substantive reports on a subject-matter study usually contain a synopsis of the testimony heard, the recommendations made by the committee, as well as the reasons for those recommendations.

STANDING COMMITTEE ON FINANCE

CHAIR

Hon. Wayne Easter

VICE-CHAIRS

Hon. Pierre Poilievre
Peter Julian

MEMBERS

Greg Fergus
Peter Fragiskatos
Tom Kmiec
Joël Lightbound (Parliamentary Secretary — Non-Voting Member)
Michael V. McLeod
Jennifer O'Connell (Parliamentary Secretary — Non-Voting Member)
Blake Richards
Kim Rudd
Deborah Schulte (Parliamentary Secretary — Non-Voting Member)
Francesco Sorbara

OTHER MEMBERS OF PARLIAMENT WHO PARTICIPATED

Dan Albas
Gary Anandasangaree
Blaine Calkins
Pierre-Luc Dusseault
Julie Dzerowicz
Mark Gerretsen
Raj Grewal
Angelo Iacono
Majid Jowhari
Pat Kelly
Kamal Khera
Wayne Long

Karen Ludwig
Richard Martel
Brian Masse
Kelly McCauley
Phil McColeman
Mary Ng
Hon. Erin O'Toole
Michel Picard
Sherry Romanado
Jean R. Rioux
Don Rusnak
Ruby Sahota
Raj Saini
Brad Trost
Dave Van Kesteren
Len Webber

CLERKS OF THE COMMITTEE

David Gagnon
Alexandre Jacques

LIBRARY OF PARLIAMENT

Parliamentary Information and Research Service

Andrew Barton, Analyst
Brett Capstick, Analyst
Michaël Lambert-Racine, Analyst

THE STANDING COMMITTEE ON FINANCE

has the honour to present its

TWENTY-FOURTH REPORT

Pursuant to its mandate under Standing Order 108(2), the Committee has studied the *Proceeds of Crime and Terrorist Financing Act* and has agreed to report the following:

TABLE OF CONTENTS

LIST OF RECOMMENDATIONS 1

STATUTORY REVIEW OF THE PROCEEDS OF CRIME (MONEY LAUNDERING) AND TERRORIST FINANCING ACT 9

INTRODUCTION 9

CHAPTER 1: LEGISLATIVE AND REGULATORY GAPS 13

A. Beneficial Ownership 13

(i) Background 13

(ii) Witness Testimony 16

B. Politically Exposed Persons 18

(i) Background 18

(ii) Witness Testimony 19

C. The Legal Profession 20

(i) Background 20

(ii) Witness Testimony 21

D. White Label Automated Teller Machines 23

(i) Background 23

(ii) Witness Testimony 23

E. The Real Estate Sector and Alternative Mortgage Lenders 24

(i) Background 24

(ii) Witness Testimony 24

F. Structuring to Avoid Reporting 25

(i) Background 25

(ii) Witness Testimony 26

G. Armoured Cars 26

(i) Background 26

(ii) Witness Testimony 26
H. High-Value Goods Dealers and Auction Houses 26
(i) Background 26
(ii) Witness Testimony 26
I. Securities Dealers 27
(i) Background 27
(ii) Witness Testimony 28

CHAPTER 2: THE EXCHANGE OF INFORMATION AND PRIVACY RIGHTS OF CANADIANS 33
A. Information Sharing and Retention Within Government 33
(i) Background 33
(ii) Witness Testimony 35
B. Information Sharing and Retention Between the Government and the Private Sector 36
(i) Background 36
(ii) Witness Testimony 38
C. Information Sharing and Retention Within the Private Sector 39
(i) Background 39
(ii) Witness Testimony 41
D. Information Sharing and De-Risking 42
(i) Background 42
(ii) Witness Testimony 42

CHAPTER 3: STRENGTHENING INTELLIGENCE CAPACITY AND ENFORCEMENT ... 45
A. Prosecution and Legal Standards 45
(i) Background 45
(ii) Witness Testimony 46
B. Bulk Cash and Bearer Instruments 47
(i) Background 47
(ii) Witness Testimony 48

C. Geographic Targeting Orders 49
(i) Background 49
(ii) Witness Testimony 50
D. Trade Transparency Units 50
(i) Background 50
(ii) Witness Testimony 50
E. Compliance and Enforcement Measures 51
(i) Background 51
(ii) Witness Testimony 52

CHAPTER 4: MODERNIZING THE REGIME 55
A. Virtual Currency and Money Service Businesses 55
(i) Background 55
(ii) Witness Testimony 57
B. Compliance and the Administrative Burden 60
(i) Background 60
(ii) Witness Testimony 60
C. Suspicious Transaction Reporting 62
(i) Background 62
(ii) Witness Testimony 62
D. Sanctions Lists 63
(i) Background 63
(ii) Witness Testimony 64

APPENDIX A: LIST OF WITNESSES 67

APPENDIX B: LIST OF BRIEFS 73

REQUEST FOR GOVERNMENT RESPONSE 75

DISSENTING OPINION OF THE NEW DEMOCRATIC PARTY OF CANADA 77

LIST OF RECOMMENDATIONS

As a result of their deliberations committees may make recommendations which they include in their reports for the consideration of the House of Commons or the Government. Recommendations related to this study are listed below.

Chapter 1 Recommendations

Recommendation 1

That the Government of Canada work with the provinces and territories to create a pan-Canadian beneficial ownership registry for all legal persons and entities, including trusts, who have significant control which is defined as those having at least 25% of total share ownership or voting rights.

- **Such a registry should include details such as names, addresses, dates of birth and nationalities of individuals with significant control.**

- **The registry should not be publicly accessible, but it can be accessed by certain law enforcement authorities, the Canada Revenue Agency, Canadian Border Services Agency, FINTRAC, authorized reporting entities and other public authorities.**

- **To ensure that the registry is accurate and properly performing its function, it should have the capability to follow up on information submitted to it.**

- **The registry should take into account the best practices and lessons learned from other jurisdictions. In particular, the Committee was interested in the United Kingdom's dual system of registration, which can be done through a legal professional or through direct online registration, as seen in the U.K.'s Companies House.**

- **Authorities should be granted appropriate powers to apply proportionate and dissuasive sanctions for failure to fully comply in the prescribed time frame.**

- **Beneficial owners of foreign companies that own property in Canada should be included in such a registry.**

- **That subject to Canadian law, requests by foreign governments for information sharing under a Canadian beneficial ownership registry should be considered by the Government of Canada, in cases where tax treaties or other lawful agreements or protocols exist for potential or existing money laundering, terrorist financing or criminal activity.....29**

Recommendation 2

That the Government of Canada review, refine, and clarify through training, the statutory definition of politically exposed persons (PEP). In particular, the notion of 'association with a PEP' under this definition creates ambiguity and inconsistency among institutions in regards to who exactly constitutes a PEP.....29

Recommendation 3

That the Government of Canada move to a risk-based model of compliance for politically exposed persons, softening the requirements for those with transparent and unsuspicious financial portfolios. 29

Recommendation 4

Given that the legal professions in the U.K. are subject to the same AML/ATF reporting requirements as other reporting entities in all non-litigious work that is performed, the Government of Canada and the Federation of Law Societies should adopt a model similar to the U.K.'s Office of Professional Body Anti-Money Laundering Supervision.

- **The Government of Canada request Reference from the Supreme Court of Canada as to whether solicitor-client privilege exists when a client requests advice on how to either launder money or structure finances for the purposes of illegal activity. 29**

Recommendation 5

That the Government of Canada bring the legal profession into the AML/ATF regime in a constitutionally compliant way with the goal of ensuring that the Canadian standards set by the PCMLTFA protect against money laundering and terrorist financing. 30

Recommendation 6

That the Government of Canada consider implementing a body similar to the U.K.'s Office of Professional Body Anti-Money Laundering Supervision with respect to Canadian self-regulated professions. 30

Recommendation 7

That the Government of Canada amend the PCMLTFA so that the armoured car and white label ATM sector be subject the AML/ATF regime, as is the case in the United States and the province of Quebec, respectively. 30

Recommendation 8

That the Government of Canada amend the PCMLTFA to require all reporting entities, including designated non-financial businesses and professions, such as the real estate sector (brokers and lenders), that are now exempt from the obligation of identifying beneficial ownership, to do the following:

- **determine and verify the identity of the beneficial owners;**
- **determine if their customers are politically exposed persons, or if they are the family members or associates of politically exposed person;**
- **prohibit opening accounts or completing financial transactions until the beneficial owner has been identified and their identity verified with government-issued identification.**

***Consideration of the above should also be applied to foreign beneficial owners.....30**

Recommendation 9

That the Government of Canada amend the PCMLTFA to extend the requirements for real estate brokers, sales representatives and developers to mortgage insurers, land registry and title insurance companies. 30

Recommendation 10

That the Government of Canada make it a criminal offence for an entity or individual to structure transactions in a manner designated to avoid reporting requirements. These provisions would be modeled on Title 31 of U.S. code section 5324. 31

Recommendation 11

That the Government of Canada require companies selling luxury items to be subject to reporting requirements under the PCMLTFA and report large cash transactions to FINTRAC if those transactions are not already reported through other means. 31

Recommendation 12

That the Government of Canada amend Canadian privacy laws with the sole purpose of permitting security regulators to fully and appropriately examine the professional record of conduct of security dealers and their employees. 31

Recommendation 13

That the Government of Canada develop a national view of AML by partnering with provinces and territories to train local regulators on best practices in order to prevent securities firms from being overlooked. 31

Chapter 2 Recommendations

Recommendation 14

That the Government of Canada examine the U.S. Government's "third agency rule" for information sharing and determine whether this rule would assist in investigation / detection of money laundering and terrorist financing in Canada.....43

Recommendation 15

That the Government of Canada expands FINTRAC's mandate to allow for:

- **a greater focus on building actionable intelligence on money laundering and terrorist financing, akin to FinCEN in the United States, and provide FINTRAC with the necessary resources to effectively undertake the corresponding analysis;**

- **the retention of data for 15 years;**

- **an operational model to allow for two-way information sharing system (rather than strictly being an information gathering system);**

    - **FINTRAC should be able to share feedback, best practices and long-term trends, so that reporting entities can properly assist FINTRAC.**

- **the ability to request more information from specific reporting agencies to clarify reported suspicious activity or to build a stronger case before referring it to law enforcement;**

- **the ability to release aggregated data, subject to Canadian law, about a group of specific reporting agencies or a sector for statistical, academic or government purposes. 44**

Recommendation 16

That the Government of Canada establish a round table partnership with industry leaders who are investing significantly in technology that more efficiently tracks suspicious activities and transactions, so as to promote best industry practices. 44

Recommendation 17

That the Government of Canada take steps to emulate the U.K.'s model of a Joint Money Laundering Intelligence Taskforce in Canada.....44

Recommendation 18

That the government of Canada consider tabling legislation that would allow information that is limited to AML/ATF subject matter to be shared between federally regulated financial institutions such as banks and trust companies, provided that FINTRAC is notified upon each occurrence of such sharing. 44

Recommendation 19

That the Government of Canada implement the necessary requirements to banking to determine a "low-risk threshold" and establish exemptions to ensure the most vulnerable Canadians are not being denied a bank account due to lack of adequate identification. 44

Chapter 3 Recommendations

Recommendation 20

The Committee recommends, in recognizing the difficulty prosecutors have in laying money-laundering charges due to the complexity of linking money laundering to predicate offences, that the Government of Canada:

- **bring forward Criminal Code and Privacy Act amendments in order to better facilitate money laundering investigations;**

- **any necessary resources be made available to law enforcement and prosecutors to pursue money-laundering and terrorism financing activities 53**

Recommendation 21

That the Government of Canada expand FINTRAC oversight to ensure that all casino operators, employees, and frontline gaming personnel are trained in anti-money laundering legislation. 54

Recommendation 22

That the Government of Canada establish an information sharing regime through FINTRAC and provincial gaming authorities to ensure more accurate and timely reporting. 54

Recommendation 23

That the Government of Canada amend the PCMLTFA to enable law enforcement agencies to utilize geographic targeting orders similar to those used in the United States.

- **Federal, provincial, and territorial governments should collaborate to close the loophole regarding the transaction of sales between parties who are not subject to PCMLTFA reporting requirements, which creates vulnerability for money laundering to occur.....54**

Recommendation 24

That the Government of Canada follow the example of the Netherlands, which gives holders of bearer shares – now prohibited – a fixed period of time to convert them into registered instruments before they are deemed void.....54

Chapter 4 Recommendations

Recommendation 25

That the Government of Canada regulate crypto-exchanges at the point that fiat currency is converted so as to establish these exchanges as money service businesses (MSB). 64

Recommendation 26

That the Government of Canada establish a regulatory regime for crypto-wallets so as to ensure that proper identification is required, and that true ownership of wallets is known to the exchanges and law enforcement bodies if needed.

- **Ensure that bitcoin purchases of real estate and cash cards are properly tracked and subjected to AML regulation;**

- **Law enforcement bodies must be able to properly identify and track illegal crypto-wallet hacking and failures to report capital gains. 64**

Recommendation 27

That the Government of Canada establish a license for crypto-exchanges in line with Canadian law, which includes an anti-money laundering program and look to the State of New York's program as a model for best practices. 64

Recommendation 28

That the Government of Canada consider prohibiting nominee shareholders. However, if nominee shareholders are permitted, they should be required to disclose their status upon the registration of the company and registered as nominees. Nominees should be licensed and subject to strict anti-money laundering obligations. 65

Recommendation 29

That the Government of Canada include clearer directions and streamline the reporting structure of Suspicious Transaction Reports, such as through the use of 'drop-down boxes,' to increase ease of use by specific reporting entities and ensure better compliance. 65

Recommendation 30

That the Government of Canada change the structure of FINTRAC's Suspicious Transaction Report to resemble the Suspicious Activity Reports used in the United Kingdom and the United States in order to focus on suspected violations rather than an arbitrary monetary threshold. 65

Recommendation 31

That the Government of Canada enhance the direct reporting system of casinos to FINTRAC through the suspicious transaction reports to include suspicious activities. 65

Recommendation 32

That the Government of Canada update reporting regulations for financial institutions to include bulk online purchasing of store gift cards or prepaid credit cards. 65

HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

STATUTORY REVIEW OF THE PROCEEDS OF CRIME (MONEY LAUNDERING) AND TERRORIST FINANCING ACT

INTRODUCTION

On 31 January 2018, the House of Commons Standing Committee on Finance (the Committee) adopted the following motion:

> That, pursuant to the motion adopted by the House on Monday, January 29, 2018, the Committee undertake a statutory review of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*….

Pursuant to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA), a review must be conducted by a committee of the House of Commons, of the Senate or of both Houses every five years. From 8 February to 20 June 2018, the Committee held 14 hearings on this review in Ottawa. In addition, from 1 to 8 June 2018, a delegation from the Committee traveled to Toronto, London United Kingdom (U.K.), Washington D.C. and New York City (the Committee's travels) to examine the methods and best practices of other jurisdictions in their efforts to address money laundering and terrorist financing, as well as discuss Canada's performance in these areas. In total, 71 groups or individuals made public presentations to the Committee over the course of this review.

Laundering the proceeds of crime (money laundering) is a criminal offence under section 462.31(1) of the *Criminal Code*, which details that:

> Every one commits an offence who uses, transfers the possession of, sends or delivers to any person or place, transports, transmits, alters, disposes of or otherwise deals with, in any manner and by any means, any property or any proceeds of any property with intent to conceal or convert that property or those proceeds, knowing or believing that all or a part of that property or of those proceeds was obtained or derived directly or indirectly as a result of
>
> - the commission in Canada of a designated offence; or
> - an act or omission anywhere that, if it had occurred in Canada, would have constituted a designated offence.

HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

In essence, money laundering is the process used to disguise the source of money or assets derived from criminal activity.

Canada's anti–money laundering regime was formally established in 2000 under the National Initiative to Combat Money Laundering. The *Proceeds of Crime (Money Laundering) Act* was adopted that year and created a mandatory reporting system for suspicious financial transactions, large cross-border currency transfers and certain prescribed transactions. The legislation also established the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) with a mandate to ensure compliance of reporting entities, to collect and analyze financial transaction reports, and to disclose pertinent information to law enforcement and intelligence agencies. In December 2001, the *Proceeds of Crime (Money Laundering) Act* was amended to include measures to address terrorist financing and was renamed the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, which formally created Canada's Anti-Money Laundering and Anti–Terrorist Financing Regime (AML/ATF regime) and fulfilled Canada's obligations under the *United Nations International Convention for the Suppression of the Financing of Terrorism*.

FINTRAC defines terrorist financing as the act of providing funds for terrorist activity. This may involve funds raised from legitimate sources such as donations from individuals, businesses and/or charitable organizations that are otherwise operating legally. Or it may involve funds from criminal sources such as the drug trade, the smuggling of weapons and other goods, fraud, kidnapping and extortion.[1]

The regime seeks to detect and deter money laundering and terrorist financing, and aims to facilitate their investigation and prosecution. The Act pursues these objectives in three main ways: by establishing record keeping and client identification standards, by requiring reporting from financial intermediaries, and by putting FINTRAC in place to oversee its compliance.

In view of the current five-year review of the Act, on 7 February 2018 the Department of Finance published a discussion paper entitled Reviewing Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime (the Discussion Paper), which the outline of this report mirrors. This report examines the regime's legislative and regulatory gaps, the exchange of information and the privacy of Canadians, ways of strengthening intelligence capacity and enforcement measures, as well as the modernization of the regime.

1 A terrorist activity financing offence is an offence under section 83.02, 83.03 or 83.04 of the *Criminal Code* or an offence under section 83.12 arising out of a contravention of section 83.08 (Freezing of Property). "Terrorist activity" is defined in section 83.01(1) of the *Criminal Code*.

With respect to the Committee's travels from 1 to 8 June 2018, various witnesses testified to the Committee under Chatham house rules to encourage openness and the frank sharing of information.[2] The testimony of these witnesses is therefore presented in this report in a manner that does not identify the source of the testimony.

2 Under Chatham House Rule, participants in a meeting are free to use the information received, so long as testimony is not attributed to any particular participant.

CHAPTER 1: LEGISLATIVE AND REGULATORY GAPS

The Discussion Paper identified a number of legislative and regulatory gaps in the regime that witnesses provided comments on; in particular, witnesses provided suggestions with respect to:

- beneficial ownership,
- politically exposed persons,
- the legal profession,
- white label automated teller machines,
- the real estate sector and alternative mortgage lenders,
- structuring to avoid reporting,
- armoured cars,
- high-value goods dealers and auction houses, and
- securities dealers.

A. BENEFICIAL OWNERSHIP

(i) Background

In contrast to a "legal owner" – who holds legal title to a property or asset in his/her own name – a "beneficial owner" is an individual who possess certain benefits of ownership over a property or asset irrespective of appearing on its legal title. For example, individuals or groups of individuals who are not the legal owners of a corporation might directly or indirectly have the power to vote or influence the actions of that company and may therefore be considered its beneficial owners. In general, legal ownership is recorded and easily determined by the government and/or law enforcement, while information pertaining to beneficial ownership is more difficult to collect or obtain.

HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Beneficial ownership is connected to the regime as the perpetrators of money laundering and/or terrorist financing may obscure their identities through their beneficial ownership of an entity, such as a "shell corporation" or other legal arrangements.[3]

Under the Act's regulations, a "beneficial owner" is the actual persons who directly or indirectly owns or controls 25% or more of entities such as corporations and trusts. Beneficial owners cannot be another corporation or entity; they must be a natural person.

In the United Kingdom (U.K.), all companies and limited liability partnerships operating in that jurisdiction are required to provide Companies House – an executive agency under the U.K.'s Department for Business, Energy & Industrial Strategy – with certain information with respect to individuals who can influence or control a company, referred to as "persons with significant control" (PSCs). PSCs can also be referred to as the "beneficial owners" of a company and are defined as those having at least 25% of total share ownership or voting rights in the corporation. This PSC register includes details such as the names, addresses, dates of birth and nationalities of the PSCs. The information of the PSC must be confirmed by the company and are made publicly available apart from their home addresses and full dates of birth.[4] Corporations may apply for an exemption from having their PSCs listed publicly for a limited number of reasons, such as to prevent activists from targeting the PSCs, but this information will still be accessible to law enforcement.

In the United States, beneficial ownership is also defined using the 25% share ownership threshold, and designated financial institutions are required to – at minimum – apply the same customer identification verification requirements to the beneficial owners of corporate clients as they would to their non-corporate clients.[5] While the Financial Crimes Enforcement Network (FinCEN) – the U.S. financial intelligence agency – ultimately decided on the 25% share ownership threshold for beneficial ownership, it noted in a clarification statement that certain stakeholders argued in favour of a 10% ownership threshold in their own determination of beneficial owners, and that setting the threshold at such a percentage would be appropriate.

On 19 April 2018, the European Parliament adopted the European Commission's proposal for a Fifth Anti-Money Laundering Directive (AMLD5) to prevent terrorist

3 A "shell corporation" is one that does not actively engage in business activities, but may be used for legitimate business purposes.

4 Companies House publishes various guidance documents concerning this registrar, including a summary guide for the registration of a company's PSCs.

5 See: FinCEN, *Frequently Asked Questions Regarding Customer Due Diligence Requirements for Financial Institutions*, 3 April 2018.

financing and money laundering through the European Union's financial systems. AMLD5 proposes that the share ownership threshold for beneficial ownership would be reduced to 10% for companies that present a real risk of being used for money laundering and tax evasion.

A "trust" is a legal instrument under which an individual transfers legal ownership of his/her assets to a trustee, who will hold those assets for the benefit of anyone named by the transferor. The individual who transfers their assets to a trustee is no longer the legal owner of those assets, and any individual(s) named as a beneficiary of those assets under the trust will be the beneficial owner of them.

With respect to the European Union (EU), in May 2015 the European Commission adopted the Fourth Anti-Money Laundering Directive (AMLD4) which requires all member states to create beneficial ownership registries for all legal persons and entities, including trusts. Under the AMLD4, companies, legal entities and others – such as trustees of express trusts – will be required to collect and disclose to their governments adequate, accurate, and current beneficial ownership information. Each Member State is required to create a central registry of beneficial ownership information that is accessible – at a minimum – to competent authorities, financial intelligence units and certain specified entities when carrying out customer due diligence measures, as well as those who can demonstrate a "legitimate interest" in the information. The AMLD4 also imposed registration and customer due diligence requirements on "obliged entities," which it defined as banks and other financial and credit institutions.

In addition to operating the registry of domestic corporate beneficial ownership, the U.K. government recently announced that Companies House will begin operating a public registry of the beneficial owners of foreign companies that own property in the U.K. in 2021. The U.K. government published draft legislation for such a registry on 23 July 2018, as well as an overview document – which sets out the way in which the register is intended to work – and an impact assessment of the proposed legislation. In brief, the draft legislation proposes a public registry of the beneficial owners of all corporations, partnerships or other entities that are governed by the law of any jurisdiction outside the U.K. that owns or seeks to own U.K property. These entities will be required to take reasonable steps to ascertain and list their beneficial owners, and if such information is not ascertainable, they would instead be required to provide information about their managing officers. Failure to comply with the registry could result in fines, imprisonment, or the inability to buy, sell or lease U.K property.

HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

With respect to trust arrangements (trusts),[6] the U.K. requires all trusts that pay or owe tax to be registered with HM Revenue and Customs (HMRC). This registry contains the name, address, date of birth and National Insurance number or passport number of any individuals who are beneficiaries under the trust. The trust registry is not publicly accessible, but it can be accessed by certain law enforcement authorities and the HMRC.[7]

Within Canada, certain corporate information is collected and subsequently made publicly accessible when a business is incorporated, including the names and addresses of the corporation's directors. Business operating in Canada can choose to incorporate federally under the *Canada Business Corporations Act* (CBCA) or under the provincial regime in which the business operates, such as under Ontario's *Business Corporations Act*. This corporate information is kept by the jurisdiction under which the incorporation took place. Corporations Canada keeps the registry of federally incorporated businesses. In the United States, businesses may similarly choose to incorporate at the federal or state level, and are not required to disclose beneficial ownership information during the incorporation process. Both Canada and the U.S. therefore do not currently operate beneficial ownership registries.

As announced on 11 December 2017, the federal and provincial ministers of Finance have agreed to pursue legislative amendments to federal, provincial and territorial corporate statutes to ensure corporations hold accurate and up-to-date information on beneficial owners, and that such information will be available to law enforcement, tax and other authorities. The goal of the agreement is to bring these changes into force by 1 July 2019.

(ii) Witness Testimony

With respect to a publicly accessible and centrally operated registry of corporate beneficial ownership information, Mora Johnson, and Vanessa Iafolla – who appeared as individuals – and the Federation of Law Societies of Canada, Canadians for Tax Fairness, and Transparency International Canada, recommended that Canada create such a registry. Furthermore, various witnesses identified the need to expand the mandate of such a registry to collect additional data, including information for other legal arrangements and entities such as trusts and real estate ownership. Witnesses advocating this expanded registry included the Foundation for Defence of Democracies,

6 With a trust, an individual – known as the "settlor" – transfers legal ownership of his/her assets to a trustee, who holds those assets for the benefit of the person(s) named by the settlor. Because the settlor is no longer the legal owner of the assets, he/she has no direct tax obligations in relation to them.

7 Additional information on the trust registry is available from KPMG, *UK Trust Register – What You Need to Know*, 11 July 2017.

Christian Leuprecht, Marc Tassé and Kevin Comeau, who appeared as individuals. Transparency International Canada and Mr. Comeau further noted that the registry required appropriate powers to apply proportionate and dissuasive sanctions if the information provided is untruthful. For her part, Ms. Johnson explained that the complexity of certain corporate ownership structures may require a sophisticated register that would be capable of following up on information submitted to properly perform its intended function.

There was no consensus among witnesses concerning the public accessibility and availability of personal information within a beneficial ownership registry. Milos Barutciski, who appeared as an individual, supports the creation of a registry that can only be accessed by government and by law enforcement and the Privacy Commissioner of Canada suggested that any data that would be made public under such a registry should be limited to what is necessary to achieve a specific purpose, such as informing another contractual party with whom they are dealing. The Investment Industry Association of Canada felt that a central registry was required, but that the public or private nature of the registry would depend on the government's policy objectives. The Canadian Life and Health Insurance Association believed that the sensitivity of the information in such a registry may not be appropriate for the public at large, but allowing limited access for authorized reporting entities would reduce certain regulatory burdens placed on their industries. Furthermore, the Canadian Bar Association explained that any law that requires a lawyer to collect client information on behalf of the government undermines solicitor-client privilege and weakens the independence of the Association. However, witnesses informed the Committee during its travels that lawyers in other jurisdictions – such as the U.K – have AML/ATF reporting requirements for their non-litigious work. In addition, the Canadian Real Estate Association did not feel that the duty to collect beneficial ownership information should be extended to realtors.

Witnesses from the public service also discussed beneficial ownership; FINTRAC noted that the Financial Action Task Force on Money Laundering (FATF) identified beneficial ownership as one of the two most important issues concerning the Canadian system.[8] The Department of Finance indicated that it was moving forward with the development of a beneficial ownership registry, while the Department of Industry emphasized that this is an area of shared jurisdiction between the federal and provincial governments and will require extensive co-operation. The Attorney General of British Columbia explained that while a centrally managed registry could be a solution; alternatively, the federal government could establish the best practice standards for beneficial ownership

8 As noted by the Department of Finance, the second of such issues identified by the Financial Action Task Force on Money Laundering was the legal profession's exclusion from the reporting regime.

disclosure and allow the provinces/territories to establish and administer their own registries. The Canada Revenue Agency (CRA) indicated that the absence of a public beneficial ownership registry hinders its investigations.

During the Committee's travels, certain witnesses explained that the U.K.'s beneficial ownership registry was the product of many years of AML/ATF work that has set the standards for the rest of Europe. They also noted that this registry was not extended to trusts that do not have tax consequences because it was felt that these trusts were personal in nature. However, they went on to say that all trustees are required to keep up-to-date records of their beneficial owners and provide those records to law enforcement upon request.

Witnesses further explained to the Committee that the U.K.'s beneficial ownership registry relies largely on public scrutiny to verify the accuracy of the information entered by each corporation, though Companies House has forensic accounting capabilities to examine any allegations of incorrect information. Furthermore, the Committee was informed that individuals tasked with entering and updating their corporation's information into the registry are required to take reasonable steps to identify the beneficial owners of their corporation and can be personally liable – including facing up to a two-year prison sentence – for failing to report that information in a timely and accurate manner.

Witnesses also believed that the European Union was considering amending the definition of PSC by decreasing the percentage of share ownership or voting rights in a corporation that constitutes a PSC from 25% to 10%.

B. POLITICALLY EXPOSED PERSONS

(i) Background

Section 9.3 of the PCMLTFA requires all reporting entities (listed in section 5 of the PCMLTFA) to determine whether it is dealing with "politically exposed persons" (PEPs), a prescribed family member of a PEP or an individual who the person or entity knows or should reasonably know is closely associated – for personal or business reasons – with a PEP. As defined under section 9.3(3) of the PCMLTFA, PEPs can be those who hold certain military or government positions either domestically or for a foreign government, as well as those who are a head of an international organization.

In addition, section 9.6(2) of the Act and section 71(1)(c) of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations* require every reporting entity to

assess the level of risk of money laundering and terrorist financing associated with each client as well as their business relationships. As a result of this risk assessment, where the reporting entity considers that the risks are high, it is required to take the special or enhanced anti–money laundering and anti–terrorist financing (AML/ATF) measures set out in section 9.6(3) of the Act and section 71.1 of the Regulations.

Within the United Kingdom and United States, the definition of a PEP is largely identical under section 14(5) of the *Money Laundering Regulations 2007*, and Department of the Treasury Regulations, respectively.

(ii) Witness Testimony

In the paper Reviewing Canada's Anti-Money Laundering and Anti-Terrorist-Financing Regime, the Department of Finance indicated that the requirements under the PCMLTFA and its regulations for reporting entities to determine whether their clients are PEPs does not extend to the beneficial owners of corporate clients, or those of other legal arrangements such as trusts. Mora Johnson pointed out that PEPs often use an associate or an agent to conduct business on their behalf, who may not have identified themselves as a PEP. She further explained that this behaviour necessitates the creation of one or more databases to establish patterns of behaviour and connections between individuals, such as the commercial World-Check database employed by banks. However, access to these databases are expensive and may therefore not be utilized by smaller reporting entities.

The Canadian Life and Health Insurance Association would welcome clarification of the definition of PEPs, both domestic and foreign, but do not support the extension of the definition to include First Nations Chiefs at this time. They also felt that the requirement to determine if a beneficial owner is a PEP should only be considered once a reliable method of identifying PEPs – such as a registry – is in place. However, the Canadian Real Estate Association suggested that implementing new requirements around beneficial ownership and politically exposed persons would cause significant frustration and increase the cost of compliance in their industry.

Over the course of the Committee's travels, certain witnesses noted that – across jurisdictions – the identification of PEPs is troublingly inconsistent. Reporting entities have been afforded the freedom to determine the extent to which they apply due diligence procedures to PEP identification, and many entities conduct little or none. For example, witnesses noted that some reporting entities will only request that a client self-identify as a PEP through a checkbox in their application for services without defining what a PEP is, while other entities have stopped accepting PEPs as clients because of the uncertainty surrounding their level of risk. Furthermore, some witnesses contend that the definition of

HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

a PEP under Canadian law is overly broad, to the extent that everyone would be a PEP if a more technical interpretation of the definition was adopted.

Witnesses explained that larger financial institution will operate or subscribe to media advisory services that will identify the names of their clients if they are engaged in higher-risk activity and/or identify them as PEPs through media reports. However, smaller reporting entities do not have the capacity to operate or subscribe to these services. They argued that a central registry or database of PEPs in Canada would address these problems in the AML/ATF regime.

C. THE LEGAL PROFESSION

(i) Background

Lawyers practicing in Canada and notaries practicing in Quebec (legal professionals) are self-regulated under their province's or territory's law society, of which there are currently 14. Prior to 2015, legal professionals were among the entities listed in the PCMLTFA that were required to keep detailed records about the financial activity of their clients, and law enforcement were permitted to search their client's information without a warrant. The Federation of Law Societies of Canada argued that these provisions in the Act were unconstitutional, and on 13 February 2015, the Supreme Court of Canada ruled that these provisions conflicted with solicitor–client privilege.[9] As a result of this ruling, these provisions of the Act do not apply to legal professionals. Provincial/territorial law societies may nevertheless require lawyers in their respective jurisdiction to conduct client verification and keep a record of monetary transactions.

Solicitor-client privilege describes the legally protected confidentiality that exists for communications between a client and his or her lawyer, which stems from the argument that people must be able to speak candidly with their lawyers to enable their interests to be fully represented, thereby facilitating the just operation of the legal system. The Supreme Court of Canada described the origins of Canadian solicitor-client privilege in the 2001 case of *R. v. McClure*, which explains that this form of privilege began as a rule of evidence and became a fundamental legal right through the common law.[10] The case explains that while limited exceptions to this privilege exist – namely, that it will not apply to a client who is not seeking legal advice – it must be as close to absolute as possible in order to function properly.

9 See: *Canada (Attorney General) v. Federation of Law Societies of Canada*, [2015] SCC 7.

10 Common law is derived from custom and judicial precedent rather than statutes, and is also referred to as "case law."

Attorney-client privilege in the United States operates similarly to Canadian solicitor-client privilege, and legal professionals are exempt from AML/AFT reporting in both jurisdictions. However, legal professionals in the United Kingdom are subject to the same AML/ATF reporting requirements as other U.K. reporting entities in all non-litigious work they perform. In general, the U.K. weighs the paramountcy of the client's interests differently than in Canada and the United States. A lawyers' duties to the court are given more weight in the U.K., and societal differences exist between our jurisdictions with respect to the interpretations of acting in the "interests of justice" and the role that members of the legal profession are expected to play in society.[11]

The legal profession is also self-regulated in the United States and the United Kingdom. However, the U.K,'s Office for Professional Body Anti-Money Laundering Supervision (OPBAS) sets out how certain professionals – such as lawyers and accountants – should comply with their professional obligations with respect to Anti-Money Laundering and Anti-Terrorist Financing (AML/ATF) initiatives. OPBAS is funded through fees placed on the professional bodies and is operated under the U.K. Financial Conduct Authority, which is the U.K.'s prudential and business conduct regulator. OPBAS aims to improve consistency of professional body AML/ATF supervision in the accountancy and legal sectors, but it does not directly supervise legal and accountancy firms.

The U.K. Treasury department controls which entities are listed as self-regulatory organizations for the purpose of compliance with the U.K's Money Laundering Regulations. OPBAS operates within the U.K's Financial Conduct Authority and has the authority to use information gathering powers, review and issue directions to self-regulatory organizations. If such an organization fails to comply with its obligations under the U.K.'s Money Laundering Regulations or provides false or misleading information to OPBAS, the Financial Conduct Authority can publicly censure the organization or recommend it be removed as a designated self-regulatory organization.

(ii) Witness Testimony

The Royal Canadian Mounted Police (RCMP) and the Department of Finance identified the exclusion of lawyers and Quebec notaries from the PCMLTFA as the most significant gap within the AML/ATF regime. The Government of British Columbia explained that the absence of lawyers from the regime is also an impediment to police investigations involving the movement of money through the real estate and financial sectors. To address this gap, Transparency International Canada and Marc Tassé recommended that the Federation of

11 For a discussion on this topic, see: A collaborative publication of the International Bar Association, the American Bar Association and the Council of Bars and Law Societies of Europe, *A Lawyer's Guide to Detecting and Preventing Money Laundering*, October 2014.

HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Law Societies of Canada, in collaboration with the federal government, bring legal professionals into the ALM/ATF regime in a constitutionally compliant way. They also argued that the Act should designate all financial transactions by legal professionals – especially those using trust accounts – as high-risk and require reporting entities to take enhanced due diligence measures on those transactions, including identifying the beneficial owner and the source of funds. Transparency International Canada indicated that the Solicitors Regulation Authority which regulates solicitors in England and Wales is a model that both the Federation of Law Societies of Canada and the government should explore. Furthermore, the Government of British Columbia recommended that legislation be created to require the legal profession to report the funds in lawyers' trust accounts. Mora Johnson recommended that agents and trustees – including nominee shareholders and directors – should be required to disclose their status as representative as well as the identity of the parties they represent to certain officials. However, these points of view were not unanimously shared among the witnesses.

The Canadian Bar Association emphasized that the legal profession's independence from government and respect for solicitor-client privilege are at the foundation of Canada's justice system. In light of this, the Association and the Federation of Law Societies recommended that the Canadian law societies should continue to self-regulate their industry with respect to anti-money laundering and terrorist financing requirements. The Federation of Law Societies argued that their rules, such as limiting the ability of legal counsel to accept cash (the "No Cash Rule") and imposing client verification obligations (the "Client ID Rule") are evidence of the Canadian law societies' commitment to proactively regulate themselves in this area. In their estimation, the combination of rules of professional conduct, financial accounting rules, the "No Cash Rule" and the "Client ID Rule" provide effective safeguards against members of the legal profession becoming involved in money laundering or terrorist financing. They also brought to the Committee's attention that they were currently engaged in a comprehensive review of the AML/AFT rules and associated compliance and enforcement measures used by the law societies, and that amendments to these rules would be implemented by late 2018. On 19 October 2018, the Federation of Law Societies approved amended AML/AFT rules.

The RCMP indicated that because lawyers have considerable involvement in real estate and corporate transactions, it is important that they are included in the regime. They undertook an audit from July 2013 to June 2017 of 51 financial crime cases and found that over 75% involved lawyers as either a direct suspect or someone identified during the investigation.

During the Committee's travels, certain witnesses brought to the Committee's attention that lawyers often perform no PEP or sanctions list screening of their clientele, and no such requirement exists for their profession. Similarly, they noted that lawyers are not required to inquire into the source of funding of heir clients, and believed that their codes of professional conduct only extend AML/ATF considerations to transactions that are obviously dubious.

With respect to reporting to FINTRAC, these witnesses explained that transfers of $10,000.00 or more from a lawyer's trust account will be reported by the bank that provides that trust account. However, it is uncertain to what extent banks would file suspicious transaction reports from these transfers.

D. WHITE LABEL AUTOMATED TELLER MACHINES

(i) Background

"White-label" or "no name" automated teller machines (ATMs) are mostly owned and operated by private companies, not financial institutions. White Label ATMs can access the Interac payment network, which allows for the sharing of electronic financial services and the electronic access to bank accounts.

In 2015, the Department of Finance released its report on the *Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada* that detailed Canada's approach to "better identify, assess and understand inherent money laundering and terrorist financing risks in Canada on an ongoing basis." This report noted that this industry is highly vulnerable to money laundering and terrorist financing, but industry participants are not subject to the PCMLTFA.

(ii) Witness Testimony

According to the ATM Industry Association, the ATM industry is subject to the to several regulations at the federal and provincial levels, as well as FINTRAC oversight through their connection with financial institutions. In their introductory statement to the Committee, it recounted that since 2009, white label ATMs have been subject to specific anti-money laundering regulations requiring ATM owners to provide information about themselves, the source of cash used in the ATM, the location of the ATM, and details about the Canadian bank account to which the ATM will deposit funds to be withdrawn. Furthermore, the association stated that business owners with multiple ATMs or high-volume ATMs are required to provide criminal background checks and regulations require annual audits. They also indicated that Quebec is the only province in Canada

HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

that has a money-services business act that includes ATMs, white label ATMs and that they would prefer this act to be repealed or have ATMs taken out of that act.

Conversely, FINTRAC stated that ATMs are a way to launder money, but conceded that it is difficult to know the extent of the problem because it is not something that is currently being measured, as the industry does not report to FINTRAC.

E. THE REAL ESTATE SECTOR AND ALTERNATIVE MORTGAGE LENDERS

(i) Background

Certain businesses and individuals in the real estate sector are subject to the PCMLTFA, such as real estate brokers, sales representatives and developers. However, other businesses and individuals such as mortgage insurers, land registries and title insurance companies are not. The Department of Finance's report on the *Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada* noted that this industry is highly vulnerable to money laundering and terrorist financing.

In Canada, the mortgage sector extends beyond Banks into a variety of non-federally regulated businesses, such as private equity companies, mortgage finance companies, real estate investment trusts, mortgage investment corporations, mutual fund trusts, syndicated mortgages or individuals acting as private lenders. Both the *Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada* and the Financial Action Task Force's most recent Mutual Evaluation Report identified complex loan and mortgage schemes, such as mortgage fraud, as areas of money laundering risk.

(ii) Witness Testimony

The Government of British Columbia outlined one example of money laundering through real estate by connecting a gambler who obtained $645,000 in small bills through a "drop off" outside a casino to ownership of a $14 million house in Vancouver. It also alleged that loans from an unregistered money service business had been used to fund real estate development and make mortgage payments, and indicated an interest in pursuing the issue of criminality in the real estate sector now that the current review of money laundering in casinos is near completion. The Government of British Columbia added that the real estate industry is of particular concern as it is estimated that one third of British Columbia's GDP is dependent on the sector, and recommend that real estate transactions be subject to PCMLTFA reporting requirements.

Transparency International Canada agreed with the Government of British Columbia, and further recommend the PCMLTFA be amended to require real estate brokers, representatives, developers and lenders to identify beneficial ownership before conducting transactions. They also indicated that the Act does not address purchases of existing commercial or residential buildings, and suggest that redevelopers of existing buildings should be included in the regime to further minimize the risk of real estate being used for money laundering and terrorist financing (ML/TF) purposes. It also called for a registry of beneficial ownership for land.

In their statement before the Committee, the Canadian Real Estate Association said that it is in favour of expanding the types of reporting entities that must report to FINTRAC to create a more level playing field in the real estate sector. It also emphasized that closing existing loopholes for the real estate sector should be a focus of the government and indicated that sales between private individuals create vulnerabilities that money launderers can exploit. Thus, it recommended that reporting and record keeping obligations should be extended to the companies that facilitate such transactions, and also recognized that education and ongoing outreach efforts are essential for new and existing realtors to make sure that they understand their requirements. It also suggested that FINTRAC improve its outreach strategy to build stronger partnerships with reporting entities and maximize compliance, as well as clarify existing guidance in a manner that is meaningful to brokers and agents, and adopt policy interpretations that are better suited to the industry.

During the course of the Committee's travels, certain witnesses believed that the real estate sector does not fully understand the requirements placed upon them under the regime. In particular, they may not understand how complex corporate ownership structures interact with their "know your client" (KYC) requirements, and that they do not check their clients against any form of sanctions lists or perform PEP scrutiny.

F. STRUCTURING TO AVOID REPORTING

(i) Background

Under the Act, it is permissible for businesses to structure themselves and/or the conduct of their business in a way such that their transactions avoid triggering AML/ATF reporting requirements. In other jurisdictions, such as the United States which adopted U.S. Code 31 USC 5324, it is a criminal offence to structure financial transactions in this way.

HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

(ii) Witness Testimony

According to the Foundation for Defense of Democracies, it should be a criminal offence for an entity or an individual to structure transactions to avoid the regime's reporting requirements, similar to the operation of title 31 of the U.S. code section 5324 in the United States. This should apply equally to financial institutions and their clients.

G. ARMOURED CARS

(i) Background

In Canada, the armoured car sector is not subject to the AML/ATF regime, unlike other jurisdictions such as the United States. Armoured cars may collect funds from various clients and deposit them into accounts controlled by the armored car company. Those funds are then transferred electronically into the accounts of their customers, which may potentially obscure their origin.

(ii) Witness Testimony

The Foundation for Defense of Democracies argued that armoured car companies operating in Canada should be subject to the AML/ATF regime, and indicated that armoured cars are one of the main ways in which drug cartels have gotten money from Mexico to the United States.

H. HIGH-VALUE GOODS DEALERS AND AUCTION HOUSES

(i) Background

In Canada, dealers of precious metals and stones are subject to the regime, while other dealers of high value and/or luxury goods are not. FATF's most recent Mutual Evaluation of Canada identified other luxury goods sectors as being areas of increased money laundering and/or terrorist financing risks, such as luxury automobiles, art and antiques. In addition, auction houses selling precious metals and stones are not subject to the AML/ATF reporting requirements.

(ii) Witness Testimony

The Government of British Columbia identified the auto sector as a high-risk area, as Vancouver has among the highest number of "super cars" in North America and auto dealers in Greater Vancouver are among the highest new and used luxury car dealers in

Canada by sales volume. They also believe that the criminal lifestyle is often attracted to expensive consumer goods such as luxury cars and pleasure crafts, and such goods are excellent ways in which illegal cash can be reintroduced into the economy. The Government of British Columbia recommended that companies that sell luxury items be subject to reporting requirements under the PCMLTFA and report cash transactions to FINTRAC. The Canadian Automobile Association noted that only 8% of new vehicle sale transactions were concluded without formal leasing or loan arrangements in 2017. Therefore, the transactions that use such arrangements, 92% of all transactions, would already be captured by the reporting of financial institutions. Moreover, only a fraction of 1% of the remaining 8% of transactions concluded without formal leasing or loan arrangements were made in physical cash.

The Canadian Jewellers Association contended that all luxury product dealers – such as those of cars, boats and art – should be required to report large cash transactions to FINTRAC. The auction houses that would be captured under the regulations and the dealers in Precious Metals and Stones that fall into a lower-risk category should be allowed to have a simplified compliance regime, or be exempted entirely if they do not engage in cash transactions above the reporting threshold. The Association also pointed out that auctions houses do not have regulated KYC requirements.

I. SECURITIES DEALERS

(i) Background

Securities are publicly traded financial assets such as shares of a corporation, bonds, treasury bills, and other debt obligations.[12] The securities industry in Canada is under the jurisdiction of the provincial and territorial government and is therefore regulated at this level. However, to ensure national policy coordination between the provinces and territories, the securities regulators formed the Canadian Securities Association, which is responsible for developing a harmonized approach to securities regulation across the country. In July 2015, the federal government created the joint federal provincial initiative, the Cooperative Capital Markets Regulatory System, which aims to streamline the capital markets regulatory framework to protect investors, foster efficient capital markets and manage systemic risk while preserving the strengths of the current system.[13]

12 For a list of other forms of securities in Canada, see: Government of Canada, *What are Securities?*, accessed by author 4 October 2018.

13 The participating provinces/territory under the Cooperative Capital Markets Regulatory System are British Columbia, Ontario, Saskatchewan, New Brunswick, Prince Edward Island and Yukon.

HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

The FATFs mutual evaluation indicated that securities dealers have a good understanding of their AML/AFT obligations, though the level of understanding is weaker in smaller securities firms.

(ii) Witness Testimony

Appearing before the Committee, the Investment Industry Association of Canada indicated that many of its members are smaller firms that carry a disproportionately high compliance burden under the regime.

During the Committee's travels, some witnesses believed that the securities sector represents a gap in the Canadian AML regime, predominantly due to the patchwork of provincial regulators and no federal AML direction or oversight. Others noted that when securities dealers are suspected of wrongdoing, they are able to resign from their position prior to the conclusion of any internal investigation against them. These individuals then move to another company or brokerage that is unable to be informed about the allegations or unfinished investigation against that broker under Canadian privacy law. This situation allows for bad actors in the security industry to continually circumvent detection and prosecution.

Chapter 1 Recommendations

Recommendation 1

That the Government of Canada work with the provinces and territories to create a pan-Canadian beneficial ownership registry for all legal persons and entities, including trusts, who have significant control which is defined as those having at least 25% of total share ownership or voting rights.

- **Such a registry should include details such as names, addresses, dates of birth and nationalities of individuals with significant control.**
- **The registry should not be publicly accessible, but it can be accessed by certain law enforcement authorities, the Canada Revenue Agency, Canadian Border Services Agency, FINTRAC, authorized reporting entities and other public authorities.**
- **To ensure that the registry is accurate and properly performing its function, it should have the capability to follow up on information submitted to it.**

- **The registry should take into account the best practices and lessons learned from other jurisdictions. In particular, the Committee was interested in the United Kingdom's dual system of registration, which can be done through a legal professional or through direct online registration, as seen in the U.K.'s Companies House.**

- **Authorities should be granted appropriate powers to apply proportionate and dissuasive sanctions for failure to fully comply in the prescribed time frame.**

- **Beneficial owners of foreign companies that own property in Canada should be included in such a registry.**

- **That subject to Canadian law, requests by foreign governments for information sharing under a Canadian beneficial ownership registry should be considered by the Government of Canada, in cases where tax treaties or other lawful agreements or protocols exist for potential or existing money laundering, terrorist financing or criminal activity.**

Recommendation 2

That the Government of Canada review, refine, and clarify through training, the statutory definition of politically exposed persons (PEP). In particular, the notion of 'association with a PEP' under this definition creates ambiguity and inconsistency among institutions in regards to who exactly constitutes a PEP.

Recommendation 3

That the Government of Canada move to a risk-based model of compliance for politically exposed persons, softening the requirements for those with transparent and unsuspicious financial portfolios.

Recommendation 4

Given that the legal professions in the U.K. are subject to the same AML/ATF reporting requirements as other reporting entities in all non-litigious work that is performed, the Government of Canada and the Federation of Law Societies should adopt a model similar to the U.K.'s Office of Professional Body Anti-Money Laundering Supervision.

- **The Government of Canada request Reference from the Supreme Court of Canada as to whether solicitor-client privilege exists when a client requests advice on how to either launder money or structure finances for the purposes of illegal activity.**

HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Recommendation 5

That the Government of Canada bring the legal profession into the AML/ATF regime in a constitutionally compliant way with the goal of ensuring that the Canadian standards set by the PCMLTFA protect against money laundering and terrorist financing.

Recommendation 6

That the Government of Canada consider implementing a body similar to the U.K.'s Office of Professional Body Anti-Money Laundering Supervision with respect to Canadian self-regulated professions.

Recommendation 7

That the Government of Canada amend the PCMLTFA so that the armoured car and white label ATM sector be subject the AML/ATF regime, as is the case in the United States and the province of Quebec, respectively.

Recommendation 8

That the Government of Canada amend the PCMLTFA to require all reporting entities, including designated non-financial businesses and professions, such as the real estate sector (brokers and lenders), that are now exempt from the obligation of identifying beneficial ownership, to do the following:

- **determine and verify the identity of the beneficial owners;**
- **determine if their customers are politically exposed persons, or if they are the family members or associates of politically exposed person;**
- **prohibit opening accounts or completing financial transactions until the beneficial owner has been identified and their identity verified with government-issued identification.**

***Consideration of the above should also be applied to foreign beneficial owners.**

Recommendation 9

That the Government of Canada amend the PCMLTFA to extend the requirements for real estate brokers, sales representatives and developers to mortgage insurers, land registry and title insurance companies.

Recommendation 10

That the Government of Canada make it a criminal offence for an entity or individual to structure transactions in a manner designated to avoid reporting requirements. These provisions would be modeled on Title 31 of U.S. code section 5324.

Recommendation 11

That the Government of Canada require companies selling luxury items to be subject to reporting requirements under the PCMLTFA and report large cash transactions to FINTRAC if those transactions are not already reported through other means.

Recommendation 12

That the Government of Canada amend Canadian privacy laws with the sole purpose of permitting security regulators to fully and appropriately examine the professional record of conduct of security dealers and their employees.

Recommendation 13

That the Government of Canada develop a national view of AML by partnering with provinces and territories to train local regulators on best practices in order to prevent securities firms from being overlooked.

CHAPTER 2: THE EXCHANGE OF INFORMATION AND PRIVACY RIGHTS OF CANADIANS

The Discussion Paper identified a number of areas related to the exchange of information between various parties in order to facilitate the AML/ATF regime. A number of witnesses also provided comments on information sharing topics, which include:

- sharing and retention within government,
- sharing and retention between the government and the private sector,
- sharing and retention within the private sector, and
- de-risking.

A. INFORMATION SHARING AND RETENTION WITHIN GOVERNMENT

(i) Background

Established by the Act and its regulations, FINTRAC is Canada's financial intelligence unit led by the Department of Finance Canada. It collects finance intelligence and enforces compliance of reporting entities with the legislation and regulations. FINTRAC acts as a financial intelligence agency independent from the law enforcement agencies and has no investigative powers. It is authorized under the Act to only disclose "designated information" as defined by sections 55(7), 55.1(3) and 56.1(5), which is dependent on the nature of the disclosure.[14]

As described by the Privacy Commissioner of Canada, the *Privacy Act* sets out the privacy rights of Canadians in their interactions with the federal government, and obliges government institutions to control the collection, use, disclosure, retention and disposal

14 Section 55(7) relates to disclosures to Canadian departments and agencies in relation to investigating or prosecuting a money laundering offence or a terrorist activity financing offence; section 55.1(3) relates to disclosures to Canadian departments and agencies in relation to information relevant to threats to the security of Canada; and section 56.1(5) relates to disclosures to an institution or agency of a foreign state or of an international organization that has powers and duties similar to FINTRAC.

HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

of recorded personal information.[15] Section 8(1) of the *Privacy Act* details that personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be disclosed by the institution except in accordance with sections 8(2)–(8). In addition, all provinces and territories have legislations that apply to how provincial/territorial agencies handle personal information.

Notably, under section 8(2)(m) of the *Privacy Act*, government institutions may disclose the information of Canadians if the "public interest in disclosure clearly outweighs any invasion of privacy" or the "disclosure would clearly benefit the individual to whom the information relates." When making a disclosure of this kind, the government institution must inform the Privacy Commissioner of the disclosure. Also, section 5(1) of the *Security of Canada Information Sharing Act* provides that specified government institutions – including FINTRAC – may, on their own initiative or on request, disclose information to another specified government institution if the information is relevant to the recipient institution's jurisdiction or if the information relates to "activities that undermine the security of Canada, including in respect of their detection, identification, analysis, prevention, investigation or disruption." Furthermore, the institution cannot be sued if they shared information in good faith under this Act. However, section 5(1) is "subject to any provision of any other Act of Parliament," meaning that the specified government institutions must still conform to any other legislated disclosure requirements – such as those that are more rigorous – should they wish to make a disclosure under section 5(1).

In the United States, there is no single federal law that regulates the collection and use of personal data.[16] Instead, the U.S. has a patchwork system of federal and state laws as well as regulations that may overlap. In addition, there are many guidelines, developed by governmental agencies and industry groups that do not have the force of law, but are part of self-regulatory guidelines and frameworks that are considered "best practices". One such practice includes the "third agency rule."

In the U.S., the Department of Justice defines the "third agency rule" as a restriction on information sharing between government departments and/or agencies. In effect, a government department or agency can only release information to a separate

15 The *Privacy Act* defines "personal information" as any recorded information "about an identifiable individual." It can include the following: an individual's race; national or ethnic origin; religion; age; marital status; blood type; fingerprints; medical, criminal or employment history; information on financial transactions; home address; Social Insurance Number; driver's licence or any other identifying number assigned to an individual.

16 U.S. Federal legislation that intersects with the privacy of information include, but are not limited to: the Privacy Act of 1974, the E-Government Act of 2002, and the Federal Records Act.

government department or agency under the condition that the receiving department or agency does not release the information to any other department or agency.

(ii) Witness Testimony

The Government of British Columbia observed that better information sharing is needed. Given the breadth of information at FINTRACs disposition, the Government of British Columbia feels that FINTRAC is in a better position to identify emerging and long-term trends and would like to see this type of information shared with the appropriate authorities at the provincial level. The Canadian Banking Association also recommended that the regime be enhanced through greater collaboration, communication, and information sharing between governments. This opinion was shared by the Government of British Columbia which recommended that an information-sharing mechanism between law enforcement and FINTRAC be regulated under the PCMLTFA. The Canadian Life and Health Insurance Association reminded the Committee that, in recent history, amendments have been made to enable FINTRAC to exchange information with more of its federal and provincial partners. For example, securities regulators and national intelligence agencies.

The Privacy Commissioner of Canada highlighted the need for rigorous legal standards around the collection and sharing of personal information, effective oversight, and minimization of risks to the privacy of law-abiding Canadians, in part through prudent retention and destruction practices. The Commissioner contends that there is a lack of proportionality in the regime, as disclosures to law enforcement and other investigative agencies made in a given fiscal year represent a very small number when compared with the information received during that same time frame; in addition, FINTRAC's retention of undisclosed reports increased from five to 10 years in 2007. Furthermore, he stated that once that information is analyzed and leads to the conclusion that someone is not a threat, it should no longer be retained; therefore, a risk-based approach of collection and retention of data should be implemented. The Commissioner highlighted the data retention practices that would be implemented by Bill C-59 An Act Respecting National Security Matters, where data is disposed of within 90 days unless a Federal Court is satisfied that its retention is likely to assist in the performance of the Canadian Security Intelligence Service's mandate. He also recommended that his office be mandated to undertake a review of proportionality review that would commence one year prior to each five-year review of the PCMLTFA by Parliament.

The Government of British Columbia raised the issue that law enforcement officials do not work within FINTRAC due to privacy concerns, and believed that there would be significant benefit to the regime if such a practice were to be implemented.

HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

During the Committee's travels, certain witnesses highlighted that long-term data retention is an important aspect of the AML/ATF regime, as the ability of criminals to obscure the financial aspects of their crime is often less advanced earlier on, and that once an individual becomes the target of an investigation, law enforcement's ability to access their data from earlier in their "criminal career" is often very useful in building the prosecution's case. FINTRAC explained that the reports it receives are disposed of after 10 years if they are not disclosed to law enforcement, and the Privacy Commissioner of Canada noted that this data retention limit was extended from the previous limit of 5 years in 2007.

Additionally, many of these witnesses believed that greater communication between government bodies leads to a more effective AML/AFT regime.

B. INFORMATION SHARING AND RETENTION BETWEEN THE GOVERNMENT AND THE PRIVATE SECTOR

(i) Background

The Canadian *Personal Information Protection and Electronic Documents Act* (PIPEDA) details how private-sector organizations collect, use, and disclose personal information in the course of for-profit, commercial activities in Canada. PIPEDA also applies to the personal information of employees of federally regulated businesses such as banks, airlines and telecommunications companies. Alberta, British Columbia and Quebec have private-sector privacy legislation that have been deemed "substantially similar" to PIPEDA, and may apply instead of PIPEDA in some cases.

Information that FINTRAC receives and analyzes may be shared in the form of studies, methods and trends in order to educate the public – including the reporting entities – on money laundering and terrorist financing issues. For example, project PROTECT was launched in January 2016 and is a public-private partnership between reporting entities and FINTRAC that targets human trafficking for the purposes of sexual exploitation by focusing on the money laundering aspect of the crime. After engagement with reporting entities, law enforcement and policy makers, FINTRAC published its operational alert, Indicators: The Laundering of Illicit Proceeds from Human Trafficking for Sexual Exploitation. This 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 FINTRAC.

The *USA Patriot Act* contains provisions aimed at the prevention, detection and prosecution of money laundering and financing of terrorism.[17] In particular, section 314(a) of the Patriot Act authorizes FinCEN to provide to financial institutions with a "Section 314(a) list," which contains the names of individuals or entities suspected of criminal activity, and to compel those financial institutions to supply information regarding the named suspects. Federal, state, local, and certain foreign law enforcement agencies that are investigating money laundering or terrorism can request that FinCEN obtain certain information from one or more financial institutions. This request must be in the form of a written certification stating that each individual, entity, or organization about which the law enforcement agency is seeking information is engaged in, or is reasonably suspected of engaging in, terrorist activity or money laundering. Upon receiving a request from FinCEN, a financial institution must verify if it maintains accounts for, or does business with, the person or entity being investigated and report its findings to FinCEN.

The U.K.'s Joint Money Laundering Intelligence Taskforce (JMLIT) is a partnership – established in May 2016 – between the U.K. government and the financial sector with the goal of combating high-end money laundering. The partnership includes the British Bankers Association, law enforcement and over 40 major U.K. and international banks under the leadership of the Financial Sector Forum. Various levels of the JMLIT meet quarterly or monthly to improve intelligence sharing arrangements between organizations, strengthen the relationship between public and private sector bodies, and discuss potential improvements and/or best practices for the AML/ATF regime.[18]

JMLIT members meet to share their respective information and experiences to come to a better understanding of funding linked to bribery and corruption, trade based money laundering, funding flows linked to organized immigration crime, money laundering through capital markets and terrorist financing methodologies. According to the U.K.'s National Crime Agency, JMLIT has produced new and effective targeted and coordinated AML/ATF interventions by law enforcement and the financial sector. In particular, JMLIT has led to, among other outcomes, 63 arrests of individuals suspected of money laundering and the freezing of £7 million of suspected criminal funds.

17 The full title of the Patriot Act is the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001."

18 See: National Crime Agency, JMLIT Toolkit, accessed 27.06.2018.

HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

(ii) Witness Testimony

The Investment Industry Association of Canada suggested that FINTRAC specifically work with other regulators to reduce duplication and overlap in rules and procedures. Vanessa Iafolla, who appeared as an individual, also suggested that there is a need for improved guidance and feedback to regulated entities that is provided by oversight bodies such as OSFI and FINTRAC to improve their AML/ATF reports.

The Canadian Life and Health Insurance Association generally supported measures – through privacy and AML legislation – which would promote better information-sharing between the private and public sectors, and suggested that Canada should adopt best practices from models used in other jurisdictions that permit effective information sharing. HSBC Bank Canada identified the need for additional action on the part of the federal government to increase information sharing and improve current feedback mechanisms.

A number of witnesses commented on the lack of feedback that FINTRAC provides to the reporting entities; in particular, the Government of British Columbia, the Investment Industry Association of Canada, the Canadian Jewellers Association, the Federation of Law Societies of Canada, the Canadian Bankers Association, and the Canadian Life and Health Insurance Association, as well as Shahin Mirkhan, John Jason, Vanessa Iafolla ,Christian Leuprecht and Mora Johnson – who appeared as individuals – explained that they do not feel that FINTRAC adequately communicates with reporting entities and that an increase in two-way communication would be beneficial. In particular, the Government of British Columbia described FINTRAC as a "black box" into which information is sent and from which no feedback is provided. In contrast, Jewellers Vigilance Canada Inc. noted that communication with FINTRAC has been very positive for over a decade. For its part, FINTRAC explained that information sharing is a careful balance between efficacy and protecting the rights of Canadians, and that they do perform outreach work with reporting entities to provide them with information on potentially suspicious transactions and indicators to identify money laundering trends.

The Investment Industry Association of Canada also believed that FINTRAC should engage in ongoing dialogue with securities dealers and other financial sector participants to ensure greater transparency in FINTRAC requirements.

In order to better assess the impact of the regime, Transparency International Canada highlighted the need for more transparency and feedback to be provided to reporting entities as well as the public, arguing that the government should create a performance measurement framework for the regime's operations and make the findings public each year.

The Privacy Commissioner of Canada cautioned that increased information sharing with the public sector might be useful to identify threats, but must be accompanied by appropriate privacy safeguards or such an approach would further exacerbate its concerns with the proportionality of the regime.

During the Committee's travels, a number of witnesses believed that the lack of direction from FINTRAC to the reporting entities constitutes a serious flaw of the regime. Reporting entities cannot properly assist FINTRAC with the identification of high-risk clients or patterns of money laundering without knowing what kinds of information is useful to the organization. They also noted that FinCEN and the National Crime Agency are able to communicate with U.S. and U.K. reporting entities, respectively, to provide them with these kinds of directions as well as request follow-up information.

Witnesses also signalled during the Committee's travels that Canadian banks would benefit from greater information sharing under a model similar to the JMLIT.

C. INFORMATION SHARING AND RETENTION WITHIN THE PRIVATE SECTOR

(i) Background

PIPEDA limits the information businesses collect to what is essential for the business transaction. If further information is requested, individuals are entitled to ask for an explanation and may decline if they are dissatisfied with the answer without adversely affecting the transaction. According to the Privacy Commissioner of Canada, PIPEDA sets out ten "fair information principles" that collectively form the underpinnings of PIPEDA, and include the following:

1) Accountability: Organizations should appoint someone to be responsible for privacy issues. They should make information about their privacy policies and procedures available to customers.

2) Identifying purposes: Organization must identify the reasons for collecting your personal information before or at the time of collection.

3) Consent: Organizations should clearly inform you of the purposes for the collection, use or disclosure of personal information.

4) Limiting collection: Organizations should limit the amount and type of the information gathered to what is necessary.

HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

5) Limiting use, disclosure and retention: In general, organizations should use or disclose your personal information only for the purpose for which it was collected, unless you consent. They should keep your personal information only as long as necessary.

6) Accuracy: Organizations should keep your personal information as accurate, complete and up-to-date as necessary.

7) Safeguards: Organizations need to protect your personal information against loss or theft by using appropriate security safeguards.

8) Openness: An organization's privacy policies and practices must be understandable and easily available.

9) Individual access: Generally speaking, you have a right to access the personal information that an organization holds about you.

10) Recourse (Challenging compliance): Organizations must develop simple and easily accessible complaint procedures. When you contact an organization about a privacy concern, you should be informed about avenues of recourse.

Within the EU, the General Data Protection Regulation (GDPR) came into force in May 2018 and introduced new privacy obligations to all companies processing and/or holding the personal data of individuals residing in the European Union, regardless of the company's location. These companies are now required to acquire the explicit and unambiguous consent from their customers to use or retain their "personal data," based on specific purposes for use of their data and for specific periods of time. "Personal data" is defined broadly, and includes an individual's name, identification number, location data or online identifier, reflecting changes in technology and the way organizations collect information.

Under the GDPR, individuals have the right to request a copy of the data that is held on them, including an explanation of how such data is used and if third parties have access to it. Individuals may also request that their data be deleted, and compensation can be claimed for any damage suffered by individuals caused by infringement of the GDPR. Organizations can be fined up to 4% of annual global turnover or €20 million for breaching the GDPR.

In the U.S., section 314(b) of the USA Patriot Act allows for financial institutions to voluntarily share – upon providing notice to FinCEN – information among each other

through the circulation of a "Section 314(b) list," and provides these institutions with immunity from private civil actions resulting from any disclosures that are in conformity with the *Bank Secrecy Act*. Financial institutions must establish and maintain procedures to safeguard the security and confidentiality of the information shared, and must only use shared information for the following purposes:

- identifying and, where appropriate, reporting on activities that may involve terrorist financing or money laundering;
- determining whether to establish or maintain an account, or to engage in a transaction; or
- assisting in compliance with anti-money laundering requirements.

(ii) Witness Testimony

The Canadian Life and Health Insurance Association was supportive of measures that would promote better information-sharing within the private sector through changes to privacy and AML legislation. It suggested that the government should adopt best practices from other jurisdictions. The Canadian Bankers Association supported the recent ethics committee recommendation that PIPEDA be amended to allow for a broader range of instances where financial institutions can share information, such as in cases of money laundering and terrorist financing. However, the Association recognized that any measures taken to enhance information sharing must be balanced with privacy considerations.

The Privacy Commissioner of Canada emphasized that any information sharing between the government and the private sector needs to be handled in a manner that complies with PIPEDA. He also recommended that the Department of Finance be legally required to consult with his office on draft legislation and regulations with privacy implications before they are tabled.

During the Committee's travels, a number of witnesses noted that reporting entities in all jurisdictions are developing advanced artificial intelligence or computer modelling to assess their clients' ML/TF risk. Some noted that these technologies can make use of publicly available data – such as that available on social media – to help develop a risk assessment of these clients, and that the private sector's use of data in this manner is relatively unregulated.

These witnesses also contended that financial institutions are better able to combat ML/TF activity when they are capable of sharing information among themselves. This is particularly true given the sophistication of organized crime, as they spread their

financial assets and transitions across many banks in order to limit any one bank's ability to detect the criminal nature of their activity.

D. INFORMATION SHARING AND DE-RISKING

(i) Background

"De-risking" – also known as de-banking – refers to the practice of financial institutions closing the accounts of clients and ceasing all business with them because they are perceived to be high-risk.

(ii) Witness Testimony

With respect to money service businesses, the Government of British Columbia indicated that the volatility of the industry has been apparent in the United States as many financial institutions have been ending their relationship with these businesses as part of a de-risking process in order to avoid the added anti-money laundering risks which they can pose. In their brief to the Committee, Dominion Bitcoin Mining Company examined the issue of de-risking, and underscored that money services businesses, including companies that work in the cryptocurrency space, have had a very difficult time establishing banking relationships due to the perceived risk of money laundering. Moreover, they outline that when FINTRAC examines financial institutions, they will automatically flag money service businesses as high risk, and therefore suggested that FINTRAC encourage financial institutions to conduct enhanced due diligence procedures instead of outright denying them banking services.

During the Committee's travels, witnesses explained that approximately ten customers are de-banked from Canadian banks every day, but they have recourse to appeal this decision with the banking ombudsman. During these discussions, witnesses cautioned that increasing information sharing between reporting entities – particularly banks – would lead to a significant increase in de-risking, as reporting entities will prioritize their financial interests over consumer access to their services. For example, witnesses highlighted a "three strike rule," under which a foreign bank will de-risk a client if it receives three separate requests from their financial intelligence unit for additional information on that client, despite the bank having no other evidence of wrongdoing with respect to that individual. As a result of de-risking behaviour, witnesses highlighted that "right to banking" legislation may be warranted in some jurisdictions, but that measures must be taken to ensure that the criminal activity does not simply move to the accounts guaranteed by this kind of legislation.

Some witnesses explained that de-risking can also pose a problem for law enforcement authorities because it is generally in their interest if the subject of an investigation continues their normal banking activity free from the suspicion of being investigated. They noted that law enforcement can be more effective when criminals make use of cellular phones and bank accounts. Throughout the U.S., U.K. and Canada, witnesses explained that law enforcement may make formal and informal requests to banks to refrain from de-risking specific clients who are under investigation, but that banks are reluctant to comply with such requests unless they are indemnified from any loss and liability resulting from their compliance.[19]

Chapter 2 Recommendations

Recommendation 14

That the Government of Canada examine the U.S. Government's "third agency rule" for information sharing and determine whether this rule would assist in investigation / detection of money laundering and terrorist financing in Canada.

Recommendation 15

That the Government of Canada expands FINTRAC's mandate to allow for:

- **a greater focus on building actionable intelligence on money laundering and terrorist financing, akin to FinCEN in the United States, and provide FINTRAC with the necessary resources to effectively undertake the corresponding analysis;**
- **the retention of data for 15 years;**
- **an operational model to allow for two-way information sharing system (rather than strictly being an information gathering system);**
    - **FINTRAC should be able to share feedback, best practices and long-term trends, so that reporting entities can properly assist FINTRAC.**
- **the ability to request more information from specific reporting agencies to clarify reported suspicious activity or to build a stronger case before referring it to law enforcement;**

19 In the United States, these indemnifications are referred to as "hold harmless letters."

HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

- **the ability to release aggregated data, subject to Canadian law, about a group of specific reporting agencies or a sector for statistical, academic or government purposes.**

Recommendation 16

That the Government of Canada establish a round table partnership with industry leaders who are investing significantly in technology that more efficiently tracks suspicious activities and transactions, so as to promote best industry practices.

Recommendation 17

That the Government of Canada take steps to emulate the U.K.'s model of a Joint Money Laundering Intelligence Taskforce in Canada.

Recommendation 18

That the government of Canada consider tabling legislation that would allow information that is limited to AML/ATF subject matter to be shared between federally regulated financial institutions such as banks and trust companies, provided that FINTRAC is notified upon each occurrence of such sharing.

Recommendation 19

That the Government of Canada implement the necessary requirements to banking to determine a "low-risk threshold" and establish exemptions to ensure the most vulnerable Canadians are not being denied a bank account due to lack of adequate identification.

CHAPTER 3: STRENGTHENING INTELLIGENCE CAPACITY AND ENFORCEMENT

Witnesses provided comments with respect to how the regime could be improved in intelligence gathering and enforcement measures, which include:

- prosecution and legal standards,
- bulk cash and bearer instruments,
- Geographic Targeting Orders,
- trade transparency units, and
- compliance and enforcement measures.

A. PROSECUTION AND LEGAL STANDARDS

(i) Background

Money laundering is a criminal offence under section 462.31(1) of the *Criminal Code*, and requires proof, beyond a reasonable doubt, that the accused intended to conceal or convert property or proceeds that they knew or believed were the result of a designated criminal offence,[20] or that they were wilfully blind to such a fact. In this context, "knowledge" is the subjective awareness of a fact that is objectively true, namely that the accused would be found guilty if they were, in fact, laundering proceeds of crimes and they were subjectively aware of that fact. "Willful blindness" is the subjective awareness of circumstances that should alert a person to the truth of a fact, and is accompanied by a deliberate refusal to confirm its existence. "Belief" is the subjective perception that a fact is true, whether or not it is objectively true.

"Willful blindness" is distinct from both "negligence" and "recklessness," as discussed in R. v. Sansregret:

20 A "designated offence" is defined under section 462.3(1) of the *Criminal Code* as "(a) any offence that may be prosecuted as an indictable offence under this or any other Act of Parliament, other than an indictable offence prescribed by regulation, or (b) a conspiracy or an attempt to commit, being an accessory after the fact in relation to, or any counselling in relation to, an offence referred to in paragraph (a)."

HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

> **Negligence** is tested by the objective standard of the reasonable man. A departure from his accustomed sober behaviour by an act or omission which reveals less than reasonable care.… In accordance with well-established principles for the determination of criminal liability, **recklessness** … is found in the attitude of one who, aware that there is danger that his conduct could bring about the result prohibited by the criminal law, nevertheless persists, despite the risk. It is, in other words, the conduct of one who sees the risk and who takes the chance. [Emphasis added]

In the U.K., the case of *R v Anwoir* [2008] resulted in it no longer being necessary for the Crown to prove – with respect to a money-laundering offence – that the crime from which the proceeds stemmed from was a particular crime or category of crime (such as Canadian designated offences), and instead can rely on the "irresistible inference" from the circumstances that the proceeds could only be derived from crime. For example, if the accused leads a lavish lifestyle but cannot account for the legitimate source of his/her funds, the Crown could argue that the circumstances justify such an irresistible inference and would not have to prove that funds stemmed from any particular crime or category of crime.

(ii) Witness Testimony

The RCMP indicated during their committee testimony that professional money launderers are aware that they have to be linked to the predicate offence to be convicted of money laundering, and have structured their criminal business accordingly to insulate them from the predicate offences, which makes it very difficult for the RCMP to investigate and prosecute these individuals. In order to address this, the RCMP recommended lowering the legal standard for an accused's awareness of the criminality of the funds from wilful blindness to recklessness.

Marc Tassé recognized the difficulty prosecutors encounter in proceeding with money-laundering charges because of the complexity of linking money laundering to predicate offences. He explained that Canada's reputation is in jeopardy, as terms such as "snow washing" and the "Vancouver model" of money laundering are now associated with Canada, and therefore recommends that the government bring forward Criminal Code amendments to make money laundering easier to investigate and prove, and suggests that additional resources be made available to law enforcement and prosecutors to pursue money-laundering crime. Canadians for Tax Fairness also made reference to "snow washing," where criminals make use of legitimate Canadian investments – such as real estate – to "clean" the proceeds of crime, and argued in favour of stiffer penalties and greater transparency to be built into the AML/ATF system. Peter German, who appeared as an individual, noted that the RCMP largely abandoned their AML work to focus their efforts on terrorism in the wake of the 9/11 attacks, and are only now re-entering the area.

During the Committee's travels, certain witnesses contended that the Canadian AML/ATF regime is not affective at curtailing sophisticated money laundering operations, though it may be more successful at curtailing smaller criminal operations. Some noted that there is a perception that Canada does not appear to take money laundering seriously, and the addition of dedicated prosecution units, expert witnesses, as well as specialized judges and courts would provide both perceived strength and actual benefit to the AML/ATF regime.

These witnesses also told the Committee that the U.K. prosecutes approximately 1,500 individuals for money laundering each year and has recovered over $2 billion since 2002 under their AML legislation. In addition, witnesses noted that the U.K. identified professional money laundering as the biggest problem for the AML regime in 2015, and remains the biggest problem today.

With respect to individuals charged with terrorist financing, witnesses believed that the U.K. prosecutes approximately five individuals each year, and they noted that public understanding of terrorist financing does not reflect the modern reality of the crime. In particular, they mentioned that the five most recent terror attacks in the U.K. were perpetrated at a total cost of under £4,000 and did not involve large or international transfers of funds, but rather inexpensive acts such as renting a vehicle to be used as a weapon. They contended that combatting terrorist activity through a financial lens should now consist of behavioural analysis software that has access to the suspect's financial data. Other witnesses advocated that all AML risk analysis should move towards implementing this type of behavioural analysis, as opposed to purely financial pattern analysis.

B. BULK CASH AND BEARER INSTRUMENTS

(i) Background

The ownership of bearer shares, bearer certificates and bearer share warrants – which function like common share ownership – is not registered with the associated corporation, as these instruments exist only as a physical document the owner carries. The Financial Action Task Force and the Global Forum on Transparency and Exchange of Information for Tax Purposes have identified bearer instruments as vehicles for laundering money and financing terrorism.

Bill C-25, An Act to amend the Canada Business Corporations Act, the Canada Cooperatives Act, the Canada Not-for-profit Corporations Act and the Competition Act received royal accent on 1 May 2018, and amended the CBCA and the *Canada Cooperatives Act* to clarify that bearer shares, bearer certificates and bearer share warrants are prohibited from being

HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

issued. Under the Act, shareholders or cooperative members that currently hold such instruments can convert them into a registered form of security, such as a common share. Furthermore, in December 2017, the federal and provincial/territorial finance ministers agreed in principle to pursue amendments to federal, provincial and territorial corporate statutes to eliminate the use of bearer shares and bearer share warrants or options and to replace existing ones with registered instruments.

FATF's most recent Mutual Evaluation of Canada identified bulk cash movement as a serious concern with respect to money laundering, as little to no record of ownership or origins may be ascertained. Furthermore, FATF notes that businesses that deal in large volumes of cash are highly vulnerable to money laundering and/or terrorist financing, such as: casinos, bars, restaurants, dealers in precious metals and stone, as well as the real estate sector.

(ii) Witness Testimony

André Lareau, who appeared as an individual, stated that bearer shares are commonly used in relation to tax evasion and noted that despite the amendments made by Bill C-25, bearer shares that have already been issued will continue to remain legal, and their holders are under no obligation to convert them into registered securities. He felt that the example of the Netherlands – where bearer shares are no longer allowed – should be explored by the government, as the system implemented in that jurisdiction allows holders of bearer instruments a period of two years to exchange them for register securities, after which they are deemed void. Transparency International Canada and Christian Leuprecht, who appeared as an individual, also recommended eliminating bearer instruments beyond the steps that the government implemented through Bill C-25.

The Committee heard testimony with respect to the Agreement to Strengthen Beneficial Ownership Transparency; in particular, reference was made to point 2 which states that "Ministers agreed in principle to pursue amendments to federal, provincial and territorial corporate statutes to eliminate the use of bearer shares and bearer share warrants or options and to replace existing ones with registered instruments." Christian Leuprecht also supported amending both federal, provincial and territorial corporate statutes to eliminate the use of bearer instruments and to replace existing ones with registered instruments.

With regards to the movement of large quantities of cash, Christian Leuprecht suggested that only the actual account holder should be allowed to make cash deposits into an account, and above a certain limit, such deposits should only be allowed in person subject to identification requirements. Furthermore, he went on to promote the

removal of $100 and $50 bills from circulation, as most Canadians do not use large bills for the majority of transactions, and these denominations are the greatest facilitator of money laundering. The Canadian Jewellers Association suggested that all luxury product dealers (i.e. cars, boats, works of art) should be required to report large cash transactions to FINTRAC. This position is supported by the Government of British Columbia. Moreover, it suggested that luxury items are of interest to money launderers because there is no tracking by government of cash purchases, and – with respect to bulk cash – that approximately $5 million per month of "suspicious cash transactions" entered the financial system through the casinos of British Columbia.

> "*Mr. Chair, I can say that my mind was, indeed, blown. The regulator walked me through extensive and overwhelming evidence of large-scale money laundering in Lower Mainland casinos. I was shown video and photographs of individuals wheeling large suitcases packed with $20 bills, others bringing stacks of cash to casino cages. I was astounded by the audacity of those involved. On a purely practical matter, $800,000 in twenties is very heavy. It looked like they were helping somebody move a box of books.*"
>
> Hon. David Eby,
> Attorney General of British Columbia,
> Government of British Columbia.

C. GEOGRAPHIC TARGETING ORDERS

(i) Background

Within the U.S., Section 5326 of the *Bank Secrecy Act* authorizes FinCEN to impose specialized reporting and recordkeeping requirements on financial institutions and nonfinancial trades or businesses over a limited time period. The requirements are imposed through a Geographical Targeting Order (GTO) that specifies the entities and geographical areas covered. FinCEN may issue a Geographical Targeting Order on its own initiative or at the request of law enforcement. For example, FinCEN issued a GTO in 2016 with respect to certain high value real estate markets, and provided detailed information to assist with their compliance to the order. Orders of this nature are currently not provided for in the PCMLTFA.

HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

(ii) Witness Testimony

The Government of British Columbia recommended that the PCMLTFA be amended to enable law enforcement to utilize geographic targeting orders similar to those used in the United States. In their brief, they reasoned that geographic targeting orders can be useful tools in geographically specific high-risk sectors. This sentiment was also shared by the Canadian Life and Health Insurance Association who believed that geographic targeting orders could be a useful addition to Canada's AML/ATF regime and could also provide reporting entities with useful information. Transparency International Canada also supported the implementation of geographic targeting orders, and went on to elaborate that these orders may provide the flexibility to the federal government to establish, on a temporary basis, obligations targeting persons or entities in certain geographic locations that represent a higher risk for money laundering and terrorist financing.

While traveling, the Committee heard from several witnesses who identified GTO's as particularly useful to the U.S.'s AML/ATF regime.

D. TRADE TRANSPARENCY UNITS

(i) Background

In order to combat trade based money laundering, which aims to misuse international trade to transfer value, the U.S. have established the Trade Transparency Unit to compare domestic and corresponding international trade data to detect and investigate anomalies that may be the result of trade based money laundering. U.S. Immigration and Customs Enforcement initiated the Trade Transparency Unit concept in Washington, D.C., in 2004 and subsequently established foreign Trade Transparency Unit partnerships with several countries.[21]

(ii) Witness Testimony

In their written submission, Transparency International Canada proposed strengthening the detection of trade-based money laundering by designating the Canada Border Services Agency's imports and exports database for purposes related to law enforcement, and share access to it with FINTRAC in order to enhance FINTRAC's ability to collect and produce financial intelligence on potential trade-based ML/TF.

21 For additional information on the United States Trade Transparency Unit, see: U.S. Department of State, *Trade Transparency Units*, March 2005.

Additionally, Transparency International Canada indicated that the Canada and the U.S. should harmonize the collection and reporting of monetary instruments at the border.

During the Committee's travels, witnesses noted that criminal typologies are changing rapidly, and sophisticated crime is becoming increasingly international in nature. Domestic financial intelligence units must adapt to this typology by building more co-operative international approaches to AML/ATF. They also noted that currency entering Canada in a manner that is designed to avoid other jurisdictions' currency controls is not necessarily the proceeds of criminal activity.

E. COMPLIANCE AND ENFORCEMENT MEASURES

(i) Background

FINTRAC and FinCEN are under the authority of the Department of Finance and the Department of the Treasury, respectively, which are responsible for federal finances. However, the USA Patriot Act authorizes FinCEN to undertake certain activities, described in Chapter 2, that FINTRAC is not authorized to undertake. Meanwhile, the United Kingdom Financial Intelligence Unit reports to the Home Office, which is responsible for security, counterterrorism, immigration and policing.

Having FINTRAC under the authority of the Department of Finance reinforces the links that exist between FINTRAC and Canadian financial institutions; it also ensures that developments in the financial system are quickly communicated to FINTRAC. That said, this structure could result in a degree of detachment between FINTRAC and law enforcement agencies.

Parts 4.1 to 6 of the PCMLTFA describe offences under the Act as well as the monetary penalties and other types of punishments that can be imposed by FINTRAC against entities that violate the Act. Section 73.22 of the PCMLTFA provides FINTRAC with the discretionary power to publicize certain information related to an administrative monetary penalty when proceedings with respect to a violation have ended, including all opportunities for appeal.

In the 2016 case of Kabul Farms Inc. the Federal Court of Appeal found that there was no transparency in the administrative monetary penalty FINTRAC levied against the corporation, which was inconsistent with FINTRAC's obligations of procedural fairness. The court quashed the penalties and returned the matter to FINTRAC for re-determination of whether a penalty should be imposed and, if so, in what amount.

HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Subchapter II of the *Bank Secrecy Act* and its corresponding regulations authorize FinCEN to impose civil money penalties for violations of the Act and its regulations in the United States. For each failure to file a report, FinCEN may impose a civil money penalty equal to the amount involved in the transaction between $25,000 and $100,000 USD. Furthermore, FinCEN may impose a civil money penalty of $25,000 for each day that a financial institution has failed to implement a reasonably designed AML program.

Section 311 of the Patriot Act, which grants the Secretary of the Treasury the authority, upon finding that reasonable grounds exist for concluding that a foreign jurisdiction, institution, class of transaction, or type of account is of "primary money laundering concern," to require domestic financial institutions and financial agencies to take certain "special measures" against that entity in order to restrict their access to the U.S. financial system.[22]

In addition, section 319(b) of the Patriot Act allows the government to seize illicit funds located in foreign countries by authorizing the Attorney General or the Secretary of the Treasury to issue a summons or subpoena to any foreign bank that maintains a correspondent account in the U.S. for records related to such accounts. Section 352 of the Act requires financial institutions to establish anti-money laundering programs, which at a minimum must include: the development of internal policies, procedures and controls; designation of a compliance officer; an ongoing employee training program; and an independent audit function to test their programs.[23]

(ii) Witness Testimony

The Investment Industry of Canada, Transparency International Canada and Christian Leuprecht, who appeared as an individual, recommended publicizing the names those who have been found to have violated their obligations under the PCMLTFA. The Canadian Life and Health Insurance Association added that regulators should wait until the conclusion of proceeding before publicly naming violators of the Act. They also support the publication of criteria for publicly naming an offending entity as well as the criteria for the calculation of monetary penalties. However, Transparency International Canada indicated that penalties for non-compliance should be sufficiently large to dissuade entities from simply factoring them into their costs of doing business. Canadians for Tax Fairness suggested that there is need for stiffer penalties to improve transparency.

22 See for example: U.S. Department of the Treasury, Fact Sheet: Overview of Section 311 of the USA PATRIOT Act, accessed 27 June 2018.

23 A number of other provisions of the Patriot Act are used by FinCEN. See: the Financial Crimes Enforcement Network, USA PATRIOT Act, accessed 27.06.2018.

From the perspective of the regulators, the Department of Finance indicated that reporting entities are also partners in the AML/ATF regime, and the use of discretion in publicizing the names of those who violate their AML/ATF obligations can facilitate this partnership. In FINTRAC's opinion, the government could consider whether the PCMLTFA's penalty calculations should be directly in the regulations, but that it is currently conducting a review of its administrative monetary penalty program as a consequence of the decision of the Federal Court of Appeal in Kabul Farms. It further explained that they are consulting with the Department of Justice in this review, which they hope will be completed by summer 2018.

Christian Leuprecht suggested the expansion of FINTRACs mandate to allow for the legal authority to conduct investigations in addition to passive analyses.

While traveling, witnesses informed the Committee that the U.K.'s Financial Conduct Authority requires corporations to appoint an AML manager among its senior employees and publicizes the names of companies that are fined for AML violations. In addition, they mentioned that the U.K.'s HMRC and OPBAS, and the U.S. Treasury also publicize entities found to commit AML violations in their respective areas of oversight.

Witnesses also speculated that the expansion of FINTRACs mandate to allow for the legal authority to conduct investigations may be beneficial, but noted that the structure of a country's anti-money laundering and anti-terrorist financing regime reflects that country's needs.

Chapter 3 Recommendations

Recommendation 20

The Committee recommends, in recognizing the difficulty prosecutors have in laying money-laundering charges due to the complexity of linking money laundering to predicate offences, that the Government of Canada:

- **bring forward Criminal Code and Privacy Act amendments in order to better facilitate money laundering investigations;**
- **any necessary resources be made available to law enforcement and prosecutors to pursue money-laundering and terrorism financing activities.**

HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Recommendation 21

That the Government of Canada expand FINTRAC oversight to ensure that all casino operators, employees, and frontline gaming personnel are trained in anti-money laundering legislation.

Recommendation 22

That the Government of Canada establish an information sharing regime through FINTRAC and provincial gaming authorities to ensure more accurate and timely reporting.

Recommendation 23

That the Government of Canada amend the PCMLTFA to enable law enforcement agencies to utilize geographic targeting orders similar to those used in the United States.

- **Federal, provincial, and territorial governments should collaborate to close the loophole regarding the transaction of sales between parties who are not subject to PCMLTFA reporting requirements, which creates vulnerability for money laundering to occur.**

Recommendation 24

That the Government of Canada follow the example of the Netherlands, which gives holders of bearer shares – now prohibited – a fixed period of time to convert them into registered instruments before they are deemed void.

CHAPTER 4: MODERNIZING THE REGIME

Witnesses provided comments with respect to areas of the regime that they believed could be improved by a number of changes; these areas include:

- virtual currency and money service businesses,
- compliance and the administrative burden,
- suspicious transaction reporting, and
- sanctions lists.

A. VIRTUAL CURRENCY AND MONEY SERVICE BUSINESSES

(i) Background

Money services businesses (MSBs) are traditionally those that exchange currencies, transfer money, and/or cash or sell money orders and traveller's cheques. In Canada, MSBs are required to register with FINTRAC, follow the AML/ATF reporting and record-keeping requirements, verify the identity of clients for certain kinds of transactions, and operate a PCMLTFA compliance program.

Initial Coin Offerings (ICOs) occur when a company creates a new cryptocurrency or digital token and offers them to the general public who may purchase them in whatever manner that company specifies, such as using fiat currency or other cryptocurrencies.[24] ICOs could be viewed as similar to Initial Public Offerings (IPOs) where a company offers their stocks to the public for the first time. However, a company's stock is connected to corporate ownership and/or performance, while the new crypto currency or digital token offered in an ICO may only be connected to a particular project that the company is pursuing. For example, a company could offer digital token through an ICO that can only be redeemed for a particular service that the company currently or hopes to provide in the future, and the monetary value of that token may fluctuate over time based on the market value of that service. The Canadian Securities Administrators published CSA Staff Notice 46-308 Securities Law Implications for Offerings of Tokens, which provides guidance on the applicability of securities laws to ICOs. Broadly speaking,

24 Initial Coin Offerings may also be referred to as Initial Token Offerings (ITOs).

HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

the Canadian provincial/territorial securities regulators will have the jurisdiction to regulate an ICO if the offering constitutes a security.

In the U.S., FinCEN updated certain definitions and other regulations relating to MSBs in 2011 to include virtual currency exchange businesses as "money transmitters," which are a type of MSB under FinCEN's rules and therefore subjected virtual currency exchange businesses to the U.S. AML/ATF regime. In particular, any business that accepts and transmits a convertible virtual currency or buys or sells convertible virtual currency for any reason is a money transmitter under FinCEN's regulations. Money transmission services are defined as "the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means." MSB's must be registered with FinCEN, and must renew that registration every two years. In addition, certain American states require licences for virtual currency business activity; for example, the state of New York implemented a BitLicense Regulatory Framework.

On 19 April 2018, the European Parliament adopted the European Commission's proposal for a Fifth Anti-Money Laundering Directive (AMLD5) to prevent terrorist financing and money laundering through the European Union's financial systems, and addresses – among other things – the potential money laundering and terrorist financing risks posed by virtual currencies. AMLD5 responds to these risks by expanding the scope of the previous directives by including virtual currency exchanges and virtual currency wallet providers as "obliged entities" subject to EU regulations. Virtual currency exchanges and virtual currency wallet providers now face the same regulatory requirements as banks and other financial institutions, which include obligations to register with national anti-money laundering authorities, implement customer due diligence controls, regularly monitor virtual currency transactions, and report suspicious activity to government entities.

On 9 June 2018, the Department of Finance published proposed regulations under the Act, which included measures targeted at virtual currency exchanges. These exchanges will be treated as MSBs, and any persons or entities dealing in virtual currencies will need to implement a full AML/AFT compliance program and register with FINTRAC. In addition, all reporting entities that receive $10,000 or more in virtual currency will have similar record-keeping and reporting obligations. Furthermore, reporting entities such as MSBs will be required to conduct a risk assessment of their vulnerability to money laundering and terrorist financing activities, and take reasonable measures to determine the sources of a politically exposed person's wealth.

(ii) Witness Testimony

Witnesses commented on the legal terminology used in the cryptocurrency space and the implications of this terminology on the PCMLTFA. The Dominion Bitcoin Mining Company suggested that Canada needs to have easily recognizable, clear, and defensible legal definitions of blockchain-backed digital tokens. To achieve this, they proposed that the PCAMLTF use definitions based on three readily identifiable functions: "cryptocurrency", "utility tokens" and "security tokens". Each is defined as follows:

- cryptocurrency: blockchain-based decentralized payment and settlement systems, for example Bitcoin, Bitcoin Cash, and others;
- utility tokens: blockchain-based digital tokens designed to represent future access to a company's product or service, for example: Ethereum;
- security tokens: blockchain-based digital assets that derive their value from an external, tradable assets or equity, and are subject to provincial securities regulations. Commonly referred to as "tokenized assets."

The Dominion Bitcoin Mining Company also proposed a multi-year "sandbox" initiative where regulated entities in the cryptocurrency space could operate in a somewhat self-regulated manner, sharing information at regular intervals with the regulator.

In their written submission to the Committee, Durand Morisseau LLP and IJW & Co. Ltd. indicated that the definition of "virtual currency" proposed in the Department of Finance's newly published regulations concerning virtual currency exchanges is insufficient, as it promotes the perception that it is:

1) a "currency", which they believe it is not;
2) a "digital currency," which they believe it should not be, as there is no definition under current Canadian legislation;
3) a form of "electronic money", for which no definition exists under current Canadian legislation; or
4) money, which they believe it is not.

Durand Morisseau LLP and IJW & Co. Ltd. went on to explain that it is not possible to ascertain whether the current definition of "virtual currency" would capture ICOs. Thus, it recommended that the definition of "virtual currency" should be replaced by

HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

"cryptoasset" so as to avoid ambiguity. Durand Morisseau LLP and IJW & Co. Ltd. argued that "cryptoasset" could be defined (as per the EU banking authorities) as: "a digital representation of value that is not issued or guaranteed by a central bank or a public authority, it is not necessarily attached to a legal established currency, and does not possess a legal status of currency or money, but is accepted by natural or legal persons, as a means of exchange, and which can be transferred, store and traded electronically." On the other hand, Dominion Bitcoin Mining Company recommended that crypto-currency be defined as non-fiat money in the *Currency Act*, empowering the Governor in Council to dictate a matrix for valuation.

Prior to releasing their new regulations, the Department of Finance explained to the Committee that they intended on bringing those regulations forward with the aim of re-establishing a level playing field for dealers in virtual currencies. They noted that the technology has the potential to revolutionize the financial technology sector but comes with risks and challenges, such as the tension between the anonymity of the currencies and KYC requirements. In his testimony to the Committee, Jeremy Clark – who appeared as an individual – identified two "postures" in dealing with illicit cryptocurrency activity, prevention and detection. In his opinion, prevention will fail given that cryptocurrencies are an open, internet-based technology, and hence the focus of these efforts should be invested in the detection of suspicious activity. The Blockchain Association of Canada reasoned that the detection of criminal activities should be done in collaboration with cryptocurrency exchanges. Académie Bitcoin also concluded that peripheral actors, such as exchanges, could deploy the security protocols required by the current money laundering and terrorist financing regime. Moreover, Jeremy Clark suggested that exchanging fiat currency into cryptocurrency and vice versa – also known as on ramps and off ramps – is where financial reporting should be dealt with. This opinion is also shared by Durand Morisseau LLP and IJW & Co. Ltd. as they underscored that it would be most prudent for Canada to concentrate its regulatory efforts on cryptocurrency exchanges to provide the greatest public benefit, and that this approach is imperative as users of cryptocurrency exchanges are theoretically able to transact in near complete anonymity. They further explained that in the absence of some degree of regulatory oversight, cryptocurrency transactions may be used by parties to swiftly move large amounts of wealth across borders, and that regulating the following conversion mechanisms would address the AML concerns of the cryptocurrency space:

1) cryptocurrency exchanges, which are operations that allow their users to exchange cryptocurrency for fiat currency or for other types of cryptocurrency and vice versa;

2) cryptocurrency ATMs, which are machines that allow users to exchange cryptocurrency for fiat currency and vice versa; and

3) conversion of fiat or cryptocurrency into an ICO, which is the method by which a user would exchange fiat currency or another cryptocurrency to purchase ICO tokens or coins issued by a start-up business.

Durand Morisseau LLP and IJW & Co. Ltd. stated that these are the points in which the enforcement of AML and KYC requirements pertaining to cryptocurrencies should occur, and that sufficient KYC information would consist of collecting the identities of the parties opening accounts (known as "wallets") at cryptocurrency exchanges, as well as their sources of funds (e.g., fiat currency that is exchanged into cryptocurrency) that are deposited into the wallets to be used in transactions.

The Government of British Columbia informed the Committee that many money services businesses are unregistered and are a fixture of the underground economy as the modern embodiment of underground banking, serving to transfer ownership of money around the world without the need for the actual transmission of fiat currency.

When questioned on cryptocurrencies, the ATM Industry Association indicated that their ATM infrastructure does not support cryptocurrencies.

During the Committee's travels, a number of witnesses spoke about the opportunities that cryptocurrencies might provide for criminal activities. Some witnesses estimated that 80% of the value of cryptocurrencies could be linked to the proceeds of illegal activities, and that while the risk of cryptocurrencies being used to launder money is low, it is a very high risk for being used as a payment method for criminal activity.

Certain witnesses commented that certain blockchain based technologies – such as secure key – should be able to fulfil the KYC requirements of reporting entities, but this is not permissible under the current legislative framework. Many of these witnesses also commented that the lack of any cryptocurrency regulation in Canada presents challenges and risks for both consumers and cryptocurrency related businesses.

With respect to the anonymity of cryptocurrency, certain witnesses during the Committee's travels presented opposing views on whether and/or how this aspect of cryptocurrency facilitates ML/TF. For example, Bitcoin transactions have been described as "pseudo-anonymous" because a record of all bitcoin transfers is recorded on the blockchain. However, the identities of participants in a transaction are encrypted through the use of their digital wallet and no personal information is recorded or transferred. The latter

characteristic leads some witnesses to described Bitcoin as functionally anonymous. Furthermore, other cryptocurrencies – such as Monero – advertise themselves as being completely anonymous and untraceable. On the other hand, witnesses informed the Committee that the U.S. government in partnership with the private sector has previously identified the personal identities of Bitcoin users for criminal prosecution. Government regulation could address some of these issues, such as regulations requiring a registry of wallet addresses linked to personal identities and placing KYC requirements on cryptocurrency exchanges and all ICOs.

Some of these witnesses identified ICOs as the largest risk to consumers in the cryptocurrency space, as those that are not characterized as a security have little or no consumer protection. Others highlighted that law enforcement requires training and education in the area of cryptocurrency and its uses.

B. COMPLIANCE AND THE ADMINISTRATIVE BURDEN

(i) Background

Compliance with the PCMLTFA comes at a cost to reporting entities, which may differ considerably between the business under the regime. Various witnesses spoke about reducing the AML/ATF reporting standards on entities that are relatively low risk for money laundering and terrorist financing and/or the financial costs of compliance with current standards, while other witnesses took the position that such standards must be maintained across all reporting entities to have an effective regime.

(ii) Witness Testimony

The Canadian Life and Health Insurance Association argued that the benefit of having reporting requirements for reporting entities should be weighed against the related implementation and operational costs for the government and the industry. HSBC Bank Canada signalled the need for additional action to reduce compliance costs and move to a more “risk-based” reporting standard.

The Canadian Credit Union Association indicated that money laundering and terrorist financing obligations impose a burden on smaller financial institutions, and recommended the adoption of a risk-based model in order to decrease the administration burden without affecting the value or quality of the gathered information. The Investment Industry Association of Canada highlighted the need to improve the efficiency of reporting and to reduce the compliance burden on securities dealers and other reporting entities; in particular, it suggested the following:

- legislation should be flexible to accommodate new technologies, such as digital identification in the verification process, and it should be sufficiently flexible to enable timely adaptation of a range of innovative technology;

- section 62(2) of the PCMLTFA – which provides certain exemptions from the record-keeping and verification requirements for reporting entities – could be expanded to certain foreign-regulated entities that are subject to a comparable regulatory regime to Canada so as not to duplicate efforts.

FINTRAC told the Committee that reviewing the administrative burden facing businesses is a priority for the organization, and that it will work with businesses in its review, but that the information required in these reports is necessary for a functional AML/ATF regime. With respect to smaller reporting entities having a disproportionate compliance burden, they explained that these organizations only file a fraction of the reports that large financial institutions do, and that they are taking steps to ascertain what – if any – burdens disproportionately affect smaller reporting entities.

During the Committee's travels, witnesses disagreed about the effect and/or extent of the administrative burden in the AML/ATF regime. On the one hand, many witnesses contended that the extent to which reporting entities undertake AML/ATF is far greater than the efforts of the government, which is overly costly for their operations. Others commented on a disproportionate burden that is placed on lower ML/TF risk sectors, and/or a lack of capacity in smaller reporting entities to run similar AML/ATF operations as larger financial institutions. In particular, some witnesses favoured moving the AML/ATF regime to a risk-based compliance model to address these concerns. Certain witnesses explained that the U.K. favours a risk-based compliance model where credit unions are subjected to lower AML/ATF requirements then larger banks, and that U.S. reporting entities are capable of filing simplified "skinny reports" in certain circumstances.

On the other hand, witnesses commented that compliance measures should generally be placed equally on all businesses to prevent weak links in the AML/ATF regime, and that while businesses always argue in favour of lowering their operational costs, the cost of compliance is simply the cost of doing business in a properly functioning sector. Witnesses further explained that many of the U.K.'s AML/ATF oversight bodies are funded through the fees collected from the entities that they regulate.

Some of these witnesses also argued that the size and complexity of the AML/ATF regulations make them unnecessarily cumbersome, and that regulatory simplification and additional direction from FINTRAC would help lower the costs of compliance for reporting

HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

entities. They pointed to the U.K., which regularly undertakes a national risk assessment of its AML regime, and works with the private sector to improve its operation.

C. SUSPICIOUS TRANSACTION REPORTING

(i) Background

Reporting entities in Canada must report to FINTRAC via a "Suspicious Transaction Report" (STR) on completed or attempted transactions if there are reasonable grounds to suspect that the transaction was related to the commission or attempted commission of a money laundering offence or a terrorist activity financing offence.

STR's are reported separately from large cash transaction reports, under which reporting entities must report to FINTRAC within 15 calendar days if they receive an amount of $10,000.00 or more for a single transaction or a number of transactions from the same individual or entity within 24 hours.

In the U.S., a financial institution is required to file a Suspicious Activity Report (SAR) – roughly equivalent to a STR – on suspicious transactions with respect to possible violations of any law or regulation. The U.K. also makes use of SARs, which are submitted based on a threshold of knowledge or suspicions of money laundering, or belief or suspicions relating to terrorist financing.

(ii) Witness Testimony

The Canadian Life and Health Insurance Association encouraged officials to consider introducing a minimum dollar threshold for suspicious transaction filing, as there is currently no such threshold. However, Christian Leuprecht proposed removing the reporting threshold in large cash transaction reports for international transactions entirely, as he believes the $10,000.00 threshold was arbitrary and had no academic basis. Mr. Leuprecht also contended that removing the threshold would greatly improve FINTRAC's transactional awareness, and make reporting easier, more efficient, and less costly because financial institutions would no longer have to filter transactions by this threshold. The Canadian Real Estate Association recommended modernizing FINTRAC's "F2R online suspicious transaction report portal," as certain aspects of the report are not relevant to the realtor industry and cause confusion and unnecessary reporting errors.

HSBC Bank Canada, the Canadian Credit Union Association and the Investment Association of Canada recommended action to reduce compliance costs through

innovation and reporting reforms to streamline the reporting process, and the Blockchain Association of Canada suggested that government work with industry – particularly the exchanges – to build the systems for collecting actionable data.

During the Committee's travels, witnesses debated the merits of the volume of reporting required under the U.S., U.K. and Canadian regimes, as well as the quality of the information being collected. Certain witnesses highlighted the high volumes of information that are provided to the respective financial intelligence units. They also questioned the value of this data or the extent to which it leads to immediate criminal investigations or prosecutions. Conversely, other witnesses argued that all such data is necessary to the development of a financial intelligence unit's computer modelling and data analytics that underpin their operations. They contend that a ratio of reports submitted to investigations undertaken is not an appropriate measure of success, and that it would be more appropriate to measure success by the extent to which those reports are used to develop informative trends and typologies.

Some witnesses believed that it is problematic that the reporting activity of reporting entities is largely driven by the fear of being fined or otherwise reprimanded by their respective regulators, while others believed that such a situation is an example of a properly functioning regulatory regime.

Certain witnesses commented that the format of the STR could be updated in a number of ways; these included: simplification for ease of use and understanding, clearer directions on how to complete these forms, the use of "drop-down boxes" for greater clarity, and the possibility of adapting the forms to the needs of specific reporting entities as opposed to a "one-size fits all" report.

D. SANCTIONS LISTS

(i) Background

The FATF recommends countries implement a targeted financial sanctions regime to comply with the United Nations Security Council Resolutions relating to the prevention and suppression of terrorism and terrorist financing, and believes that efforts to combat terrorist financing are greatly undermined when countries do not quickly and effectively freeze the funds or other assets of designated persons and entities.

Canadian sanctions laws implement United Nations Security Council sanctions regimes under the *United Nations Act*, as well as Canadian autonomous sanctions regimes under the *Special Economic Measures Act*. In addition, the *Justice for Victims of Corrupt Foreign*

HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Officials Act enables Canada to impose sanctions against foreign nationals in a foreign state for human rights abuses or against foreign public officials and their associates who are responsible or complicit in acts of significant corruption. A Consolidated Canadian Autonomous Sanctions List is made available by Global Affairs Canada.

(ii) Witness Testimony

During the Committee's travels, certain witnesses brought to the Committee's attention that lawyers and real estate agents do not check their clients against sanctions list, and that no list of ML/TF bad actors is readily accessible in Canada apart from that provided by Global Affairs Canada, which is of limited use to the AML regime. In contrast, witnesses said that the U.K.'s Office of Financial Sanctions Implementation keeps a consolidated sanctions list that reporting entities must use to screen their clients.

Chapter 4 Recommendations

Recommendation 25

That the Government of Canada regulate crypto-exchanges at the point that fiat currency is converted so as to establish these exchanges as money service businesses (MSB).

Recommendation 26

That the Government of Canada establish a regulatory regime for crypto-wallets so as to ensure that proper identification is required, and that true ownership of wallets is known to the exchanges and law enforcement bodies if needed.

- **Ensure that bitcoin purchases of real estate and cash cards are properly tracked and subjected to AML regulation;**
- **Law enforcement bodies must be able to properly identify and track illegal crypto-wallet hacking and failures to report capital gains.**

Recommendation 27

That the Government of Canada establish a license for crypto-exchanges in line with Canadian law, which includes an anti-money laundering program and look to the State of New York's program as a model for best practices.

Recommendation 28

That the Government of Canada consider prohibiting nominee shareholders. However, if nominee shareholders are permitted, they should be required to disclose their status upon the registration of the company and registered as nominees. Nominees should be licensed and subject to strict anti-money laundering obligations.

Recommendation 29

That the Government of Canada include clearer directions and streamline the reporting structure of Suspicious Transaction Reports, such as through the use of 'drop-down boxes,' to increase ease of use by specific reporting entities and ensure better compliance.

Recommendation 30

That the Government of Canada change the structure of FINTRAC's Suspicious Transaction Report to resemble the Suspicious Activity Reports used in the United Kingdom and the United States in order to focus on suspected violations rather than an arbitrary monetary threshold.

Recommendation 31

That the Government of Canada enhance the direct reporting system of casinos to FINTRAC through the suspicious transaction reports to include suspicious activities.

Recommendation 32

That the Government of Canada update reporting regulations for financial institutions to include bulk online purchasing of store gift cards or prepaid credit cards.

APPENDIX A
LIST OF WITNESSES

The following table lists the witnesses who appeared before the Committee at its meetings related to this report. Transcripts of all public meetings related to this report are available on the Committee's webpage for this study.

Organizations and Individuals	Date	Meeting
Department of Finance	2018/02/08	131
Maxime Beaupré, Director Financial Crimes Policy		
Annette Ryan, Associate Assistant Deputy Minister Financial Sector Policy Branch		
Ian Wright, Director Financial Crimes Governance and Operations		
Department of Foreign Affairs, Trade and Development	2018/02/14	133
Jamie Bell, Executive Director International Crime and Terrorism		
Department of Industry	2018/02/14	133
Mark Schaan, Director General Marketplace Framework Policy Branch		
Financial Transactions and Reports Analysis Centre of Canada	2018/02/14	133
Luc Beaudry, Assistant Director Collaboration, Development and Research Sector		
Dan Lambert, Assistant Director Intelligence, Operations		
Joane Leroux, Assistant Director Regional Operations		
Office of the Superintendent of Financial Institutions	2018/02/14	133
Erin Feeney, Director Anti-Money Laundering and Compliance Division		
Christine Ring, Managing Director Anti-Money Laundering and Compliance Division		

Organizations and Individuals	Date	Meeting
Canada Border Services Agency	2018/02/26	134
Sébastien Aubertin-Giguère, Director General Traveller Program Directorate		
Canadian Security Intelligence Service	2018/02/26	134
Cherie Henderson, Director General Policy and Foreign Relations		
Department of Justice	2018/02/26	134
Paul Saint-Denis, Senior Counsel Criminal Law Policy Section		
Department of Public Safety and Emergency Preparedness	2018/02/26	134
Trevor Bhupsingh, Director General Law Enforcement and Border Strategies Directorate		
John Davies, Director General National Security Policy		
Office of the Director of Public Prosecutions	2018/02/26	134
George Dolhai, Deputy Director of Public Prosecutions		
Royal Canadian Mounted Police	2018/02/26	134
Joanne Crampton, Assistant Commissioner Federal Policing Criminal Operations		
Canada Revenue Agency	2018/02/28	135
Alastair Bland, Director Review and Analysis Division, Charities Directorate, Legislative Policy and Regulatory Affairs Branch		
Stéphane Bonin, Director Criminal Investigations Division, Criminal Investigations Directorate, International, Large Business and Investigations Branch		
Tony Manconi, Director General Charities Directorate, Legislative Policy and Regulatory Affairs Branch		

Organizations and Individuals	Date	Meeting
Department of Public Works and Government Services	2018/02/28	135
Lynne Tomson, Director General Integrity and Forensic Accounting Management Group, Integrity Branch		
Nicholas Trudel, Director General Specialized Services Sector, Integrated Services Branch		
Office of the Privacy Commissioner of Canada	2018/02/28	135
Lara Ives, Acting Director General Audit and Review		
Daniel Therrien, Privacy Commissioner of Canada		
Kate Wilson, Legal Counsel		
Académie Bitcoin	2018/03/19	137
Jonathan Hamel, President		
As an individual	2018/03/19	137
Shahin Mirkhan, Broker of Record Max Realty Solutions Ltd.		
Financial Transactions and Reports Analysis Centre of Canada	2018/03/19	137
Dan Lambert, Assistant Director Intelligence, Operations		
Joane Leroux, Assistant Director Regional Operations		
Barry MacKillop, Deputy Director Operations		
As an individual	2018/03/21	138
Mora Johnson, Barrister-Solicitor		
Canadian Jewellers Association	2018/03/21	138
Brian Land, General Manager		
Federation of Law Societies of Canada	2018/03/21	138
Sheila MacPherson, President		
Frederica Wilson, Executive Director and Deputy Chief Executive Officer Policy and Public Affairs		

Organizations and Individuals	Date	Meeting
Jewellers Vigilance Canada Inc.	2018/03/21	138
Phyllis Richard, Former Executive Director		
As an individual	2018/03/27	140
Jeremy Clark, Assistant Professor Concordia Institute for Information Systems Engineering, Concordia University		
Blockchain Association of Canada	2018/03/27	140
Kyle Kemper, Executive Director		
Canadian Real Estate Association	2018/03/27	140
Dina McNeil, Director Government Relations		
Simon Parham, Legal Counsel		
Government of British Columbia	2018/03/27	140
Hon. David Eby, Attorney General of British Columbia Ministry of Attorney General		
Investment Industry Association of Canada	2018/03/27	140
Ian Russell, President and Chief Executive Officer		
Transparency International Canada	2018/03/27	140
Denis Meunier, Senior Advisor on Beneficial Ownership		
As an individual	2018/03/28	141
André Lareau, Associate Professor Faculty of Law, Université Laval		
Canadian Bankers Association	2018/03/28	141
Stuart Davis, Chief Anti-Money Laundering Officer AML Enterprise, BMO Financial Group		
Sandy Stephens, Assistant General Counsel		
Canadian Credit Union Association	2018/03/28	141
Sabrina Kellenberger, Senior Manager Regulatory Policy		
Marc-André Pigeon, Assistant Vice-President Financial Sector Policy		
Canadian Life and Health Insurance Association	2018/03/28	141
Jane Birnie, Assistant Vice-President, Compliance Manulife		
Ethan Kohn, Counsel		

Organizations and Individuals	Date	Meeting
As individuals	2018/04/16	142
John Jason, Counsel Cassels Brock and Blackwell Limited Liability Partnership		
Marc Tassé, Senior Advisor Canadian Centre of Excellence for Anti-Corruption, University of Ottawa		
ATM Industry Association	2018/04/16	142
Curt Binns, Executive Director Canada Region		
Canadian Automobile Dealers Association	2018/04/16	142
Michael Hatch, Chief Economist		
Peter MacDonald, Chairman of the Board		
Foundation for Defense of Democracies	2018/04/16	142
Sheryl Saperia, Director of Policy for Canada		
Heffel Gallery Limited	2018/04/16	142
Andrew Gibbs, Representative Ottawa		
As individuals	2018/04/18	143
Vanessa Iafolla, Lecturer Department of Sociology and Legal Studies, University of Waterloo		
Christian Leuprecht, Professor Department of Political Science, Royal Military College of Canada		
Canadian Gaming Association	2018/04/18	143
Paul Burns, President and Chief Executive Officer		
Canadians for Tax Fairness	2018/04/18	143
Dennis Howlett, Executive Director		
Imperial Tobacco Canada Limited	2018/04/18	143
Eric Gagnon, Head Corporate and Regulatory Affairs		
Kevin O'Sullivan, Head Security and Intelligence		

Organizations and Individuals	Date	Meeting
Financial Transactions and Reports Analysis Centre of Canada	2018/05/24	158
Luc Beaudry, Assistant Director Collaboration, Development and Research Sector		
Barry MacKillop, Deputy Director Operations		
Nada Semaan, Director and Chief Executive Officer		
As individuals	2018/05/30	160
Milos Barutciski, Partner Bennett Jones LLP		
Peter German, President International Centre for Criminal Law Reform, University of British Columbia		
Department of Finance	2018/06/20	163
Hon. Bill Morneau, P.C., M.P., Minister of Finance		
Maxime Beaupré, Director Financial Crimes Policy		
Annette Ryan, Associate Assistant Deputy Minister Financial Sector Policy Branch		
Ian Wright, Director Financial Crimes Governance and Operations		

APPENDIX B
LIST OF BRIEFS

The following is an alphabetical list of organizations and individuals who submitted briefs to the Committee related to this report. For more information, please consult the Committee's webpage for this study.

Canadian Bar Association

Canadian Federation of Independent Business

Canadian Jewellers Association

Canadian Life and Health Insurance Association

Canadian Real Estate Association

Comeau, Kevin

Dominion Bitcoin Mining Company

Durand Morisseau LLP

Federation of Law Societies of Canada

Government of British Columbia

HSBC Bank Canada

IJW & Co. Ltd.

Imperial Tobacco Canada Limited

Investment Industry Association of Canada

Leuprecht, Christian

Office of the Information Commissioner of Canada

Ontario Lottery and Gaming Corporation

Transparency International Canada

REQUEST FOR GOVERNMENT RESPONSE

Pursuant to Standing Order 109, the Committee requests that the government table a comprehensive response to this Report.

A copy of the relevant *Minutes of Proceedings* (Meetings Nos. 131, 133, 134, 135, 137, 138, 140, 141, 142, 143, 158, 160, 162, 163, 179, 180, 182 and 186) is tabled.

Respectfully submitted,

Hon. Wayne Easter, P.C., M.P.
Chair

NDP Dissenting Report on the Statutory Review of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*

Restoring public trust with increased transparency: Establishing a public register of beneficial owners

The Liberal government promised to focus on openness and transparency in order to restore public trust in our institutions. During this study, numerous witnesses told the Committee that establishing a public register of beneficial owners of corporations and trusts would be an effective way of combatting tax evasion and money laundering. This register would also help rebuild Canadians' trust in our tax system and laws.

The Honourable David Eby, Attorney General of the Government of British Columbia, argued that this kind of register is needed, in part by citing a study from Transparency International Canada. The study showed that it is impossible to determine the true owners of more than half of real estate properties for sale. He also pointed to British Columbians' lack of confidence in the enforcement of tax laws and added that the public must have access to the register in order to remedy this crisis of confidence.

In addition, Canada would benefit from drawing on the European approach to a public register by including any person with significant control of 10% or more of a corporation or trust. The testimony heard from individuals in the United Kingdom further confirmed that an easily accessible public register is the right option for Canada.

Marc Tassé, Senior Advisor with the Canadian Centre of Excellence for Anti-Corruption at the University of Ottawa, noted the following: "With public access to the beneficial ownership information, the Act should also be amended to require all reporting entities to verify the identity of the beneficial owner; verify if their customers are politically exposed persons or their family members or associates; and identify the beneficial owner and verify their identity with government-approved ID before opening an account or completing a financial transaction."

It is important to remember that, like the many witnesses who appeared before the Committee, the government committed to fighting tax cheats and the fraudulent use of tax havens. One way to achieve this goal is obviously to increase transparency through the rules governing corporations and trusts so that beneficial owners can be identified and authenticated.

Furthermore, as did most of the witnesses, Denis Howlett of Canadians for Tax Fairness emphasized that the register must be "in an open, searchable format. That's our main recommendation." Barrister-Solicitor Mora Johnson added that a transparent public register would enable those searching the database to track the most common methods taxpayers use to avoid paying their fair share of taxes and to find individuals involved in money laundering.

The vast array of testimony that the Committee members heard was unequivocal: the federal government needs to co-work with the provinces to establish a central public

register that would provide the identity of the beneficial owners of corporations and trusts.

The Liberals and Conservatives chose to join forces and ignore the recommendation of the majority of the witnesses that a public register be established. We were discouraged to discover that the Liberals and Conservatives refuse to work closely with civil society to provide transparent, accessible and reliable information to Canadians. The NDP is disappointed that it must submit this dissenting opinion in order to highlight the blatant discrepancy between the testimony heard and the Committee's final recommendation regarding a register of beneficial owners of Canadian-registered corporations.

Appendix D:

Canada, Parliament, House of Commons, Standing Committee on Finance, *Government Response to the Twenty-Fourth Report of the Standing Committee on Finance*.

GOVERNMENT RESPONSE

INTRODUCTION

The Government of Canada is pleased to respond to the twenty-fourth Report of the House of Commons Standing Committee on Finance entitled *Confronting Money Laundering and Terrorist Financing: Moving Canada Forward*, tabled in the House of Commons on November 8, 2018.

The Government of Canada appreciates the work of the Committee and welcomes its analysis, views and recommendations, which we recognize are based on consultations with stakeholders and experts in the field of anti-money laundering and anti-terrorist financing (AML/ATF). The Government shares the Committee's commitment to better understand money laundering and terrorist financing in order to combat it effectively.

CANADA'S FIGHT AGAINST MONEY LAUNDERING AND TERRORIST FINANCING

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 *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (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. In addition to the federal response, 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) 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.

To support the five-year review by the Committee of the PCMLTFA, the Department of Finance published a discussion paper entitled "Reviewing Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime" on February 7, 2018. Themes included: closing legislative and regulatory gaps; enhancing information sharing; intelligence and enforcement; framework modernization and supervision. The measures described in this paper focused on improving the PCMLTFA and addressing gaps noted in the 2016 Financial Action Task Force Mutual Evaluation

Report. From February-May 2018, 60 unique submissions were received from a diverse range of stakeholders, including financial entities, life insurance companies, securities dealers, money services businesses, lawyers, industry associations, real estate agents and individual Canadians. On balance, the discussion paper was generally well received, and stakeholders signaled their support for key actions set out in the paper.

The Government is committed to a strong and comprehensive Regime that is at the forefront of the global fight against money laundering and terrorist financing. The Government recognizes that measures to enhance Canada's AML/ATF legislative framework should strike the appropriate balance among sometimes-conflicting objectives of providing actionable intelligence to law enforcement agencies and protecting the privacy and *Charter* rights of Canadians. Careful and deliberate use of financial intelligence supports the effectiveness of the Regime to improve the safety and security of Canadians, while respecting their privacy and constitutional protections. Yet, it is important 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.

RECOMMENDATIONS

After carefully reviewing the Committee's Report, the Government has chosen to respond to the recommendations by chapter.

CHAPTER 1: LEGISLATIVE AND REGULATORY GAPS

The Government of Canada substantively agrees with the direction of all the Committee's recommendations in Chapter 1 (Recommendations 1-13).

With respect to Recommendation 1, the creation of a pan-Canadian beneficial ownership registry for all legal persons and entities including trusts, the Government has already taken steps to strengthen beneficial ownership transparency under federal corporate law by requiring corporations to hold information on beneficial ownership in corporate records. Changes to the *Canada Business Corporations Act* were announced in Budget 2018 included in *Bill C-86, Budget Implementation Act 2*, which received Royal Assent on December 14, 2018. This step represents the first of two phases of work to improve the transparency and availability of beneficial ownership information in Canada as set out in the Agreement to Strengthen Beneficial Ownership Transparency announced by federal, provincial and territorial Finance Ministers in December 2017. A second phase of work with provinces and territories is also underway to assess options to improve access to the beneficial ownership information for law enforcement agencies, including the possible use of a registry.

In respect to Recommendations 2 and 3, changes related to new legal requirements were implemented in June 2017 in relation to politically exposed persons in Canada and heads of international organizations. Politically exposed persons in Canada (domestic PEPs) are people

who hold, or have held, important public functions in Canada, including heads of state, senior politicians, senior government and judicial officials at all levels of government, senior military leaders, senior executives of state-owned corporations, and important political party officials. Reporting entities are required to take enhanced measures if a domestic PEP is assessed by the reporting entity as presenting a high risk of money laundering or terrorist financing. The Government acknowledges that operational adjustments may be appropriate to ensure that the implementation is measured and effective. Emphasizing the risk-based approach, FINTRAC published a FAQ in relation to politically exposed persons in Canada on its website. Moving forward, the Department of Finance, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), and Office of the Superintendent of Financial Institutions (OSFI) will continue to monitor how compliance with these obligations evolves over time and provide further regulatory clarification and guidance as needed.

Recommendations 4 and 5 speak to specific measures that would address gaps in the Regime that relate to lawyers in regards to AML/ATF following Canada (Attorney General) *v*. Federation of Law Societies of Canada, 2015 SCC 7, [2015] 1 S.C.R. 401. The Government recognizes that the legal profession represents a high AML/ATF risk to the Regime, and continues to work towards bringing the legal profession into the framework in a constitutionally compliant way. To note, the Federation of Law Societies Canada have recently revised their model rules, including the no cash rule, as well as client identification and record keeping. The Government will continue to engage with the Federation of Law Societies Canada towards greater inclusion of the legal profession in the Regime.

The Government agrees with the direction of Recommendations 6, 12 and 13, which address the supervision of self-regulated professions, the examination of security dealers by security regulators, and the training of security regulators. However, the Government notes there are considerations that must be taken into account with respect to self-regulated professions and security regulators, such as constraints in our AML/ATF Regime framework, in order to respect the *Charter of Rights and Freedoms* and privacy rights, as well as federal/provincial/territorial jurisdictional issues.

As proposals outlined in the Department of Finance discussion paper, the Government is currently reviewing Recommendations 7 to 11 (amending the PCMLTFA to include armoured cars, white label ATMs, designated non-financial businesses and professions, real estate brokers, sales representatives and developers to mortgage insurers, land registry and title insurance companies, companies selling luxury items; making structuring of transactions a criminal offence).

CHAPTER 2: THE EXCHANGE OF INFORMATION AND PRIVACY RIGHTS OF CANADIANS

The Government of Canada substantively agrees with the direction of all the Committee's recommendations in Chapter 2 (Recommendations 14-19).

The Government will need to undertake further review and analysis of some of the provisions mentioned in Recommendation 14, which suggested the examination of the U.S. Government's "third agency rule" for information sharing. In the Canadian context, there are no "third agency" restrictions related to FINTRAC disclosures. Once disclosed, disclosure recipients may share information under their own authorities. Restrictions for other private-sector entities and agencies exist in various privacy statutes such as *Personal Information Protection and Electronic Documents Act* (PIPEDA), and/or the *Criminal Code*.

The Government is reviewing Recommendation 15, which calls for expanding FINTRAC's mandate to allow for greater focus on building actionable intelligence on money laundering and terrorist financing, longer data retention, two-way information sharing, the ability to request more information from specific reporting entities, and the ability to release aggregated data. There will be a need to balance anti-money laundering and anti-terrorist financing objectives with the *Charter* and privacy rights of Canadians in terms of implementing changes to the statute and regulations. The current legislation allows FINTRAC to receive financial information for criminal law purposes without prior judicial authorization. To support the reasonableness of the law, FINTRAC was created as an independent, arm's length agency from its disclosure recipients whose mandate explicitly includes ensuring against unauthorized disclosure. Its role is to analyze private information which it receives from various sources and to disclose information to law enforcement only upon meeting certain legal thresholds. In other words, law enforcement and intelligence agencies cannot merely compel access to FINTRAC's database or its analysis of specific cases. Without prior judicial authorization, the information that is permitted to pass to law enforcement is restricted.

In response to Recommendations 16-18, which call for a round table partnership with industry leaders, an emulation of the U.K.'s model of a Joint Money Laundering Intelligence Taskforce, and legislation that would allow information that is limited to AML/ATF subject matter to be shared between federally regulated financial institutions, the Government is reviewing the Recommendations to enhance public-private and private-private information sharing options. Building on recent success of Project PROTECT, a private sector led project with FINTRAC to combat human trafficking, the Government will continue to explore mechanisms and models to enhance information sharing in the AML/ATF Regime, including between the public and private sector. As highlighted in the experience of other countries, the Government recognizes that enhanced information sharing between private sector and government institutions, as well as between themselves, can facilitate more targeted disruption of illicit activities related to money laundering/terrorist financing (ML/TF), ultimately contributing to the effectiveness of an AML/ATF regime.

In terms of Recommendation 19, which would ensure that the most vulnerable Canadians are not being denied a bank account due to lack of adequate identification, policies for access to basic banking are already in place in the *Bank Act* and the PCMLTFA. Policies, such as the *Access to Basic Banking Services Regulations*, help ensure that the most vulnerable Canadians are not being denied a bank account due to lack of adequate identification.

CHAPTER 3: STRENGTHENING INTELLIGENCE CAPACITY AND ENFORCEMENT

The Government of Canada substantively agrees with the direction of all of the Committee's recommendations in Chapter 3 (Recommendations 20-24).

The Government is currently reviewing Recommendations 20 and 23, which suggest bringing forward *Criminal Code* and *Privacy Act* amendments in order to facilitate money laundering investigations and enable geographic targeting orders, as also outlined in the departmental discussion paper.

Recommendations 21 and 22 look to expand FINTRAC oversight to ensure casino entities are trained in AML and establish information sharing regime through FINTRAC and provincial gaming authorities. In response, the requirement to have a training program and reporting requirements for AML/ATF is already in place for all reporting entities. As reporting entities, casino operator entities have requirements to train employees and establish compliance programs. A comprehensive and effective compliance program is required to meet obligations under the PCMLTFA and associated Regulations. During a FINTRAC examination, reporting entities must demonstrate that the required documentation is in place, and that employees, agents, and all others authorized are well trained and can effectively implement all the elements of the compliance program. Moving forward, FINTRAC will seek to deepen engagement and clarify expectations and responsibilities within the casino sector.

The Government is reviewing Recommendation 24, which calls for giving holders of bearer shares a fixed period of time to convert them into registered instruments before they are deemed void, and will continue policy development work to this end. Bill C-25, which amended the *Canada Business Corporations Act* (CBCA) and the *Canada Cooperatives Act* to prohibit the issuance of new bearer shares, received Royal Assent on May 1, 2018. While the CBCA has required that shares be in registered form since 1975, with these additional amendments, the issuance of options and rights in bearer form is prohibited, and corporations which are presented with bearer instruments are required to convert them into registered form.

CHAPTER 4: MODERNIZING THE REGIME

The Government of Canada substantively agrees with the direction of the majority of Committee's recommendations in Chapter 4 (Recommendations 25-32).

Recommendations 25, 26, 29 and 32, which speak to the regulation of crypto-exchanges, crypto-wallets, and prepaid cards, and the streamlining of the reporting structure of Suspicious Transaction Reports (STRs), are being substantively addressed through proposed regulatory amendments to the PCMLTFA, which were pre-published in the *Canada Gazette* in June 2018. The proposed amendments address risks associated with dealers in virtual currencies (VCs). Businesses that provide VC-related financial services, such as exchange and value transfer services, will be deemed financial entities or money services businesses (MSBs). As required of current MSBs, businesses dealing in VC will need to implement a full compliance program,

identify their clients, keep records, report certain financial transactions, and register with FINTRAC. With respect to "crypto wallets", it should be noted that the proposed regulations are function-based and would ensure that businesses that provide associated financial services, such as value transfer or exchange services in/out of their clients' wallets, would be subject to the same AML/ATF regulations as MSBs. The proposed amendments also address prepaid cards. Prepaid payment products (e.g., prepaid credit cards) would be treated as bank accounts for the purposes of the Regulations. Therefore, reporting entities issuing prepaid payment products would be subject to the same customer due diligence requirements as those imposed on these reporting entities who offer bank accounts (e.g., verifying the identity of their clients, keeping records, and reporting suspicious transactions related to a prepaid payment product account). The amendment would not apply to issuers of products restricted to use at a particular merchant or group of merchants, such as a shopping-centre gift card. The reporting structure of STRs is also being updated through regulatory amendments to increase ease of use by reporting entities.

The Government will review Recommendation 27, which proposes to establish formal licensing mechanisms for crypto-exchanges. However, all MSBs must register with FINTRAC and have obligations to FINTRAC as reporting entities.

The Government will review Recommendation 28, which would prohibit nominee shareholders and subject nominees to anti-money laundering obligations. This measure will be considered within forward policy development work.

The Government has identified challenges to adopting Recommendation 30 (changing the structure of FINTRAC's STRs to resemble the Suspicious Activity Reports (SARs) used in the United Kingdom and the United States) and Recommendation 31 (enhance the direct reporting system of casinos to FINTRAC through STRs to include suspicious activities). Though these approaches are applied in the United States, they have not been adopted in Canada as they do not reflect Canadian legal requirements, which balance the goals of Canada's AML/ATF Regime and *Charter* and privacy considerations. Whereas STRs are more narrow in scope to reflect completed or attempted ML/TF transactions, SARs are more broad-based. In the Canadian constitutional context, a number of safeguards exist to strike an appropriate balance between privacy rights anti-money laundering and anti-terrorist financing objectives. The system to report Suspicious Transaction Reports has been carefully developed with this balance in mind. Furthermore, a legal threshold of "reasonable grounds to suspect" must be met before FINTRAC can share information with the RCMP and other disclosure recipients because they contain confidential private information that law enforcement would otherwise require a search warrant to obtain. The Government will continue to review how the Regime can be improved without jeopardizing this balance.

Regarding Recommendation 31, recent legislative changes have clarified that the provinces, who have the authority under the *Criminal Code* to manage and conduct legal casinos in Canada, are responsible for reporting to FINTRAC. In practice, depending on the operating model adopted in a given province, this obligation can be passed on by the province to the

private sector operator of the casino. These changes were implemented to address previous challenges related to duplication and confusion on which entities bear these obligations.

CONCLUSION

This Government Response describes concrete actions, policies and programs, both in place or underway, that address many of the Committee's recommendations. The Government substantively agrees with the direction of the majority of the Committee's recommendations, which are well-aligned with the Government's current direction on anti-money laundering and anti-terrorist financing. Officials are working to address the Committee's recommendations by developing forward policy and technical measures that could help shape or inform the Government's longer-term approaches to anti-money laundering and anti-terrorist financing through coordinated horizontal action among the federal government departments and agencies that are part of Canada's AML/ATF Regime.

Appendix E:

Canada, Criminal Intelligence Service Canada, *Public Report on Organized Crime 2019* (Ottawa: Criminal Intelligence Service Canada, 2019).

CRIMINAL INTELLIGENCE SERVICE CANADA

PUBLIC REPORT
ON ORGANIZED CRIME IN CANADA

2019

PUBLICATION DATE: DECEMBER 18, 2019

FOREWORD FROM THE DIRECTOR GENERAL, CRIMINAL INTELLIGENCE SERVICE CANADA

On behalf of Criminal Intelligence Service Canada (CISC), I am pleased to present the first *Public Report on Organized Crime in Canada.* This strategic assessment provides an overview of the Canadian criminal landscape and the activities of the organized crime groups that operate within it. It combines federal, provincial, and municipal law enforcement reporting, open source reporting, and intelligence from other domestic and international government agencies to assess significant organized crime threats to Canada.

Organized crime remains the pre-eminent threat to public safety, contributing to thousands of deaths annually from overdoses related to illicit drugs and gang violence that is affecting Canadian communities. While most intelligence produced by CISC is shared only with law enforcement agencies, CISC is increasingly releasing information to the public in order to raise awareness about the nature and extent of organized crime threats in Canada. This national perspective helps ensure that law enforcement, government, and the general Canadian public have a consistent view of organized crime, and contributes to building and maintaining the partnerships that are instrumental to our ability to combat this threat.

CISC works collaboratively with its provincial bureaus and with many federal, provincial, and municipal law enforcement agencies. These partnerships allow for the exchange of vital information without which our ability to assess and ultimately disrupt organized crime threats would be compromised. I would like to express my sincere appreciation to our partners for their valued contributions to this report.

Chief Superintendent Rob Gilchrist
Director General
Criminal Intelligence Service Canada

TABLE OF CONTENTS

Background

Criminal Intelligence Service Canada....1
Integrated Threat Assessment Process....1
Organized Crime Group Threat-Levels....1

Organized Crime Group Overview

Assessment of Organized Crime Group Threat-Levels....3
National High-Level Threats....3
Threat Evolution of National High-Level Threats....5
Key Facilitators....5
Geographical Scope....6
International Links....6

Network Assessment

Interconnectivity of High-Level Threat Networks and Priority Issues....8
Outlaw Motorcycle Gang Networks....9
Traditional Organized Crime Networks....10
Cocaine Importation Networks....10
Precursor Chemicals and Synthetic Drugs Networks....11
Money Laundering Service Provision Networks....11
Illegal Online Gaming....12
Violent Street Gangs....12

BACKGROUND

Criminal Intelligence Service Canada

Criminal Intelligence Service Canada (CISC) is an umbrella organization that unites Canada's criminal intelligence community. It consists of approximately 400 member agencies, including federal, provincial, and municipal police services and partner agencies, and supports the effort to reduce the harm caused by organized crime through the delivery of criminal intelligence products and services. It informs partners, government, and other stakeholders about criminal markets in Canada and assists law enforcement leaders in making decisions regarding organized crime enforcement priorities.

The organization is comprised of ten CISC Provincial Bureaus, which provide leadership and guidance in the creation of provincial intelligence products and services, and CISC Central Bureau, located in Ottawa, which assesses the national scope and direction of organized criminal activity in Canada. While each Bureau operates independently, each assesses organized crime through a common Integrated Threat Assessment (ITA) process, which ensures a consistent national approach to assessing organized crime and facilitates comparisons between provinces.

Integrated Threat Assessment Process

In 2012, the National Executive Committee (NEC) of CISC and of the Canadian Integrated Response to Organized Crime (CIROC) approved the establishment of an ITA Working Group to develop and define a common threat measurement tool to assess organized crime groups (OCGs) across Canada. Subsequently, Central Bureau and each Provincial Bureau adopted a common set of business rules for the application of the ITA process that facilitates the scoring of the threat posed by the OCGs operating in their regions.

Threat-scoring is based on information and intelligence within the last two years ranked against eight ITA Threat Measurement Criteria. Although older information and intelligence can provide context to a group's capabilities, it is not used to assess the current threat-level. The eight criteria focus on the following attributes:

- involvement in corruption or infiltration of law enforcement, security, or government agencies
- use of violence
- involvement in the private sector
- geographical scope (criminal reach)
- associations to other OCGs
- involvement in criminal enterprise (illicit drugs, financial crime, and other illicit goods and services)
- technological capability
- specialized skills

Organized Crime Group Threat-Levels

The threat-level of each assessed OCG is determined by combining the weights for all eight criteria, conducting a comparative review of each group's ranking, and analyzing the threat they present. Each criterion is classified as High, Medium, or Low. OCGs that have been identified as higher-level threat groups are those that, as a general rule: use violence as an integral part of their strategy; are involved in the infiltration of law enforcement, security, or government agencies; have access to multiple types of business; are criminally associated to several other OCGs; and possess an interprovincial or international scope.

A group does not have to rate "high" in all criteria to be considered a national High-Level Threat (HLT). The final assessment is based on an analysis of all ITA attributes. Although provincial bureaus are required to use the same criteria and definitions to assess OCGs, they can weigh the individual criteria differently. This flexibility allows for regional, provincial, and national threat-level distinctions, based on the requirements of the bureau's clients. For instance, a group that may present an overall high provincial threat may pose a different level of threat at the

national level, depending on the relative ranking of each criterion. The use of common threat criteria and definitions allows for a consistent analysis of the information and intelligence gathered for each OCG.

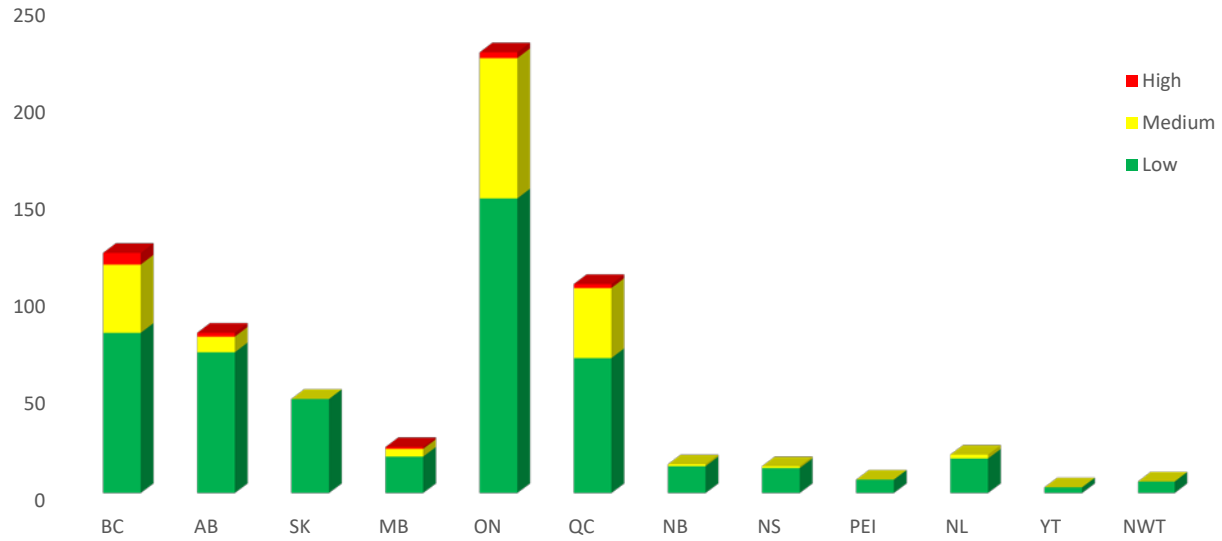
In November 2018, CISC developed a common definition to identify potential Key Facilitators. This definition assesses a potential Key Facilitator as *a person responsible for coordinating the work of a criminal network, or who plays an important role within it, whose disruption may compromise the criminal activities of multiple groups in this network*. This definition is intended to serve as a guide for the identification of potential Key Facilitators, and has been phrased in such a way as to account for regional and thematic differences, and to allow for the final determination to be subject to analytical judgement.

ORGANIZED CRIME GROUP OVERVIEW

Assessment of Organized Crime Group Threat-Levels

More than 1850 OCGs are believed to be operating in Canada. Of these, 680 have been assessed in 2019 as part of the ITA process. Limited recent reporting on the remaining identified OCGs prevents an in-depth assessment on their capabilities at this time. **Figure 1** shows the number of assessed groups, per province or territory, and by their threat-levels: high, medium, and low.

Figure 1 – Assessed OCGs in 2019, by Province and Territory, and by Threat-Level*



** No OCGs based in Nunavut were reported in 2019.*

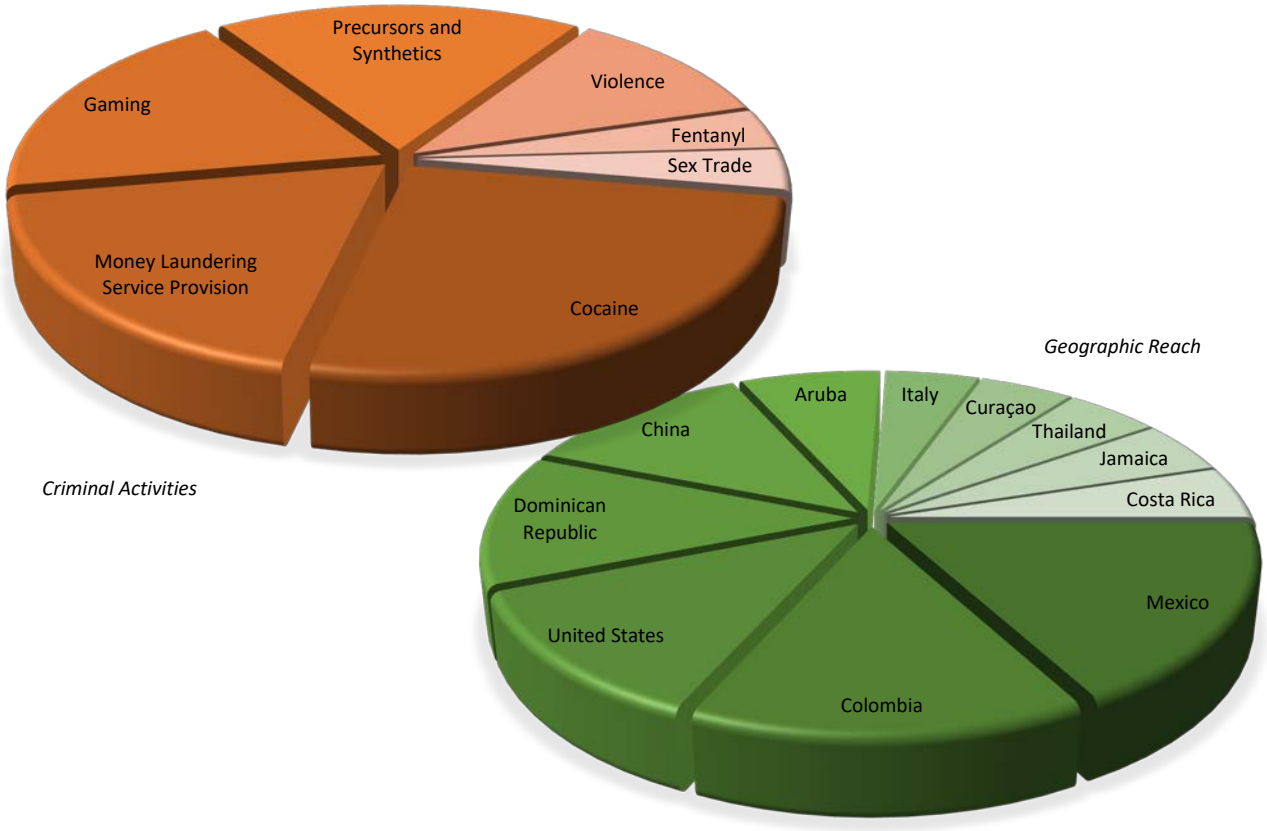
Although numbers are relatively consistent with those reported last year, representing only a slight increase from the number of OCGs assessed in 2018, almost 30 percent of assessed OCGs in 2019 are newly-reported. This trend can be attributed to different factors, including changes in targeting to focus on newly-identified priorities, on previous investigations being concluded, and on limited law enforcement resources available to continue reporting on previously-identified groups. Increased reporting of OCGs that have been assessed over multiple years through the ITA process has also led to the identification of new groups that interact with previously-reported ones. Moreover, as law enforcement gains a better understanding of the ways that criminal actors work together, moving away from reporting based on hierarchical and cultural structures to more fluid and interchangeable memberships, the identification of new groups has increased.

The increase of almost 39 percent in the identification of all groups believed to be operating in Canada, however, can be attributed in large part to enhanced sharing among law enforcement partners. For example, more than 375 street gangs were identified through the ITA process in 2018-2019, representing an increase of 68 percent.

National High-Level Threats

Fourteen OCGs have been assessed as national HLTs in 2019. They have interprovincial networks, if not always international connections, engage in multiple criminal markets, use violence to further their criminal business, and have a large number of criminal OCG association links. **Figure 2** on the next page provides an anonymized proportional overview into these HLTs' criminal activities and international scope.

Figure 2 – Proportional Overview of 2019 National High-Level Threat Groups' Criminal Activities and Scope



Five HLTs are involved in some of the largest cocaine importing networks in Canada, which leverage ties to Mexican and Colombian drug trafficking organizations, such as the Sinaloa Cartel, to import up to 1000 kilograms of cocaine per month. They are believed to use land or marine modes to import via the United States, or through Mexico, the Dominican Republic, and Colombia. These networks are often highly-entrenched, use multiple cocaine importation facilitators, and have extensive international criminal connections throughout Latin and Central America that likely facilitate cocaine importations into Canada and overseas to destinations such as Italy, Australia, and New Zealand.

An equal number of HLTs are also involved in large methamphetamine networks. Their activities include the importation of precursor chemicals from China for the domestic production of methamphetamine, the diversion of unregulated chemicals in Canada to domestic clan labs, and, increasingly, the importation of methamphetamine or precursors from sources in Mexico. Several of these groups are also involved in money laundering as a primary criminal activity or maintain associations to professional money laundering service providers with extensive ties to South East Asia, and are potentially associated to Triads based in China.

At least four HLTs are linked to money launderers for large international organized crime networks, providing laundering services for domestic and international drug traffickers. Many of these groups have links to Mexican cartels, are suspected of importing synthetic drugs and cocaine and of being involved in illegal gaming, and are involved in the international movement of bulk cash and in loan sharking.

One of the largest and most influential street gangs in Canada is included as a 2019 HLT due to its extensive use of violence (including firearms) to expand its territory beyond its traditional provincial base and its substantial infiltration of the private and public sectors. This OCG has one of the highest reported number of rivalries, resulting in violent conflicts in the Prairies and in Central Canada.

Many of the HLTs are involved in violence, with members suspected of being involved in homicides, shootings, and assaults. Within the past two years, an unusual number of the more entrenched groups have been targeted and their members have been killed in Canada and overseas, suggesting that a new generation of criminal threats may be gaining power, or that foreign competitors, such as Colombian or Mexican drug trafficking organizations, may be attempting to increase their influence in Canada.

Of note, most HLTs are involved in numerous illicit commodity markets that are organized by members operating from abroad. Many have access to strategic drug trafficking points along national and provincial borders, as well as extensive business interests, including importing/exporting and transport companies, that can be used for drug trafficking and money laundering.

Threat Evolution of National High-Level Threats

OCGs are fluid and continuously evolving, which creates challenges for law enforcement targeting and intelligence reporting. Changes in the list of national HLT groups from year to year are representative of the ongoing transformative criminal networks operating in Canada and the threats that they pose. A five-year comparison of the evolving threat-levels of the 2019 national HLTs reveals that half have been assessed as important threats for the past three or more years. Despite repeated law enforcement efforts against some of these OCGs, reporting shows that many have remained resilient and adaptive to their changing environments.

Barring successful law enforcement action against higher-level OCGs, they are likely to continue evolving and to develop into increasingly pre-eminent threats. Twelve of the 14 national HLTs identified in 2019 have evolved from medium-level threats in the past five years. The other two national HLTs have maintained their status for more than five years, demonstrating a high degree of entrenchment and insulation against law enforcement targeting.

Since many of these OCGs operate in more than one province, interprovincial collaboration and cooperation between multiple law enforcement agencies is essential in order to impact and disrupt these entrenched groups and their criminal activities. Additionally, facilitators that work with more than one OCG should also be considered when identifying law enforcement opportunities and targeting, as they often provide further connectivity between multiple groups.

Key Facilitators

In addition to the national HLT groups, seven key facilitators have been assessed in 2019. They were identified by applying the newly-approved definition and assessing the role of potentially important players within the key networks. **Figure 3** provides an anonymized overview of these key facilitators.

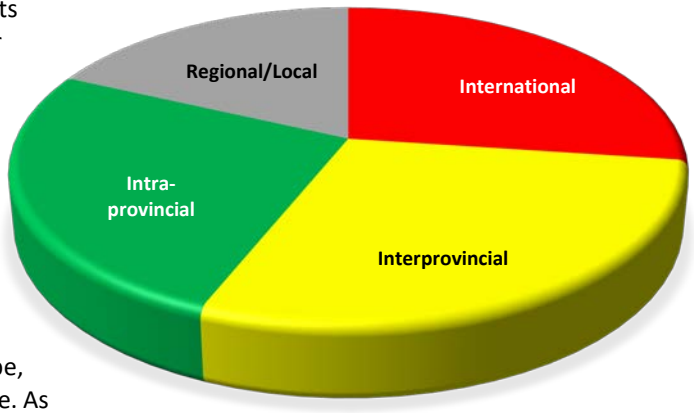
Figure 3 – Overview of 2019 Key Facilitators

Precursor chemical diverters	*Cocaine importation facilitators for various OCG networks*	*Canadian operations manager for international crime syndicate*	*Cocaine shipment financier for various OCG networks*	*Cocaine importer and distributor*

Geographical Scope

Figure 4 provides a graphical representation of the scope of assessed OCGs, based on the ITA criterion. Reporting on the geographical scope of OCGs assists in assessing the depth and breadth of their criminal networks, and the threat they may pose to Canada and its international partners. The ITA criterion dealing with scope is broken down into international, interprovincial, intra-provincial, and regional / local.

Figure 4 – Geographical Scope of Assessed OCGs in 2019



More than half of all assessed OCGs are involved in criminal activities that are multi-jurisdictional in nature. Twenty-six percent of these OCGs have an international criminal scope, and another 28 percent have an interprovincial one. As a result, increased collaboration and simultaneous multi-jurisdictional targeting of OCGs is key for long-term impact. National-level collaboration or coordination between jurisdictions is essential to effectively optimize enforcement targeting efforts and disrupt criminal activities.

It should be noted that the ITA criteria preclude the identification of groups that have multiple scopes, in favour of identifying the highest scope threat. For example, whereas 28 percent of OCGs are assessed as having a medium scope threat (i.e. interprovincial), there are actually 44 percent of OCGs reported to have an interprovincial reach. The remaining 16 percent have both an interprovincial and an international scope, and are therefore assessed as having a high scope threat. Whereas international connections are an important indicator of a group's potential threat to Canada and its international partners, interprovincial links are important in assessing a group's domestic reach and its interoperability in collaborating with OCGs in other areas of the country.

International Links

OCGs' international nature has often been underreported. While this remains an intelligence gap, improvements have been made with respect to intelligence sharing, including, for example, with the RCMP's International Policing Program. Continued sharing will help augment the intelligence on Canadian OCGs operating abroad.

OCGs operating in Canada are known or suspected of having international associations to 72 countries. While travel to countries considered source or transit countries for certain illicit commodities could have been for non-criminal purposes, such as social activities and events, they have been included in the statistical analysis, as the determining motive remains unknown.

Many OCGs are linked to multiple countries, which may demonstrate their ability to establish international networks. Of those with international connections, almost 30 percent are linked to three or more countries. The top five countries to which the most Canadian-based OCGs are linked include the United States, Mexico, Colombia, China, and Australia. The four first countries remain unchanged from previous assessment; the increased reporting of links to Australia may be as a result of enhanced sharing with international partners. **Figure 5** provides an overview of the countries to which Canadian-based OCGs are linked.

Figure 5 – Countries (in blue) with Reported Links to Canadian OCGs

Of the OCGs with international links, approximately 54 percent have bilateral links between Canada and the United States. Additionally, of those OCGs linked to the United States, approximately 21 percent also have connections to Mexico. Both of these countries are considered transit countries for illicit drugs being shipped from South America to Canada.

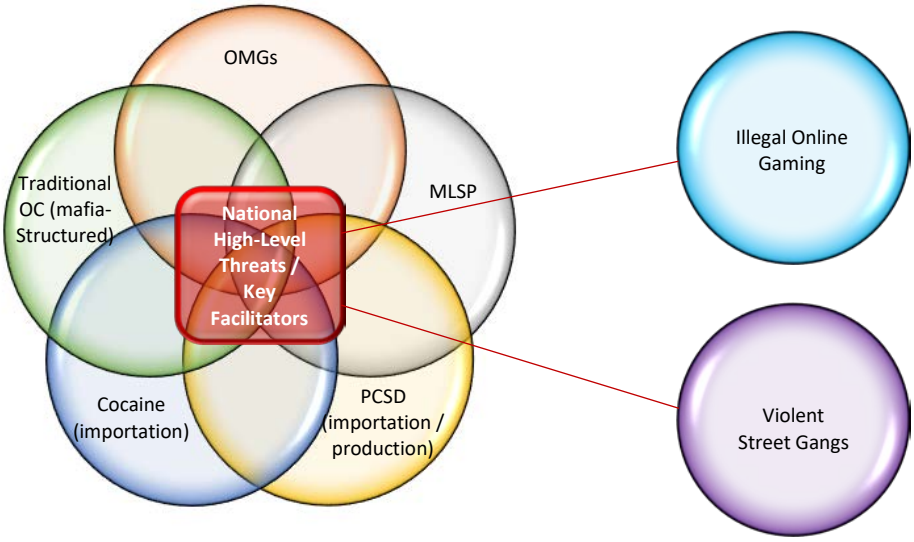
Of all OCGs, outlaw motorcycle gangs (OMGs) maintain the broadest international scope. One OMG global network consists of more than 500 chapters in 60 countries across Europe, North America, South America, Africa, Asia, and Oceania. Members of this OMG in Canada and their support clubs continue to travel extensively to the Caribbean, Europe, and Central/South America. Some of these countries represent source and transit points for importing/exporting cocaine.

NETWORK ASSESSMENT

Interconnectivity of High-Level Threat Networks and Priority Issues

In response to the potential for shifting priorities in operational targeting, an interconnected approach to assessing higher-level networks – and the HLTs and key facilitators that are involved within them – has been adopted in order to allow CISC to assess and propose a broad range of potential national-level targets for law enforcement operations. As illustrated in **Figure 6**, these networks include OMGs, traditional mafia-structured organized crime (TOC), cocaine importers, precursor chemicals and synthetic drugs (PCSD) – specifically those networks involved in the importation of precursors and the manufacture of methamphetamines and fentanyl, and money laundering service provision (MLSP). The priority issues include illegal online gaming and violent street gangs.

Figure 6 – Interconnectedness of High-Level Threat Networks and Priority Issues



The high-level threat networks and priority issues identified in 2019, when considered together, encompass a large proportion of interconnected OCGs in Canada. These interconnected networks and priority issues all include OCGs assessed as high-, medium-, and low-level threats, and the national HLTs and key facilitators assessed in 2019 all participate in one or more of these criminal spheres. No group is currently assessed to be involved in all of them. The networks are composed of OCGs that operate independently and also collaborate to further their collective criminal goals. While some include more national HLTs than others, each network in itself poses a national high-level threat, given its geographical scope, the number and nature of the OCGs involved within it, and the harm that the criminal activities in which the OCGs engage presents to the Canadian public.

OMGs collaborate with other OCGs in the importation of cocaine and other illicit drugs, and have networks stretching across Canada that facilitate their well-established distribution lines. They are criminally associated to groups that form the TOC network, and are involved with OCGs involved in illegal online gaming, which is seen as a high-profit/low-risk market. While generally not part of the larger PCSD networks, OMGs are involved in the supply and distribution of synthetic drugs. They are also closely associated to street gangs and leverage these associations to maintain/enforce their drug trafficking territories and outsource violence.

TOC groups, in addition to their links with OMGs, are involved primarily in cocaine importation, illegal online gaming, and money laundering via multiple private sector businesses. The networks benefit from groups' and members' high level of interconnectedness, both domestically and internationally. The OCGs also use street gangs for homicides and attempted homicides of rivals.

Importation networks are often controlled by OMGs and TOC, and involve street gangs as part of their distribution channels. These established networks also have redundancies implemented into their operations to limit disruptions: with more than 100 OCGs reported to import cocaine, these networks' operations are unlikely to be significantly affected by individual groups being compromised by law enforcement targeting. For example, in 2018, one of the more important key facilitators in Canada involved in cocaine importation and trafficking was arrested; however, this individual's network reactivated its operations within hours due to these redundancies.

The networks involved in **PCSD** (specifically the importation of precursors and the manufacture of methamphetamine and fentanyl) and **MLSP** are highly-interconnected, with the majority of the OCGs in the Western Canada network being involved in both markets and having ties to Southeast Asia, notably China.

Outlaw Motorcycle Gang Networks

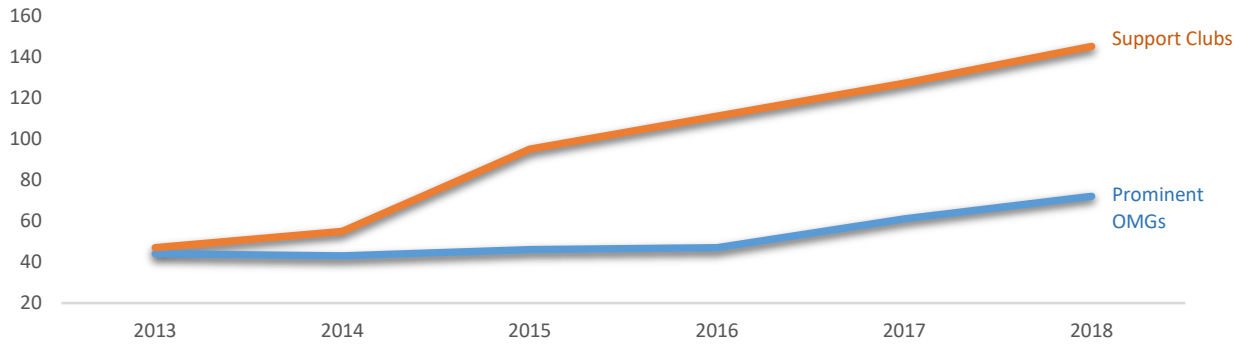
OMG networks continue to be among the most prominent OCGs in Canada. One prominent OMG is expanding across the country, consisting of 44 chapters, more than 500 full-patch members, prospects, and hangarounds, and more than 100 support clubs, which have also expanded more than 200 percent in the past five years. Through their networks, members manage vast drug territories. They are involved in importing cocaine, money laundering, gaming, the sex trade, synthetic drug production, and financial crime. OMG members use intimidation and violence, either directly or through their subordinates, to maintain control of their criminal territories. The expansion of certain OMGs has increased the threat of violence, much of which can be attributed to competition for control of drug territories.

Together, OMG members reach more parts of Canada than any other networks. Their scope reaches internationally to members overseas, as well as to Latin American cartels and other foreign figures, providing them with ample connections for the importation of drugs as well as money laundering opportunities. With multiple drug supply lines across the country, and by using intimidation to tax traffickers that seek their drugs from other sources, OMG members profit from a large part of drug trafficking in Canada.

Another competing OMG network, second only to one referred to above, continues to expand in Canada. Even though its membership is smaller, it is one of three major international OMGs, and its network has been expanding in Ontario and in the Atlantic Provinces via support clubs and new chapters.

Support clubs are sanctioned by and closely associated to, but not necessarily controlled by, prominent OMGs. Their members often socialize with these prominent OMGs, and some are involved in their criminal activities. Support club expansion – led by certain members of prominent OMGs – is inconsistent across Canada; some provinces are reporting a consolidation of support clubs. Additionally, the development of provincial coalitions of clubs, or councils, facilitates the management of these clubs. An OMG, or one of its support clubs, is believed to control coalitions in most provinces. **Figure 7** shows the expanding number of major OMG chapters and support clubs reported between 2013 and 2018.

Figure 7 – Number of Select OMG Chapters and Support Clubs, 2013-2018



Traditional Organized Crime Networks

TOC networks in Canada, comprising about two dozen OCGs forming overlapping criminal networks, are mainly based in the Greater Hamilton, Toronto, and Montreal areas and include OCGs whose membership is primarily of Italian descent and who ascribe to the hierarchy, norms, and rituals of the Italian mafia. These OCGs are likely operating beyond their traditional bases, extending to at least five other provinces in Western and Eastern Canada. These extended networks exist not only through the presence of members, but also through various contacts, private companies, and criminal enterprises. Some of the most lucrative domestic criminal associations in the TOC network are with OMG members. TOC networks are considered to be the most interconnected of OCGs in Canada, with links to approximately 20 percent of the assessed OCGs in 2019.

These networks are involved in various criminal activities, including importing, exporting, and distributing illicit drugs, illegal gaming, loan sharking, extortion, intimidation, violence, homicide, money laundering, financial crime, and fraud. Illegal online gaming is considered one of their more lucrative markets. They have an extensive number of importation channels, suggesting that enforcement activity against one or two related groups will have a limited impact on the networks' overall criminal activities. Likely as a result of their dominant roles in Ontario and Quebec, respectively, TOC groups maintain some of the most interconnected networks in Canada.

TOC groups maintain control of hundreds of businesses in multiple industries, including food services, transportation, construction and haulage, property management, finances/loans, payday loan businesses, real estate companies, and businesses that can be run primarily using cash, all of which can be used for laundering proceeds of crime. They continue to infiltrate the public and private sectors to facilitate the laundering of proceeds of crime, to maintain their status as reputable community members, and to increase their geographical scope.

In order to further their criminal activities, TOC groups maintain links with individuals and OCGs in drug source and transit countries such as Colombia, the Dominican Republic, and Mexico for the purpose of importing illicit substances and laundering their money. Approximately 90 percent of OCGs assessed to be part of the TOC network in Canada maintain international links.

There has been a rise in violence in the Greater Toronto Area (GTA) involving individuals associated to TOC. Most of the violence seems to be primarily directed at individuals, associates, or businesses belonging to OCGs linked to the 'NDRANGHETA[1]. The violence in the GTA may have been a result of a power struggle for territorial control and conflicts related to cocaine importing, illegal gaming, and debts owed. Instability within the groups and the roles they play within the network in Quebec is leading to violence. Nonetheless, several influential TOC figures have recently been released from custody and may be positioning themselves within the networks. Consequently, the potential for violence is likely to increase by attempts to re-assert their roles within the TOC networks. However, the leadership of TOC in the GTA is relatively stable and there does not seem to be a current threat to its dominance.

The TOC network in Montreal is likely to be characterized and shaped by a new, younger generation of members. The likelihood that they will use technology, including encrypted communications and other technological advancements, will present new challenges for enforcement.

Cocaine Importation Networks

Cocaine remains one of the most prevalent criminal markets in Canada, with importers playing a vital role. In 2019, nearly 100 Canadian OCGs have been identified as importing cocaine into Canada, or of using Canada as a transit country to move cocaine to more profitable markets, such as in Oceania and Europe. These networks are criminally linked to cocaine source countries (Colombia and Peru) and key transit countries (Aruba, the Dominican Republic, Jamaica, Mexico, Panama, and the United States). Collaboration between Canadian OCGs and Mexican cartels / Colombian OCGs continues to occur, often in source or transit countries.

[1] The 'NDRANGHETA is a mafia-type organized crime group based in Calabria, Italy. It operates independently from the Sicilian mafia, though there is contact between the two due to the geographical proximity and shared culture and language between Calabria and Sicily.

Several of the OCGs included in the cocaine importation networks are entrenched in the Canadian criminal landscape; their involvement in importing cocaine dates back several years. The importance of these OCGs and of their networks is their interoperability and their resilience to law enforcement action, as disrupted groups are quickly replaced by other members of the network and some lesser-known groups are gaining prominence. Moreover, although not part of the larger networks, other OCGs and criminal entrepreneurs are also important actors in the cocaine market, exploiting connections to Colombia and access to businesses and transportation modes that can be used to facilitate the import and export of cocaine and other illicit commodities.

A significant number of key Canadian cocaine importation facilitators have been assassinated, both inside and outside the country, over the past few years, raising the possibility that Mexican cartels may be attempting to re-establish operational cells in Canada that had previously been largely disrupted through an integrated enforcement response. Cartels members are likely exploiting the absence of visa requirements for Mexican nationals entering Canada to send associates to play a more direct role in importing cocaine into Canada, as in the past. However, resulting violence of such a trend is not expected to rise to the level seen in the southern United States.

Precursor Chemicals and Synthetic Drugs Networks

The Canadian PCSD landscape includes more than 30 OCGs that are involved in the movement (international and/or domestic) of precursors and other essential chemicals used in synthetic drug production, and nearly 50 OCGs that produce methamphetamine and fentanyl (and its analogues). Moreover, about 20 OCGs import methamphetamine, and 15 import fentanyl. While many of these groups appear to work independently from one another, two distinct networks have an established history of collaboration and represent approximately 50 percent of all groups involved in the movement of precursors and other essential chemicals in Canada.

Higher-level OCGs that have almost unlimited access to chemicals used in synthetic drug production are the likely operators of recently-dismantled highly-sophisticated and large-scale illicit clandestine labs. Despite past targeting, the leadership and membership of these groups remain intact. As these networks also manufacture, they likely sell at the wholesale level and have associations to locally-based distributors that distribute intra- and interprovincially.

The announcement of new regulatory amendments on precursors under the *Controlled Drugs and Substances Act*, coupled with low prices and high profit margins, will likely prompt OCGs with connections to drug trafficking organizations in Mexico and/or the United States to increase the import of methamphetamine and/or fentanyl from Mexico. In the absence of stronger precursor and essential chemical-related legislation, OCGs involved in PCSD will continue operating, supplying clandestine labs and manufacturing and trafficking drugs to domestic and international markets while using laundered proceeds to re-invest into and further their criminal activities.

Money Laundering Service Provision Networks

Money laundering is a key activity for OCGs, and the practice is pervasive throughout all scopes of criminal enterprise. Money laundering service providers coordinate and move large sums of money to legitimize criminal proceeds, on behalf of Canadian and international OCGs. One high-level network based in British Columbia and in Ontario, for example, represents several key service providers nationally and internationally, conducting self-laundering, and providing third-party money laundering services to OCGs by conducting complex money laundering operations through their exploitation of casinos, underground banking systems, illegal gaming houses/sites, nominees/shell companies, trade based money laundering, and real estate investments.

The money laundering techniques used include: the exploitation of casinos and the real estate sectors, including large cash buy-ins at casinos by wealthy gamblers that have been provided proceeds of crime from members of the MLSP network; deposits of casino cheques, representing cashed-out casino chips bought with proceeds of crime, into Canadian banks and subsequently used to buy real estate; using nominees to hide ownership of real estate; and purchasing real estate with hundreds of thousands of dollars in cash, using mortgage brokers and lawyers. This network is comprised predominantly of career criminals and highly-interconnected OCGs, and is believed to have laundered proceeds of crime totalling upwards of hundreds of millions of Canadian dollars.

Illegal Online Gaming

These networks are comprised of OCGs either operating or profiting from illegal gaming websites. In Canada, this market is controlled by TOC and OMGs, either working together or on their own in numerous urban centres throughout Canada.

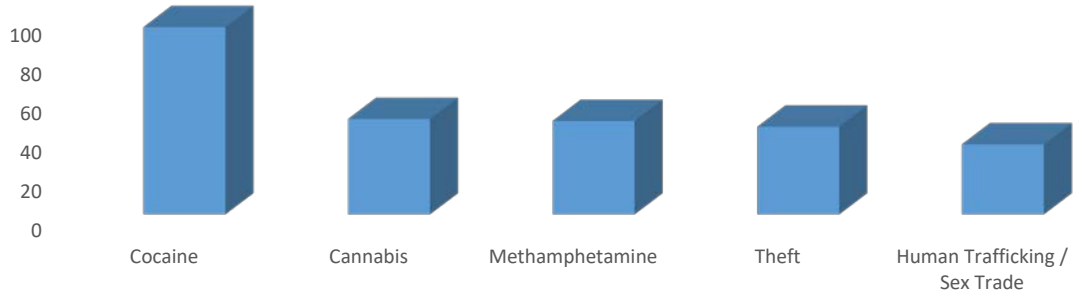
Although groups operating these gaming networks often try to circumvent Canadian law by running their websites on offshore servers, monetary transactions on Canadian soil make this a criminal activity. They also use violence, extortion, and intimidation to further their criminal goals. Gaming networks generate millions of dollars of revenue each year, and OCGs involved in this market use these illicit funds to finance other forms of criminality, such as drug importing and trafficking.

According to the Canadian Gaming Association, Canadians are estimated to wager four billion dollars CAD annually through offshore online sportsbooks.[2] When this figure is compared to the $500 million CAD wagered annually through legal provincial sports lotteries, it is evident that OCGs are capitalizing on a market service in high demand.

Violent Street Gangs

More than 375 street gangs have been reported in Canada in 2019. Street gangs continue their involvement in high-visibility crimes. **Figure 8** provides an overview of the primary markets in which street gangs are heavily involved.

Figure 8 – Primary Reported Criminal Market Involvement of Street Gangs, 2019



Street gangs also continue their involvement in illicit drug markets (primarily in a retail to mid-level distribution role, with cocaine, cannabis, and methamphetamine being the most popular), in theft-related activities (including break and enters and home invasions), in violent incidents including shootings, and in sex crimes, causing them to come to the attention of the media, and subsequently of the general public, more frequently than higher-level, more insulated OCGs. Although street gangs are present in most areas of the country and collectively represent a national-level issue, their composition and operations vary to some degree from region to region.

Although some street gangs maintain a core group of longstanding members, gang membership is reportedly becoming more fluid, with alliances and rivalries among members and groups often quickly shifting. Additionally, information suggests that alliances are more frequently being formed based on "for profit" business deals, with violence often resulting from disputes over profit-making ventures such as control over drug trafficking territory, rather than the more traditional "blue vs red" or "Bloods vs Crips"-type conflict. Furthermore, street gang members based primarily in Quebec are believed to have been involved in murders both on behalf of higher-level OCGs, such as TOC, as well as against members of other groups, including OMGs.

The increasing fluidity and evolution of gang membership presents difficulties relating to accurate and timely reporting of their statuses, rivalries, and members. Many street gangs, regardless of their threat-level, are of concern

[2] http://canadiangaming.ca/canadian-gaming-association-calls-on-all-party-support-for-single-event-sports-betting/

within the communities and provinces in which they operate, given their use of violence, engagements in conflict with other OCGs, and multi-jurisdictional criminal activities. From a national perspective, street gangs' individual levels of threat increase as they expand their territories, develop more rivalries, become increasingly violent, and engage in higher-level criminal activities. In 2019, 22 street gangs have been identified and assessed as posing a national medium-level threat; two have been assessed as national HLTs. Many of these street gangs exhibit characteristics that may indicate an evolution of their capabilities to higher threat-level OCGs.

Street gang members continue to commit violent acts, create fear within the communities in which they operate, and pose public safety concerns across Canada. Ongoing rivalries between street gangs and the associated violence that results presents an important public safety concern. Cities that report higher volumes of firearm-related violent offences also have a higher number of street gangs, and street gangs are more frequently involved in shootings than other OCGs. In British Columbia alone, there were 33 gang-related reported homicides in 2018, 15 of which were linked to the Lower Mainland Gang Conflict that involves several higher-level street gangs.

Similar to social media's popularity among the general public, its use by gang members in various regions of the country is reportedly becoming more prevalent. Street gangs are using their social media presence in recruitment efforts, often by promoting and/or glorifying the gang lifestyle, and to instigate conflicts with rival gang members, with at least some of the violence occurring on the street being precipitated by some form of online feud. The continued use of communication tools such as Snapchat, Instagram, and WhatsApp by gang members poses increasing investigational challenges for law enforcement agencies, and particularly agencies without dedicated open source/social media resources, as many of these applications offer varying levels of encryption and allow users to securely delete data before investigators become aware of their existence.

Street gang members, particularly in Ontario jurisdictions, seem to be more comfortable with carrying firearms on their person. Ready access to firearms in the hands of those street gang members with poor impulse control may lead to an increase in opportunistic gang-related shootings, compromising general public safety. Furthermore, as Ontario-based gang members continue to expand their scope both intra- and inter-provincially, other jurisdictions like Thunder Bay, to which Toronto- and Ottawa-based gangs have expanded operations, may subsequently experience continued increase in gang-related firearms violence in the future. The spread of firearms-related violence is not unique to Ontario, and will continue to follow the territorial expansion of violent groups across jurisdictions.

Appendix F:

Canada, Criminal Intelligence Service Canada, *2018-19 National Criminal Intelligence Estimate on the Canadian Criminal Marketplace: Illegal Drugs* (Ottawa: Criminal Intelligence Service Canada).

CISC ✦ SCRC

Criminal Intelligence Service Canada
Service canadien de renseignements criminels

2018-19 NATIONAL CRIMINAL INTELLIGENCE ESTIMATE

on the Canadian Criminal Marketplace

ILLICIT DRUGS

Canada

National Criminal Intelligence Estimate

2018-19

On The Canadian Criminal Marketplace

Illicit Drugs

Foreword from the Director General of Criminal Intelligence Service Canada

I am pleased to present the unclassified version of the *2018-19 National Criminal Intelligence Estimate (NCIE) on the Canadian Criminal Marketplace – Illicit Drugs.* This strategic assessment provides an overview of the scope and magnitude of the main illicit drug markets in Canada and the role of serious and organized crime within these markets. It combines federal, provincial, and municipal law enforcement reporting, public health data, open source reporting, and intelligence from other domestic and international government agencies to explore existing and emerging threats to Canada.

While most intelligence produced by CISC is shared only with law enforcement agencies, CISC is increasingly releasing information to the public in order to raise awareness about the nature and extent of organized crime threats in Canada. This national perspective helps ensure that law enforcement, government, and the general Canadian public have a consistent view of serious and organized crime, and contributes to building and maintaining the partnerships that are instrumental to our ability to combat this threat.

CISC works collaboratively with its provincial bureaus and with many federal, provincial, and municipal law enforcement agencies. These partnerships allow for the exchange of vital information without which our ability to assess and ultimately disrupt organized crime threats would be compromised. I would like to express my sincere appreciation to our partners for their valued contributions to this report.

Chief Superintendent Rob Gilchrist
Director General
Criminal Intelligence Service Canada

Table of Contents

Executive Summary 1

Introduction 5

Methamphetamine 7

Fentanyl and its Analogues 12

Cocaine 16

Heroin 19

Cannabis 24

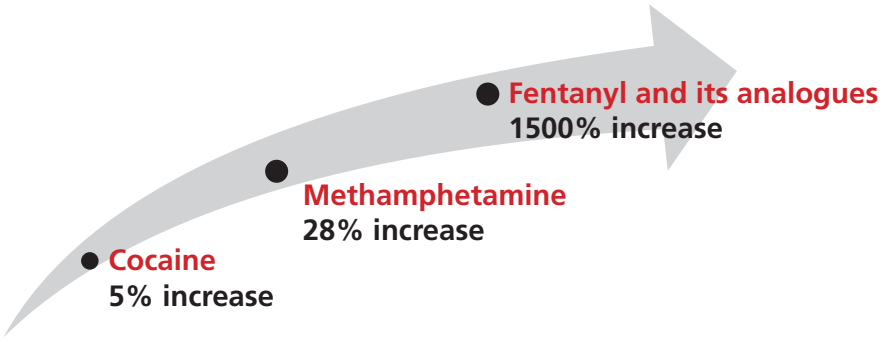
Other Illicit Drug Markets 30

Executive Summary

Highlights

- Methamphetamine, fentanyl and its analogues, and cocaine are assessed as having the highest level of threat due to their geographical reach, high burden of harm, and increased involvement of domestic organized crime groups (OCGs). This is expected to continue into 2019-20.
- Regionally, the threat levels of methamphetamine, fentanyl and cocaine vary with methamphetamine and cocaine being the pre-eminent threats in most regions, and the dominant threat in British Columbia and Alberta being fentanyl and its analogues.
- The heroin market, assessed as a medium threat, is being displaced by fentanyl and its analogues in provinces such as British Columbia.
- The legalization of cannabis creates an unprecedented shift in this market, posing a low level threat in the long term (3 + years), as licit market supply increases.
- Increased OCG involvement in the fentanyl market is likely to increase the availability of fentanyl across the country through wider distribution networks – especially if entrenched groups such as the Outlaw Motorcycle Gangs (OMG) and Italian Organized Crime (IOC) become involved.
- Based on past trends and the increased involvement of entrenched organized crime, with its expansive distribution networks, intelligence indicates that over 4000 opioid-related deaths in Canada can be expected in 2019. The number of accidental deaths may exceed this number, with the increasing availability of new and more potent opioids and fentanyl analogues.
- Despite Mexico's traditional role in the cocaine market, Mexican cartel representatives are increasingly exporting methamphetamine, heroin, and fentanyl to Canada.

Assessed OCG involvement, 2015-2018



Methamphetamine is assessed as one of the most important illicit drug threats in Canada, with substantial increases in trafficking and use and a 28 percent increase in OCG involvement over three years.

- The Canadian methamphetamine market is and will continue to be mostly supplied by domestic clandestine labs located in British Columbia, Ontario and Quebec, with OCGs effectively obtaining inexpensive, readily available chemicals from hardware, grocery, pharmacy and supplement stores.

- Despite domestic production meeting Canadian demand, Mexico, with its cartel-related smuggling networks, is increasingly becoming a source of methamphetamine.

- Whereas ephedrine-based production and methamphetamine in crystal or powder form is the norm in Western Canada and Ontario; in Quebec, phenyl-2-propanone (P2P) based production remains prevalent. Methamphetamine, usually in tablet form, is subsequently moved interprovincially from Quebec to Atlantic Canada and parts of Eastern Ontario.

Based on past trends and the increased involvement of entrenched organized crime, with its expansive distribution networks, intelligence indicates that over 4000 opioid-related deaths in Canada can be expected in 2019, largely as a result of **fentanyl,** its analogues and other opioids such as hydromorphone. Fentanyl is now a distinct opioid market, with stronger analogues becoming more prevalent, and represents a pre-eminent threat in British Columbia and Alberta, and, increasingly in Ontario.

- OCG involvement in fentanyl has increased by 1500 percent since 2015, and entrenched OCGs, such as outlaw motorcycle gangs, are becoming more involved.
- Independent criminal entrepreneurs also continue to be involved in the online procurement and trafficking of fentanyl from China via dark web marketplaces using virtual and cryptocurrencies.
- China will remain the primary supplier for illicit fentanyl, its analogues and precursor chemicals to Canada, although increasing amounts will likely originate from Mexico, as Mexican cartels shift from heroin production to fentanyl production.
- Canada is increasingly used as a transshipment country for fentanyl due to a rising international demand.

The **cocaine** market has more OCGs involved (75 percent) than any other market. This trend is expected to continue as a result of increasing domestic and international demand ensuring continued profits for OCGs.

- Mexican cartels, as well as a number of Colombian OCGs, are the main sources of cocaine consumed in Canada.

- An unusual number of high-level cocaine importers from Canada with links to Mexican cartels have been recently killed in Mexico, suggesting that the cartels may be looking to remove competition and to re-establish operational cells in Canada.

The **heroin** market was displaced by fentanyl and its analogues in British Columbia; other provinces will likely follow this trend. Nonetheless, the number of OCGs reported to be involved in the heroin market is increasing. This is likely in part due to heightened law enforcement action dedicated to combatting opioid trafficking in Canada, and is not necessarily reflective of an increase in the number of heroin users in Canada.

- The number of assessed OCGs involved in the heroin market has risen 44 percent in one year, but most groups are also involved in fentanyl.
- The majority of the heroin in Canada continues to be sourced from Afghanistan. South Africa remains a key transit point for heroin to Canada.
- The Greater Toronto Area (GTA), with its longstanding heroin importing and trafficking networks with ties to source and transit countries, continues to be a key point of entry for high quality, competitively priced Afghan heroin. The Greater Montreal Area (GMA) is likely an emerging entry point.
- Mexican heroin, often adulterated with fentanyl, will likely increasingly be imported into Canada through established cocaine trafficking routes.

Approximately 44 percent of assessed OCGs were involved in the **cannabis** market leading up to the implementation of the Cannabis Act. Almost all of these groups are also involved in at least one other illicit drug market and are unlikely to be disrupted by legalization given their alternate streams of revenue. In the short term (1-2 years), as the legal supply continues to be insufficient to meet demand, OCGs are well-placed to fill the gap. However, the number of OCGs in the illicit cannabis market is expected to decrease incrementally over the long term (3+ years), as the licit market supply increases.

- OCGs involved in illicit cannabis will likely, in the long term, increase their involvement in cocaine, methamphetamine and fentanyl to counteract the displacement of their market shares in cannabis as a result of legalization.
- Other adaptive strategies will include: exporting to jurisdictions where it remains illegal, such as in the U.S. and the U.K. focusing on more potent cannabis products; targeting consumers that are unable or unwilling to purchase cannabis from legitimate suppliers; and exploiting regulatory differences between provinces.
- On the eve of legalization, there was a marked 60 percent decrease in the number of illegal cannabis storefronts in Ontario, including the shuttering of all but one storefront with OCG links. Many of these storefront operators are expected to seek the acquisition of a legal retail license to resume operations in April 2019.
- The appearance of illicit dispensaries on First Nations Territories suggests that the illicitly sourced cannabis market will likely emulate the contraband tobacco market by exploiting the tax exemptions extended to Indian Status card-holders.

A total of 140 (23 percent) of OCGs involved in the illicit drug market are importing illicit drugs. The vast majority of these are importing cocaine.

A comparatively low number of OCGs are exporters: 28 groups (5 percent) are exporting illicit drugs beyond Canada's borders - primarily cocaine, cannabis, and MDMA.

- OCGs will continue to be attracted by a combination of high demand and high prices in some countries, such as those for cocaine and methamphetamine, to export to those areas, such as Australia and New Zealand.
- MDMA and cannabis will likely remain the most common drugs smuggled from Canada to the U.S., although to a lesser degree than in previous years.

Illicit drug trafficking is facilitated by dark web marketplaces and cryptocurrencies, which are providing anonymity to vendors and purchasers and posing new challenges for law enforcement. Despite domestic and international law enforcement efforts to take down illicit trading platforms, they are constantly re-appearing.

Introduction

Background

The *2018-19 NCIE* is produced by CISC Central Bureau, in collaboration with its network of ten Provincial Bureaus through the Integrated Threat Assessment (ITA) process, as well as contribution from member agencies and other federal and provincial partners. The NCIE is one of CISC's flagship products that was first introduced in 2005, and recognizes the need for law enforcement decision-makers and government policy makers to receive specific strategic intelligence on the scope and magnitude of criminal markets in Canada. This unclassified version of the *2018-19 NCIE* is shared with the Canadian private industry and the general public to help harden the environment against serious and organized crime.

Structure

The *NCIE - Illicit Drugs*, is a comprehensive strategic assessment of the threat posed to Canada by domestic and international drug trafficking. It centers around five drug markets posing the most significant level of threat to Canada: methamphetamine, fentanyl and its analogues, cocaine, heroin, and cannabis. Brief overviews of other illicit drug mar-kets are also included in the NCIE and will be the subject of ongoing monitoring for potential inclusion in future intelligence assessments and bulletins.

Another iteration of the NCIE, focusing on OCG involvement in financial crime markets, including fraud and money laundering, will be produced at a later date.

Illicit Drug Criminal Market Profile

A total of 664 OCGs are assessed as high, medium or low level threats in 2018. The illicit drug trade provides organized crime with one of its most financially lucrative criminal markets; over 90 percent of assessed OCGs are involved in at least one illicit drug market in 2018. These OCGs either directly control or indirectly influence all aspects of the illicit drug market whether it be production, importation or distribution. Of these:

- 186 are involved in the methamphetamine market
- 128 are involved in the fentanyl and analogues market
- 496 are involved in the cocaine market
- 118 are involved in the heroin market
- 293 are involved in the cannabis market

The NCIE assesses the scope and magnitude of the main criminal markets. A focus on organized crime activities and their markets, in addition to groups or individuals, is necessary to produce an objective basis for setting law enforcement investigative priorities. For instance, strictly focusing on specific OCGs may not properly consider organized crime involvement in new and emerging markets causing substantial harm, such as fentanyl and other new potent opioids. The *2018-19 NCIE* aims to provide additional context to law enforcement, government and the Canadian public by assessing the markets at highest risk. This assessment will be repeated in subsequent iterations of the NCIE to monitor trends and improve methodology.

Table 1 provides the level of threat attributed to the five primary drug markets in Canada. Methamphetamine, fentanyl and its analogues, and cocaine are the criminal markets posing the highest level of threat to Canada in 2019-20. Heroin is assessed as a medium threat, and the threat posed by the illicit cannabis market is low. For the purpose of this assessment, levels of threat were determined by considering variables such as customer demand, supply (availability of products, ease of movement/sale), ease of market entry and profitability, law enforcement capability, harm, and history of organized crime involvement.

Table 1 – Illicit Drug Market Threat

Market	Threat	Rationale	Page
Methamphetamine	**High**	High potential for abuse and dependence, with reported increases in the availability, demand and harms in most regions of Canada and growing OCG involvement at all levels of production, importation and distribution.	**7**
Fentanyl and its analogues	**High**	Intelligence indicates that over 4000 opioid-related deaths in Canada can be expected in 2019 as a result of increasing availability across Canada, including new and more potent opioids and fentanyl analogues. Profitability and relative ease of entry will continue to entice OCGs to enter this market, and law enforcement capability will continue to be challenged by importation and trafficking by independent cyber-enabled operators.	**12**
Cocaine	**High**	This market remains profitable and consistently attracts more OCGs than any other criminal market in Canada. Resurgence in domestic and international use and trafficking against a backdrop of signs of rising coca cultivation and cocaine production in Latin America.	**16**
Heroin	**Medium**	The market is being displaced by fentanyl and its analogues in Western Canada; however, longstanding heroin importing and trafficking networks continue to import competitively priced Afghan heroin in the Greater Toronto Area (GTA).	**19**
Cannabis	**Low**	Cannabis is a relatively safer drug, but it is not benign and risks and harms are associated with its use. OCG involvement will not be overly affected in the short term in light of shortfalls in the legal cannabis supply. In the long term, OCG market share will decrease as licit market supply increases. However, OCG involvement in the licit domestic economy will likely increase overtime.	**24**
Other Drug Markets	**Ongoing Monitoring**	Markets to be monitored include, but not limited to: Opium, Ketamine, Hydromorphone, MDMA, New Psychoactive Substances.	**30**

Methamphetamine

Overview

Methamphetamine has emerged as one of the most significant national-level market threats in Canada with entrenched organized crime involvement at all levels of production, importation and distribution. Domestic use of methamphetamine has risen over the past five years, and its prevalence is expected to continue to grow due to its availability, low costs and ease of production. Its harmful impacts will increasingly be felt beyond the individual user, posing greater risks to communities, including law enforcement and first responders.

The domestic market is largely supplied by Canadian-produced methamphetamine, which is moved interprovincially from three main production hubs in British Columbia, Ontario and Quebec to meet domestic demand. 'Super labs' capable of producing large amounts of methamphetamine cater to wholesale distributors from various organized crime spheres and threat levels. Methamphetamine is also imported from abroad, though in smaller quantities. Overall, the total supply of methamphetamine likely exceeds domestic demand and OCGs will continue to export methamphetamine to meet international demand in profitable international markets such as Australia and New Zealand.

The number of OCGs involved in this market has increased from 145 groups in 2015, to 186 in 2018, representing a 28 percent increase over the last three years. OCGs will continue to exploit the characteristics that make this market appealing, including the fact that methamphetamine can be produced domestically with readily available, inexpensive chemicals. Moreover, most of these chemicals are not controlled and can be purchased at hardware, grocery, pharmacy and supplement stores.

Supply Origins – Domestic and Foreign

The majority of methamphetamine consumed in Canada will continue to be produced domestically in illegal-clandestine laboratories. In 2018, 23 assessed OCGs are involved in methamphetamine production, with the majority of groups based in British Columbia and Ontario. Methamphetamine production is also known to occur in Quebec and Alberta, albeit to a lesser degree. Methamphetamine is moved interprovincially from these main production hubs to meet demand throughout Canada (See Figure 1 for an overview of organized crime involvement in the methamphetamine market, by province and role).

Ephedrine-based production is currently the most common production method utilized, supplying methamphetamine in crystal (crystal meth) or powder form to domestic and international markets. However, in Quebec, where up to 95 percent of the market is in the form of pills, OCGs usually produce methamphetamine using the reductive amination method, which uses the precursor Phenyl-2-propanone (P2P) instead of ephedrine. Methamphetamine pills are subsequently moved interprovincially from Quebec to Atlantic Canada and Eastern Ontario.

Interconnectivity analysis suggests that that a number of OCGs are likely collaborating in the production of methamphetamine in British Columbia, including in the acquisition of precursor chemicals. While some of these groups individually may pose a low- or medium-level threat, when combined they form the highest threats nationally. These British Columbia and Ontario-based groups likely have access to 'super labs' capable of producing kilogram-levels of methamphetamine.

In addition to domestic production, the supply of methamphetamine in Canada continues to be furnished by imports from abroad, albeit to a lesser degree, mostly originating from Mexico and the Netherlands. A total of 12 assessed OCGs are importing methamphetamine in 2018. A majority of these groups are international in scope with associations to either the U.S. or Mexico, and are also involved in importing of cocaine. After a series of U.S. federal government restrictions on the sale of medicine containing methamphetamine precursors, a significant proportion of the production moved from the U.S. to Mexico and the U.S. market is now largely supplied by Mexican 'super labs'. It is likely that methamphetamine is smuggled through established cocaine supply lines and trafficking routes, suggesting that Canadian OCGs will face increasing competition from Mexican methamphetamine moving into domestic and international markets.

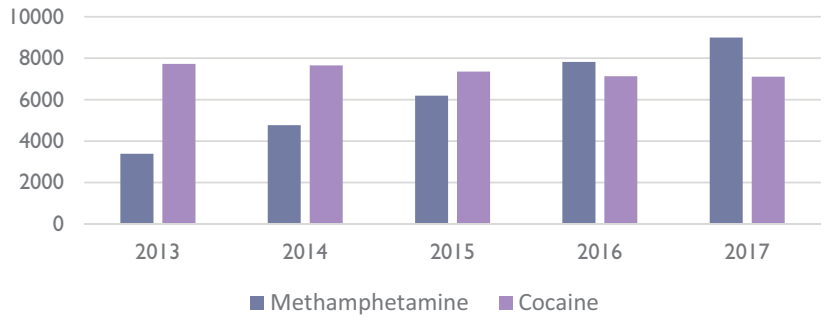
Most of the precursors and other chemicals used for methamphetamine production in Canada are nonregulated or have regulations that will continue to be successfully circumvented by OCGs. Ephedrine and pseudoephedrine, both of which are legally available, are two common precursors used in the production of methamphetamine in Canada. Pseudoephedrine can be extracted from common cold and decongestant medications, while ephedrine can be bought from nutritional, pharmacy and supplement stores. Canadian-based methamphetamine production is fueled by the overwhelming domestic availability of ephedrine tablets. Ephedrine can be sold to anyone in Canada respecting the established threshold on a maximum of 8 mg per tablet and a maximum of 40 mg per container. Currently, there is no limit existing on the amount of containers a person can obtain. The remainder of the essential chemicals for methamphetamine production, such as solvents, acids and bases, can be found in common household items or purchased independently on their own. For example, iodine crystals continue to be imported legally, despite having few legitimate uses for Canadian businesses.

Figure 1 - Organized Crime Involvement in the Methamphetamine Market, by Province and Role

Demand and Use Trends

Methamphetamine is amongst the most prevalent substances in the Canadian illicit drug supply. This trend is likely to continue as methamphetamine is highly addictive, easy to obtain, and relatively inexpensive. Methamphetamine is now the third highest controlled substance seized by Canadian law enforcement agencies, following cannabis and cocaine. Moreover, a comparison of methamphetamine and cocaine possession incidents over time show contrasting trajectories (see Figure 2). While methamphetamine possession incidents have increased by over 160 percent between 2013 and 2017, cocaine possession incidents have steadily trended downward during the same period. British Columbia, Alberta, and Saskatchewan had the highest methamphetamine possession rates per capita in 2017, while Manitoba had the greatest increase in possession incidents since 2013. Likewise, the number of times that methamphetamine was identified by Health Canada's Drug Analysis Service (DAS) increased by 152 percent between 2012 and 2017 and its presence in DAS analysis results is now as common as cocaine. The biggest increase were reported in Manitoba, Alberta, and Saskatchewan with 606 percent, 633 percent and 1400 percent, respectively.[1]

Figure 2 - Methamphetamine and Cocaine Possession Incidents in Canada, by Year



Source: Statistics Canada

Despite supply reduction efforts, methamphetamine prices are generally trending downward domestically, further enticing use. Internationally, a combination of high demand and high prices in some regions will continue to prompt Canadian-based OCGs to export methamphetamine. Methamphetamine is currently inexpensive in all its forms nationally, with an average of around $90 per gram, but is noticeably cheaper in Vancouver. Prices can vary for several reasons, such as proximity or access to producers or importers, quality, and form. Cocaine, like methamphetamine, is classified as a stimulant and is generally more expensive – $100 per gram on average in Canada. Additionally, the high that comes from using methamphetamine is much longer than cocaine, with effects lasting up to 24 hours. This makes methamphetamine an attractive and affordable alternative for some users. Nonetheless, the total supply of methamphetamine likely exceeds domestic

1 Health Canada's Drug Analysis Service (DAS) is responsible for testing suspected controlled substances that are seized. DAS asks that exhibits be submitted only when verification of the actual substances is required for court purposes. It is not uncommon for multiple exhibits to be submitted from the same seizure nor is it uncommon for multiple results to be entered in the database for the same exhibit. Exhibits analyzed by DAS likely represent a subset of the substances seized by law enforcement agencies, which would also be a subset of the substances found on the illicit market.

demand and OCGs will continue to export methamphetamine to meet international demand in profitable international markets. For instance, given that prices in Australia and New Zealand can be over eight times higher than in Canada, it is expected that Canadian OCGs will continue exporting to these countries.

As methamphetamine use increases, it will likely continue to be consumed in conjunction with other stimulants and depressants, increasing the risk of overdoses. There are indications that fentanyl users are actively mixing fentanyl with methamphetamine. Fentanyl was detected in 77 percent of methamphetamine overdose cases in British Columbia between 2016 and 2017. There are indications that methamphetamine is also being mixed with cocaine in parts of Saskatchewan, Nova Scotia and Ontario, suggesting traffickers are mixing the two in order to increase profits.

Harmful impacts will increasingly be felt beyond the individual user. Methamphetamine is believed to be a major contributing factor in recent surges of violent offences, including use of weapons and violent attacks on individuals. Hospitals are facing increasing rates of methamphetamine fueled violence on staff members, prompting the need for additional security measures. With no current treatment to counteract the effects of methamphetamine, risks to communities is high due to the psychotic and irritable symptoms of methamphetamine that may escalate situations.

Future Consideration

The ease with which methamphetamine can be obtained or manufactured is a major contributing factor to the increase in methamphetamine use. Domestic methamphetamine production will continue to expand as long as OCGs can successfully circumnavigate the existing precursor control regulations. The violent behaviours associated with methamphetamine use will continue to pose challenges to law enforcement and first responders. Moreover, an expanding methamphetamine market will be a factor in the number and severity of instances of violent occurrences.

Fentanyl and its Analogues

Overview

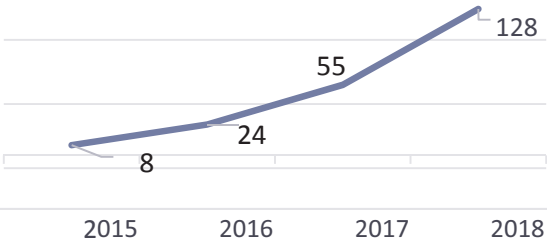
Fentanyl is now present across Canada. It has emerged as a distinct market in communities hit hardest by the opioid crisis. Overdoses continue to escalate in Western Canada and Ontario, placing increasing pressure on health care and public safety resources and exposing frontline personnel and first responders to the risk, albeit limited, of inadvertent exposure. Misuse and diversion of pharmaceutical fentanyl has contributed to the opioid epidemic, however illicit fentanyl and its analogues increasingly taint illicit drugs, causing the majority of unintentional apparent opioid-related deaths in Canada.

Opportunistic individuals and OCGs are increasingly involved in fentanyl trafficking and continue to exploit the characteristics that make fentanyl appealing. These include the fact that fentanyl is easily procured through various surface and dark web platforms; its potency allows for trafficking in small amounts; its ease of concealment makes it difficult to detect; and it is addictive and highly profitable. Fentanyl is predominantly imported from China, however increasing enforcement on Chinese fentanyl, its precursor chemicals, and analogues has and will lead to diversification of transshipment routes and new source locations such as Mexico. The trend toward new and more potent fentanyl analogues to which standard doses of naloxone are less effective will increase the potential of overdoses and deaths, as well as limited risk of inadvertent exposure to first responders.

Organized Crime Involvement

In the past year, the number of OCGs reported to be involved in the fentanyl market has increased by 133 percent (see Figure 3). These groups are present in every province and territory, except for Prince Edward Island, Northwest Territories, and Nunavut, with the majority of groups concentrated in British Columbia and Ontario. The latter two provinces are also where assessed groups are reported to be involved in fentanyl precursor chemical importation. Vancouver and Toronto are two of Canada's busiest container port and air cargo destinations, which likely allows groups with frequent and ease of access to incoming shipments. Groups facilitate the acquisition of precursor chemicals by using businesses or shell companies that exploit precursor licences in order to supply the illicit market.

Figure 3 - OCG Involvement in the Fentanyl Market, by Year



Seizures of fentanyl precursor chemicals continue to increase. Few clandestine labs have been detected and are likely increasingly difficult to locate due to a shift from the use of urban locations to rural properties. To date, labs have been located in British Columbia and Quebec. These labs have been described as sophisticated, with value in equipment consistent to the investment made by large OCGs. OCGs in Canada are known to be involved in poly-drug trafficking, and those already involved in the synthetics market face minimal barriers for producing fentanyl, including supplies easily obtained via online vendors and basic laboratory skills.

In addition to the rise in OCG involvement, independent criminal entrepreneurs continue to exhibit a presence in the online procurement and trafficking of fentanyl. In 2017, FINTRAC data revealed a significant increase in individuals providing online payment to chemical and pharmaceutical companies in China known to fulfill orders for fentanyl. Fentanyl is mainly imported and re-distributed using the mail stream with customers placing orders mostly via dark web marketplaces using virtual and cryptocurrencies, which provides anonymity to vendors and purchasers. Dark web vendors have shipped fentanyl to hundreds of domestic and international customers, including in Europe, Australia, and New Zealand. Most opportunistic individuals work independently and have no connection to or background in organized crime.

Production, Transportation and Distribution

China will likely remain the primary supplier for illicit fentanyl, analogues and precursor chemicals to Canada, although diversification of transshipment points will likely be the preferred strategy of suppliers and purchasers in an effort to avoid targeted enforcement on shipments. Online sellers from China have begun to transship purchases through other countries to reduce the risk of a package being identified and seized by customs officials. Suppliers are also using new and innovative concealment methods and creating new forms of fentanyl and analogues with similar or more potent effects in response to increasing regulations, and in order to transit borders undetected.

Canada will likely see part of its fentanyl supply sourced from other countries, with Mexico as the greatest threat. Mexican drug cartels are believed to be shifting from heroin production to fentanyl production, given declining opium prices in Mexico and the recent discovery of a clandestine lab. As seen in the U.S., the cartels will likely use existing transportation lines for cocaine to ship fentanyl to Canada. With the Canadian border in close proximity to the northeastern U.S., it is likely that Mexican drug trafficking organizations will aim to expand their operations north using their nexus to criminal groups in Canada.

Canada is likely to increase its role as a transshipment country for fentanyl due to the increasing demand for synthetic drugs in North America and abroad. The U.S. has the highest number of deaths associated to non-medical use of pharmaceutical opioids, including fentanyl and fentanyl analogues. Beyond North America, fentanyl use and related overdoses are also increasing in the U.K. (England, Wales), and Australia. A proposed reduction in the availability of prescription opioids in the U.S. by one-third within three years will likely result in users seeking fentanyl from the illicit market. In Canada, criminal entrepreneurs already involved in the sale of diverted pharmaceutical fentanyl patches and dark web vendors selling fentanyl internationally are likely to capitalize on the opportunity to supply a potentially growing demand for fentanyl. In 2018, CBSA noted a rising number of outbound postal seizures of fentanyl. Moreover, Canadian fentanyl export quantities seized in the first half of 2018 were eight times higher than in mid-year 2017, an indication that Canadian involvement in export activities is on the rise.

Fentanyl will likely continue to displace heroin as the preferred opioid of choice by OCG traffickers and consumers in niche markets within Western Canada and Ontario as the continuous influx of illicit fentanyl perpetuates user demand. Fentanyl now represents the largest proportion of all opioids identified in substances seized by law enforcement, surpassing that of heroin (see Figure 4). Furthermore, fentanyl and analogues are increasingly identified in exhibits of illegal drugs seized (see Figure 5)[2].

Figure 4 - Seized Exhibits, Heroin vs. Fentanyl, by Year

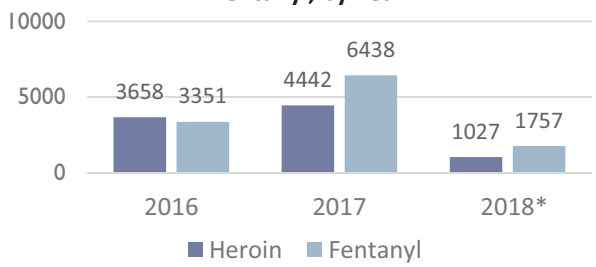
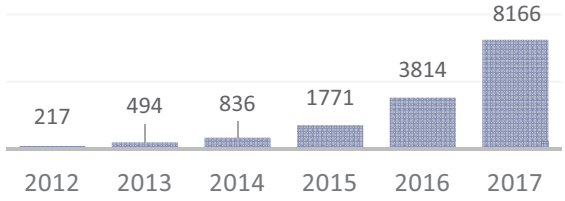


Figure 5 - Number of Exhibits Containing Fentanyl or Analogues, by Year



Source: Health Canada
* Jan-March 2018 only

Fentanyl is now predominantly seized in powder form in Canada, while pills and patches are more commonly seized in Quebec and Atlantic Canada. Although predominantly marketed to heroin and methamphetamine users, fentanyl is also marketed to new consumers, disguised as counterfeit prescription pills or other illicit drugs. Users unknowingly consume fentanyl, resulting in inadvertent addiction. Users who prefer heroin and are inadvertently exposed to fentanyl via adulteration may develop greater opioid tolerance.

Law enforcement in Ontario and British Columbia have reported seizing naloxone kits alongside illicit drugs, as dealers are said to be handing out kits and educating their clients on the proper use of naloxone as a strategy to prevent overdose deaths. In several provinces, dealers are incorporating dyes as a way to differentiate or distinguish their products and in Ontario a spectrum of coloured fentanyl is helping consumers to distinguish the relative strength of products.[3]

With the decrease in dispensing of prescription opioids in Canada, particularly in British Columbia, Alberta and Ontario, individuals who no longer have access to prescriptions may revert to the black market. Illicit fentanyl activity in Saskatchewan, Manitoba, Quebec and Atlantic Canada has remained relatively stable over the past two years, and is not expected to supplant heroin in these regions.

Demand and Use Trends

Stronger fentanyl analogues will likely become more prevalent in the illicit drug supply, with current naloxone doses less effective in combatting overdoses. This may result in the requirement for the administration of more naloxone than is contained in a standard dose, and possibly in the need for multiple administrations. With fentanyl

[2] See footnote on page 10.
[3] Relative potencies are anecdotal and have not been confirmed through analyses.

emerging as a distinct market in communities hit hardest by the opioid crisis, users are reportedly now specifically seeking out carfentanil directly. Carfentanil, a substance which is 100 times more toxic than fentanyl, is being detected more often in the analysis of seized samples. Figures released by Alberta included a 330 percent increase in accidental overdose deaths related to carfentanil in 2017. Moreover, Canada's largest carfentanil seizures occurred within the past year, with police in Durham region and Edmonton seizing 42 and 16 kg, respectively. Following three deaths in a single week in October 2018, health officials in Ottawa issued a warning regarding the circulation of a new fentanyl analogue which can be found in an array of colours. Some new, emerging analogues are said to be very potent, and a standard dose of naloxone may be insufficient, which can result in unsuccessful reversal of overdoses if additional doses are not available.

An emerging trend to purposefully combine fentanyl or fentanyl analogues with non-opioids will likely result in more overdoses and deaths amongst individuals who are traditionally non-consumers of opioids. While some fentanyl and non-opioid combinations are believed to be unintentional as a result of cross contamination, a recent trend suggests that these mixtures are becoming more purposeful by traffickers and users. Users are intentionally exposed to opioids in order to increase addiction, thereby expanding customer base. In British Columbia, illicit fentanyl was detected in 72 percent of cocaine-detected cases and 77 percent of methamphetamine/amphetamine-detected cases between 2016 and 2017. Whether taken unknowingly or deliberately, cocaine and methamphetamine users who have never developed a tolerance for opioids are at greater risk of overdose death. "Speedball 2.0" is an emerging trend whereby users combine fentanyl or fentanyl analogues with cocaine or methamphetamines. There is potential for this trend to grow in Canada, particularly with the increases in availability of fentanyl, methamphetamine and cocaine, and as Mexican and American OCGs with a nexus to Canada supply their products north of the Canada-U.S. border. This trend will not only present greater danger to recreational users who have never developed a tolerance for opioids, but to emergency personnel and law enforcement who should be aware and exercise vigilance and caution when handling victims or drugs that may seemingly involve non-opioids.

Future Considerations

The rapid evolution of synthetic drugs and in particular the prevalence of extremely potent synthetic opioids such as carfentanil will continue to pose challenges as naloxone becomes less effective in reversing overdoses. New, unregulated fentanyl analogues, enhanced concealment methods, diversified transshipment points, expanding e-commerce and increasing shipments via the postal mode will amplify the already difficult task of interdicting packages, specifically for fentanyl which can be sent in minute amounts and into multiple shipments.

Though Bill C-37 introduces amendments to the Controlled Drugs and Substances Act making it more difficult for OCGs to import and possess designated devices such as pill presses and encapsulators, these added controls do not affect existing groups who already have access to such equipment. Increasing regulations on China along with targeted enforcement on dark web activity and the postal stream may lead to domestic fentanyl synthesis. As OCGs become increasingly involved in the fentanyl market, with the potential likelihood for Canada to become an export country, policing agencies can likely expect increased requests from international partners to assist in addressing these activities.

Cocaine

Overview

Cocaine is available predominantly in two forms, powdered cocaine and crack cocaine, and is present across the country. Following years of stability, the domestic demand for cocaine is on the rise with usage rates doubling from one percent (353,000 users) in 2015 to two percent (730,000 users) in 2017. Historically coca production has been limited to Colombia, Bolivia (Plurinational State of) and Peru. However, coca plantations have recently been found in Guatemala and Honduras. While these are much smaller in scale, they may represent test fields to determine the viability of growing coca in new regions closer to Mexico. Not only could this lead to an increase in the global supply of cocaine, it could also represent a change in transportation and distribution routes.

High level Canadian cocaine importers have been recently killed in Mexico and in Canada. While the reason for the murders and the perpetrators behind them remain unknown, it could signal an attempt by Mexican cartels to remove competition and re-establish operational cells in Canada to oversee the import of cocaine for Canadian distribution. Should this occur an increase in violence can be expected; however the level of violence is not expected to reach that seen in Mexico.

Recent large international seizures indicate that transit routes for cocaine destined for Canada are shifting towards smaller Caribbean and South American countries in an effort to circumvent the increased presence of law enforcement around known transit routes.

Production and Supply Trends

Since 2016, there has been an increase in coca cultivation, led predominantly by Colombia which accounts for 68.5 percent of the global cultivation area. The profitability of coca cultivation for farmers coupled with the profits for organized crime will remain obstacles to a sizeable reduction in the supply of cocaine, for the foreseeable future.

Along with the increase in production, there has also been an increase in global cocaine seizures. The UNODC reported a 20 percent increase in its 2018 report compared to the previous year. This is in line with data released by the Drug Enforcement Administration (DEA) which showed a 23 percent increase in cocaine seizures along the southwest border of the U.S. In Canada, while the number of cocaine seizures at the border is on track with 2017 figures, the quantity of cocaine seized is down 68 percent compared to the same time period in 2017. Given the suggested increase in Canadian cocaine consumption, as well as the increased world production, the reduction in seizure quantities could be attributed to smaller quantities sent in higher frequency to minimize seizure losses, or an increase in international seizures before they arrive at Canada's border, or law enforcement targeting lower yielding modes, such as the postal system.

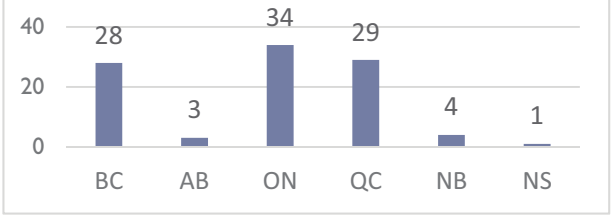
Organized Crime Group Involvement

Domestic

In 2018, approximately 75 percent of assessed Canadian OCGs play a role in the cocaine market. The large number of groups involved is indicative of the availability of cocaine and the continued profitability of the illicit commodity. While there are some conflicting reports on the shortage of cocaine or price increase at the kg level in Nova Scotia, Quebec and British Columbia, this shortage is likely temporary, attributed to larger international seizures that occurred over the summer that were likely destined for Canada, and are likely affecting certain distribution networks.

Out of the 496 OCGs, there are 99 groups that are importing wholesale quantities of cocaine. The majority of these groups are located in British Columbia, Ontario and Quebec (see Figure 6) parallel to the distribution of Canadian population in many of Canada's largest urban centres along with the location of marine ports and international airports. A number of Canadian OCGs, as well as individuals linked to OCGs, travel extensively to source countries or known transit countries for cocaine.

Figure 6 - OCG Involvement in the Importation of Cocaine, by Province



International

The wholesale movement of cocaine to the Canadian market is believed to be controlled primarily by Mexican cartels, as well as a number of Colombian organized crime groups. In Colombia, with the peace agreement reached between the government and the Fuerzas Armadas Revolucionarias de Colombia (FARC) there has been a rise in FARC dissident groups that do not abide by the FARC peace process. The large hierarchal cartels in Colombia are being replaced by smaller more fluid OCGs. As a result, there are many new groups which keep a lower profile and are harder to target.

Although it is believed that nearly all of the cocaine transiting Canadian borders is a result of cartel involvement to some degree, at present, collaboration between Canadian individuals and Mexican/Colombian OCG members continues to occur primarily outside of Canada in source or transit countries, rather than cartel members physically operating in Canada.

High level cocaine importers with known links to Mexican cartels have been recently killed in Mexico. Although Canadian cocaine traffickers have been killed in the past in Mexico, the number of high level importers killed in 2018 represents an anomaly. While the reason for the murders, as well as the perpetrators behind the killings remain unknown, they could signal a shift whereby Mexican cartels may be looking to remove competition and to re-establish operational cells in Canada. Conversely, it is possible that their killings may be a result of the resistance of Mexican cartels to an increased presence of Canadian OCGs in Mexico proper.

Emerging Transit Countries

The Dominican Republic, Mexico and the U.S. are well known and established transit countries for cocaine destined for Canada; however, a number of recent Canadian seizures and seizures involving Canadians abroad suggest that alternative transit routes are becoming more popular. In 2018, seizures have occurred in smaller countries in the Caribbean and in Latin America that may represent an effort to circumvent the heavy presence of law enforcement around traditional transit routes. In Oceania, likely as a result of increased enforcement around Australia and New Zealand, OCGs have started using smaller Pacific Island nations as transit points.

Canada as a Transit Country

Even though the Canadian demand for cocaine has increased, the stability of the domestic price at the kilogram level, between $50,000 and $65,000, and at the street level, around $100 per gram, suggests that domestic OCGs are continuing to export cocaine to more lucrative markets. Canada is one of the top origin countries for cocaine seized through the postal system in Australia. This is likely to continue, as cocaine prices in Australia and New Zealand at the kg level range from $177,000 to $295,000. Additionally, Western Europe has seen an increase in both demand and consumption rates as well as an increase in cocaine seizures, and there are indications that Canadian OCGs are already involved in the trafficking of cocaine to Europe.

Future Considerations

Importers will continue to be a viable group for targeting due to their reduced numbers and vital role they play in the Canadian cocaine market, however intelligence gaps still exist as individuals with seemingly no links to organized crime continue to be apprehended entering Canada with wholesale levels of cocaine.

Recent interdictions of larger shipments of cocaine will likely lead to a shift towards smaller quantities being sent in higher volume to diminish the impact of future seizures. Additionally, OCGs are likely to continue establishing new transit countries and routes to circumvent law enforcement detection.

If Canada continues to export cocaine to other markets, international partners are likely to increase requests for Canada to prevent cocaine from reaching their countries. This will present resource challenges for existing law enforcement and border service resources.

Heroin

Overview

Heroin is a highly addictive semi-synthetic opioid derived from the opium poppy plant which is grown in regions such as Southeast and Southwest Asia, Mexico, and Colombia. In Canada, this drug commonly appears in the form of a white or off-white powder, which is similar looking to a synthetic opioid, fentanyl.

The adulteration of heroin with fentanyl and its analogues reached 62 percent nationally in 2017 with levels ranging as high as 70-85 percent in some western provinces. The heroin and fentanyl markets are highly intertwined as they belong to the same family of opioids and target similar users. OCGs and local drug traffickers are cutting heroin with fentanyl and its analogues to increase its potency and profits, or inadvertently mixing the two drugs during the milling process. Health risks to users have increased as consumers misidentify fentanyl as heroin. Refer to fentanyl section for further information on this synthetic opioid.

The number of reported OCGs involved in the heroin market continues to increase, and this is likely in part due to heightened law enforcement action dedicated to combatting the opioid issue in Canada. The number of reported OCGs assessed as being involved in the heroin market rose 44 percent (82 to 118 OCGs) from 2017 to 2018, while during the same period, the number of OCGs reported as being involved in both heroin and fentanyl markets approximately tripled from 20 to 62 groups. The increase in the number of OCGs involved in heroin occurred even though the known heroin user population did not increase, suggesting the increased targeting of fentanyl helped identify groups also involved in the heroin market.

Production

The majority of the heroin in Canada continues to be sourced from Afghanistan, with some coming from Mexico. Afghanistan will continue to remain the primary source country for heroin seized in Canada, with Mexico becoming a viable source country. This is in contrast to the current U.S. situation, where the majority of heroin is sourced from Mexico. According to the United Nations Office on Drugs and Crime (UNODC), there was an increase in the global supply of heroin as the total global opium manufacture reached its highest estimate recorded in 2017. Afghanistan was the largest driver of this increase from 2016 to 2017, however, this global increase has not been linked to a growth or price fluctuation in the Canadian heroin market.

Mexico is becoming a source country due to its increased levels of opium production, rising levels of heroin quality, and its close geographic proximity to Canada. Opium production levels in Mexico rose to record levels in 2017, and subsequently, the potential pure heroin production in Mexico also rose by 37 percent (81-111 metric tonnes) during this time period. Additionally, Mexican cartels now use more refined processing methods to produce a higher quality white powder strain of heroin known as China White[4]. Due to Canada's close geographic proximity to the U.S., and the rising quality of Mexican heroin, it is expected that Mexican heroin will be increasingly be seized within Canada.

[4]China White is believed to have purity levels up to 98 percent.

Afghan heroin, known to be of high quality, is likely being adulterated by Canadian drug traffickers after arriving into Canada. In contrast, Mexican heroin has a greater potential for being adulterated or contaminated with fentanyl within its country of origin. This suggests that Mexican heroin could present greater safety risks to users than Afghan heroin as it is likely to have been contaminated with fentanyl prior to entry into Canada.

Transportation and Distribution

Smuggling Routes

South Africa continues to be a key transit point for heroin to Canada. Afghan heroin typically arrives in South Africa via the "southern route" of heroin trafficking through East Africa. According to the UNODC, traffickers are likely to increasingly shift heroin landing points in Africa in order to avoid law enforcement activity around Kenya and Tanzania. Other common heroin transit countries include Malaysia, India, and Pakistan.

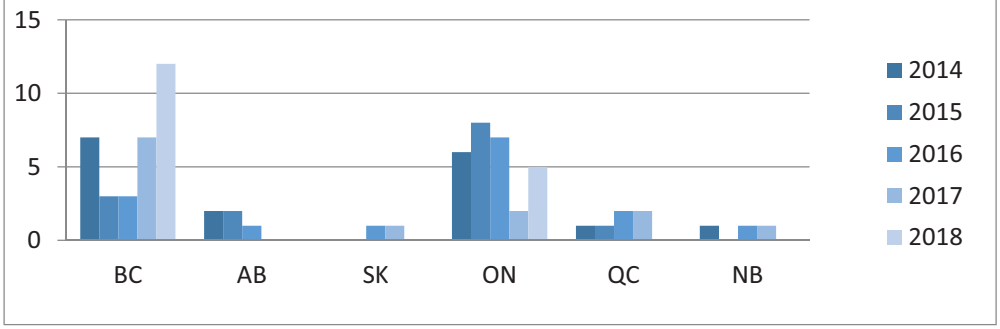
Canadian OCGs importing heroin via Sub-Saharan Africa could become increasingly difficult to disrupt due technological advances within this region. In 2018, approximately 18 percent of Canadian OCGs involved in importing heroin were linked to African countries or regions. In northern Mozambique, the growth in the number of users of mobile software and encrypted message systems have led to the creation of networks of freelance drug traffickers. This creates additional challenges for the disruption of Canadian OCGs involved in heroin due to their evolving and increasingly anonymous heroin supply chain.

Additionally, Mexican cartels, or Canadian OCGs with connections to them, can increasingly push Mexican heroin into Canada via well-established cocaine trafficking routes. Direct travel links and lifted visa restrictions, coupled with the increased level of heroin production in Mexico and saturation of the U.S. market, may increasingly make Canadian cities along direct flight paths as entry points for Mexican heroin.

Canadian Organized Crime Group Involvement

In 2018, a total of 17 OCGs were assessed as being involved in the importing of heroin, with the majority based in British Columbia, followed by Ontario and Quebec. Figure 7 shows the provinces that have OCGs that are involved in heroin importing.

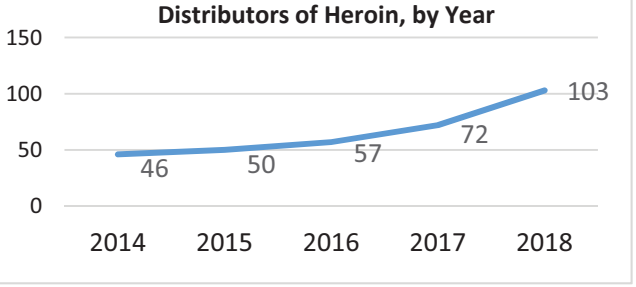
Figure 7 - OCG Networks Involved as Importers in the Heroin Market by Province, 2014-2018



OCG networks based in western and central Canada likely source heroin from differing countries of origin. The OCGs reported as importers based in British Columbia are most commonly linked to the U.S. and Mexico, whereas those based in Ontario are linked to Pakistan and India. This suggests that Ontario-based OCGs are sourcing heroin predominately from Afghanistan via their Southwest Asian connections, and British Columbia-based OCGs may be sourcing Mexican heroin via well-established drug supply lines, and transiting through the U.S.

The targeting of groups involved in distributing illicit opioids contributes to the higher number of reported and assessed OCGs in the heroin market. In 2018, there were 103 OCGs assessed to be involved in distributing heroin versus 72 in 2017 (see Figure 8). Similar to importers, most distributors are reported as being based in British Columbia, with 55 OCGs having this role in 2018, which is up from 38 OCGs in 2017. Of note, 66 percent (21 groups) of the newly reported OCGs involved as distributors of heroin in British Columbia were also involved in the fentanyl market. Thus, the reported increase in number of British Columbia-based OCGs involved as heroin distributors is likely due to enhanced discovery of groups involved in fentanyl.

Figure 8 - Number of OCGs Involved as Distributors of Heroin, by Year



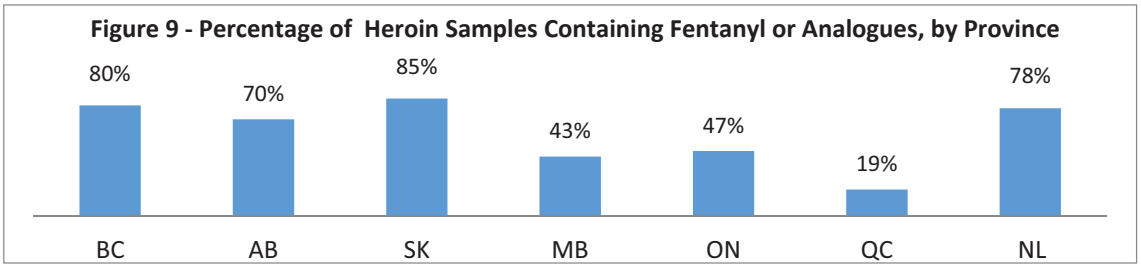
Regional Markets

The introduction of fentanyl into the heroin supply has created distinct regional heroin markets within Canada. In British Columbia, the market is already saturated with heroin adulterated with fentanyl, and some western provinces are already following this trend (i.e. Alberta and Saskatchewan). There continues to be a market for heroin in central Canada, however, there are reports of a trend of heroin laced with fentanyl already occurring in Ontario, albeit at a slower rate than British Columbia. It is expected that heroin laced with fentanyl will continue to spread west to east across the country, infiltrating the heroin market within central Canada. (See Figure 10 on the next page for an overview of adulteration rates per province).

Western Canada

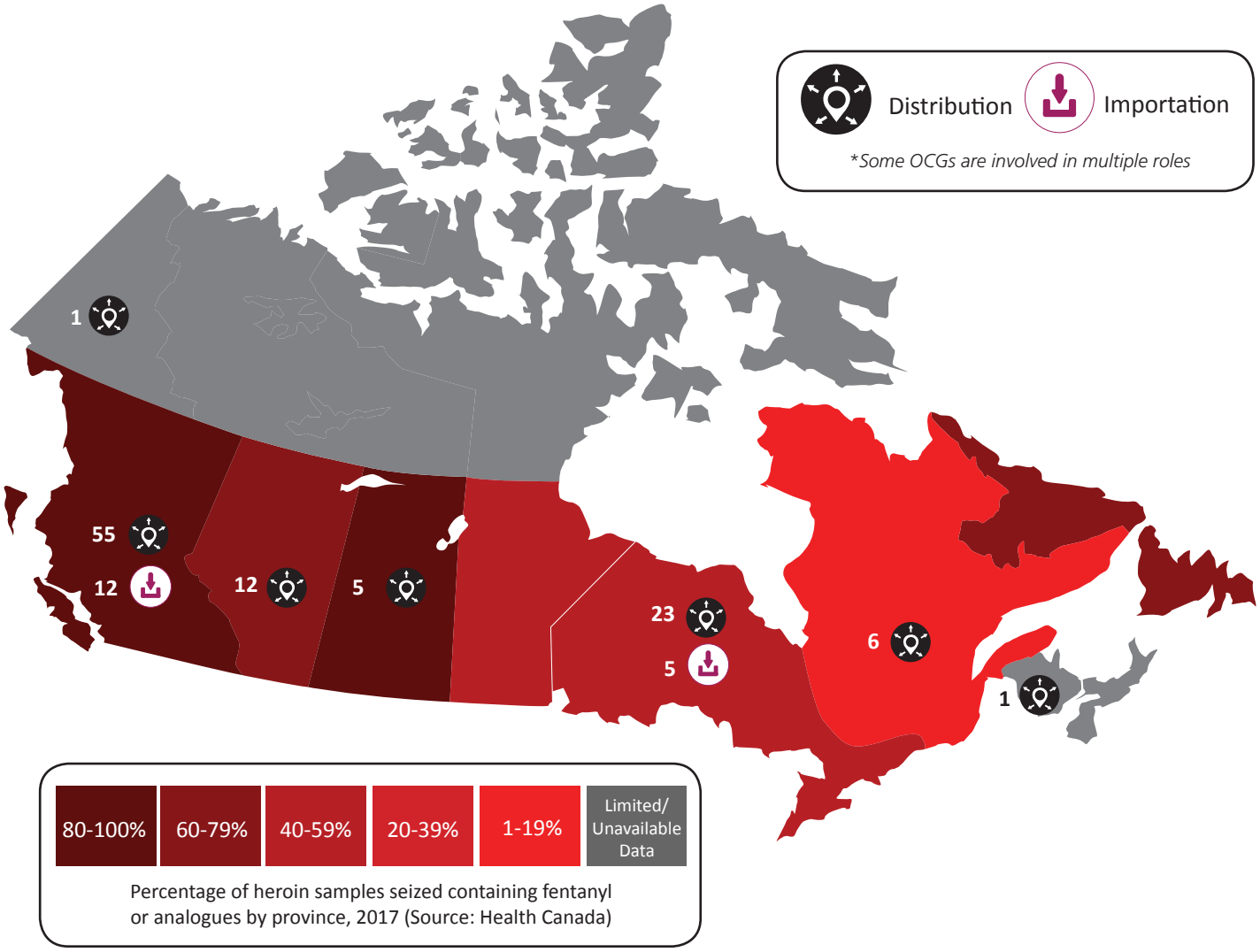
The heroin market in British Columbia has already experienced displacement, and Alberta and Saskatchewan will likely follow this trend as the prevalence and purity levels of heroin are becoming increasingly lower, and the majority of heroin in these provinces now contains fentanyl or analogues. In urban centres such as Vancouver, the reported opioid market of choice by users is now fentanyl and pure heroin is rare and difficult to find. In Alberta and Saskatchewan, a total of 70 percent or higher of heroin samples analyzed by Health Canada contained fentanyl or analogues (see Figure 9).

Figure 9 - Percentage of Heroin Samples Containing Fentanyl or Analogues, by Province



(Source: Health Canada)

Figure 10 - Heroin Market in Canada by Adulteration Rate and Organized Crime Involvement



Central Canada

In central Canada (i.e. Ontario, Quebec), the heroin market continues to be present due to higher availability and purity levels, but this market will likely follow trends seen in western Canada in coming years, especially if OCGs distribute Mexican heroin.

Over half of the samples analyzed in central Canada did not contain adulterants such as fentanyl or analogues. Further, heroin remains competitively priced with fentanyl in certain cities within Ontario and Quebec, ranging roughly from $30-40 per point (0.1 grams) for both substances. This is likely due to these provinces having an established heroin user base, and receiving low priced, quality Afghan heroin from OCGs having ties to Southwest Asia.

The heroin market in Ontario is experiencing the spread of a strain of heroin called “purple heroin”. The street name is “purple pebbles” and it is a mixture of heroin and fentanyl or analogues, which is then dyed with purple food colouring. The colour is sometimes used as an indicator of purity and the presence of fentanyl. While this has been increasingly available in Ontario, this type of heroin has been declining in British Columbia over the past year, further demonstrating the regional differences within Canada. Purple heroin overdose alerts to the public were issued within several jurisdictions in Ontario, and a large seizure of this type of heroin has occurred. As the user base for purple heroin grows, this will likely lead to fentanyl more highly infiltrating the heroin market within this province in the medium to long-term.

Quebec has the lowest reported adulteration rates for heroin within Canada. Montreal has a unique market that consists mostly of white or pale powder, with the main substances used to cut the heroin being powdered sugar, acetaminophen powder, and to lesser degree, caffeine and Dextromethorphan. There were a few reported cases where fentanyl and carfentanil were used as a cutting agent, and this is believed to be due to the smaller opioid consumer market within Quebec. However, due to the ease at with which OCGs can obtain fentanyl via the dark web and use it as a cutting agent to enhance profits, it is likely that there will be a shift to increasingly using this drug as an adulterant over time.

Atlantic Canada

In Atlantic Canada, heroin is likely supplied by OCGs based in Ontario and Quebec, but user demand is low. The market for heroin in this region is expected to remain limited for the foreseeable future due to the well established illicit pharmaceutical opiates market. Users in this region traditionally use pills and they are not likely to seek alternative opioids such as heroin. OCGs in this region have been involved in the distribution of OxyCodone (e.g. OxyContin) and Hydromorphone (e.g. Dilaudid) for the past decade, without disruption.

Future Considerations

As OCGs are driven by user demand together with drug availability, they will continue to be involved in the heroin market in central Canada. Should OCGs and local traffickers follow the trends in British Columbia, the highly profitable, well-established, affordable, and quality heroin supply from Afghanistan could see more competition from Mexican heroin. This could result in the heroin supply being increasingly adulterated with fentanyl and its analogues.

OCGs based in Central Canada with direct links to countries involved in heroin manufacturing or distribution will likely seek to expand their illicit activities by targeting ethnic communities via shared cultural ties. It is likely that OCGs such as these will leverage their cultural connections to exploit growing cultural diasporas within Canada that are familiar with Afghan heroin.

Dominance over the heroin market in the GMA is in transition due to law enforcement’s targeting of Montreal-based heroin trafficking groups that had a former monopoly over this market, and this could potentially lead to growing conflict.

Cannabis

Overview

Cannabis was legalized for recreational use on October 17, 2018. The Cannabis Act is intended to create a competitive legitimate market and displace opportunities for OCGs to profit from this industry. Such displacement will largely depend on the availability, quality, and cost of cannabis produced anddistributed legally.

To date, given the varying provincial regulatory restrictions in regards to the sale and availability of cannabis – such as price, source, supply, quality, and consumer age – OCGs have unlikely experienced a measurable impact to their market share and are not likely to in the near future. Legalization may, in the short-term, actually place OCGs in an advantageous competitive position by creating increased consumer demand that cannot be met due to shortfalls in the legal cannabis supply, thereby allowing OCGs to maintain a significant presence in this market.

If the legitimate market does begin to displace illicit activities in the longer term, OCGs can be expected to continue to exploit implementation challenges, demand-management issues, and regulatory loopholes to push illicitly-sourced cannabis products into the marketplace. They may also increase their activities in other illicit markets; the majority of OCGs involved in cannabis are also involved in other illicit drug markets, and are unlikely to be disrupted by diminished returns in one commodity. Moreover, higher-potency cannabis products, such as shatter and a cannabis concentrate called THCA, remain illegal. While marijuana constitutes the bulk of cannabis manufactured and trafficked by OCGs, these products will continue to provide an alternate sale venue for involved groups.

Pre-Legalization

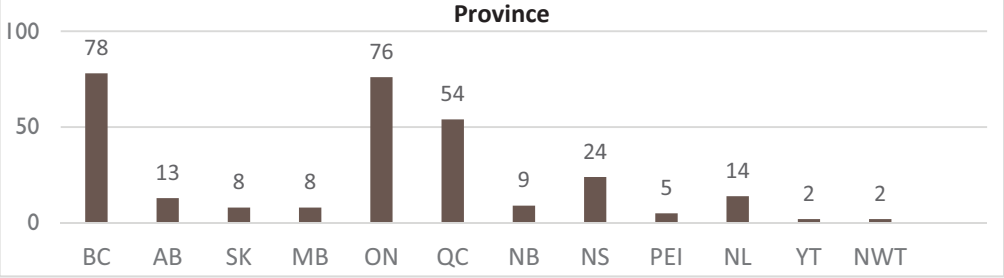
Organized Crime Landscape

The proportion of OCG involvement in the cannabis market has remained relatively stable over the past five years. Approximately 44 percent of OCGs were reported to be involved in the cannabis market leading up to the implementation of the Cannabis Act, primarily as marijuana manufacturers and distributors. Almost all of these OCGs are also involved in at least one other criminal drug market, such as cocaine, methamphetamines, fentanyl, andpharmaceutical opiates.

Numerous illicit cannabis dispensaries were operating in various provinces without licenses leading up to the implementation of the Cannabis Act. Several of these dispensaries have been linked to OCGs, and are reported to have provided extremely lucrative revenues.

While present in every province, the highest concentrations of OCGs involved in cannabis were in Ontario, British Columbia, and Quebec (see Figure 11), which correlates with Canada's primary criminal hubs and the largest proportion of overall OCG involvement. Although the modus operandi may shift to adapt to new regulations, their illicit cannabis activities are unlikely to cease. The same can be stated for cannabis exporters, although there is limited information in regards to OCG involvement in cannabis exports; only 10 OCGs were reported to be involved in this activity. Similarly, only a few OCGs were reportedly involved in cannabis importation, primarily in niche submarkets such as hashish (predominantly imported into Nova Scotia) and resin from Jamaica, Morocco, and Afghanistan.

Figure 11 - Number of OCGs Involved in the Cannabis Market, by Province



Key Assumptions of Legalization

One of the stated goals of the Cannabis Act was to combat the illegal market; it was enacted with the aim of removing an illicit and highly-profitable venue for criminals, and ultimately disrupting OCG operations. As such, the government has established a framework intended to control the production, distribution, sale, and possession of cannabis across Canada. The legitimate market was also intended to be competitively priced, easily accessible to consumers 18 years of age or older (subject to provincial or territorial restrictions), of high quality, and readily available – provisions intended to provide incentive to customers who purchase it illegally to acquire cannabis via legal means.

Post-Legalization

Exploiting Regulatory Variances and Undercutting the Legal Market

Cannabis legalization is unlikely to disrupt poly-drug OCGs, as their involvement in other markets secures an alternate stream of revenue. As almost every OCG reported to be involved in cannabis is also active in other drug markets, their diversity ensures continued profit in the event that the legitimate industry cuts into their illicit cannabis market share. Moreover, in the short-term, the current shortfall in the legitimate cannabis supply in Canada provides OCGs with a favourable competitive edge, whereby they continue to supply illicit cannabis to meet demand, at least until legitimate stock becomes more readily available.

Despite the large number of licensed producers, demand is exceeding supply and OCGs with existing grow operations are well-placed to fill this production gap. Given the delays in establishing licensed retailers in some provinces, OCGs are also likely to maintain their profit margins and shares in illicit retail cannabis sales while new licensing applications and approvals await processing. According to intelligence reporting, the current cannabis supply is unable to meet the projected demand. The limited number of approved retail establishments have already reported shortages in stock as initial consumer demand has exceeded expectations,

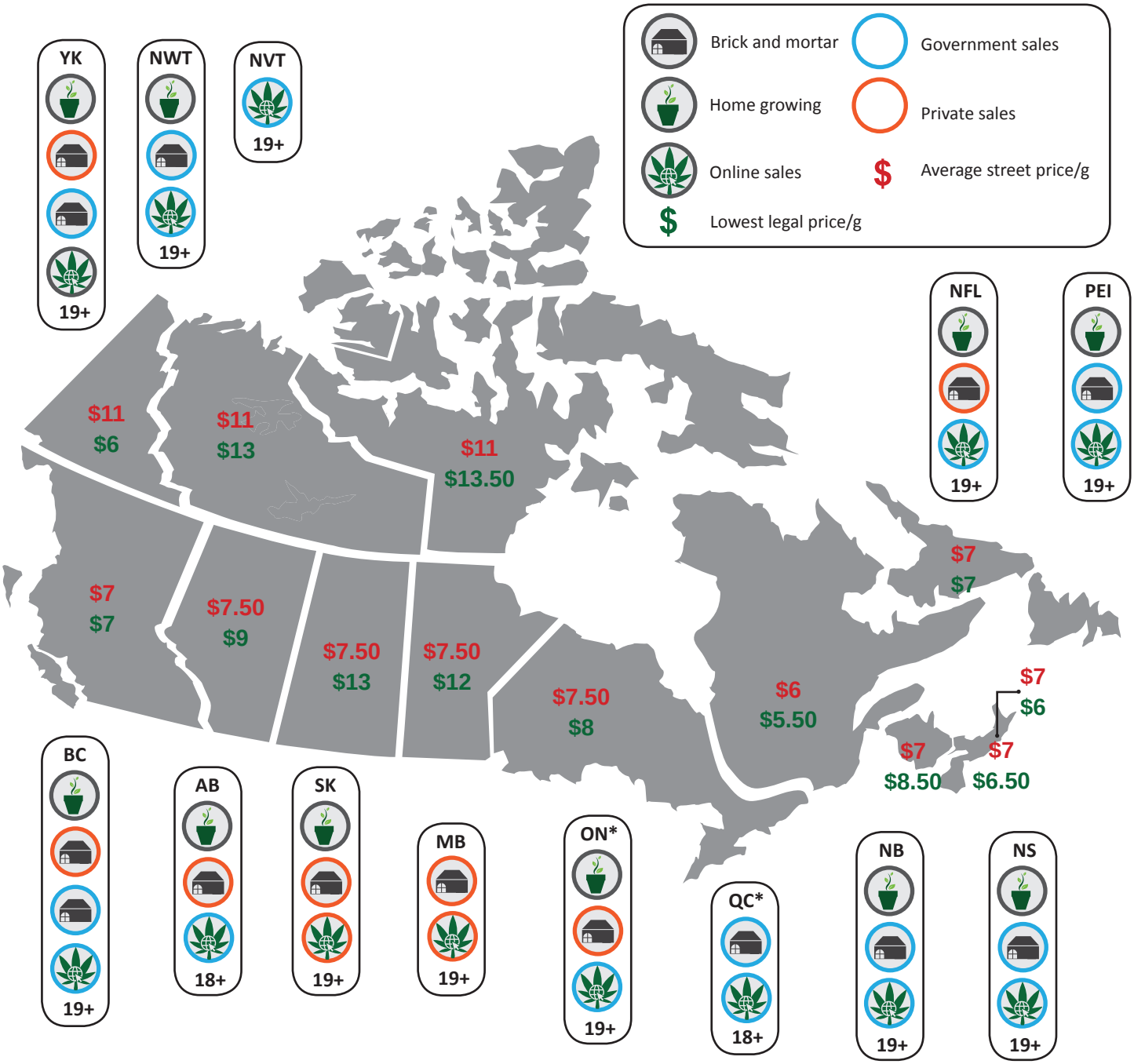
and delivery delays have resulted in some consumers turning to the illicit market to purchase cannabis. If intelligence reporting remains unchanged, the legitimate supply will not be able to meet demand until 2020. OCGs with an established grow operation, including those that have been using medical marijuana production licenses, are likely to be best-positioned to exploit any continued shortfall in the legitimate supply. As of September 2018, 118 producers were licensed by Health Canada under the Access to Cannabis for Medical Purposes Regulations (ACMPR), with the majority located in Ontario and British Columbia. The number of licensed producers nearly doubled since 2017.

The multiple stakeholders involved in large-scale licensed production may create some confusion and jurisdictional overlap in the early stages of implementation, which could leave the legitimate supply chain vulnerable to criminal infiltration. Although OCGs have dominated illegal large-scale cannabis production for many years, government-regulated production under the Cannabis Act now allows large corporate wholesale producers to supply cannabis for recreational use. The oversight of the cannabis supply chain is shared across federal, provincial, and territorial governments, municipalities, industry, and other stakeholders. Through the Cannabis Tracking and Licensing System (CTLS), Health Canada is responsible for tracking the movement of cannabis in order to prevent diversion from the regulated supply. Despite restrictions regarding licensing and regulations intended to secure licensed cultivation sites and prevent infiltration by organized crime, associates or nominees of several OCGs were believed to hold such licenses in 2017-2018. Moreover, the online sale of cannabis provides additional opportunities for criminal elements to fraudulently advertise illicit drug distribution websites as approved cannabis retail sites, and profit from consumers seeking convenient door-to-door delivery, those that are underage, and those who want to avoid face-to-face contact.

OCGs are undercutting the legitimate market price for cannabis in some jurisdictions, ensuring a continued illicit market share. The price of legal cannabis needs to ensure profitable tax revenue while also preventing the illicit market from undermining/destabilizing sales by offering significantly cheaper product. Provincial, territorial, and federal governments intend to keep duties low (10 percent of the product price, in addition to provincial taxes) to discourage contraband. However, if priced too low, it may encourage higher consumption rates, which present challenges to health care costs as well as to contributing to future supply shortfalls. According to some estimates, 63 percent of cannabis products are expected to be purchased through legal channels in Canada once licit cannabis supply meets demand. However, these estimates vary by province, and less than half (47 percent) of Quebec consumers are reported to be likely to shift into legal purchase channels leaving a significant percentage of Quebec consumers to sustain illicit cannabis markets in that region. In cases where legal cannabis proves to be more expensive than illicitly-sourced cannabis, or when legitimate supplies have run dry, consumers have reportedly been inclined to purchase their supply from illegal sources, driven by familiarity with the quality, price, and accessibility of their illicit source.

OCGs are likely to exploit variations in provincial legislation (see Figure 12), such as the limited accessibility of cannabis storefronts and the disparity between the legal age of consumption, to cater to consumers who feel underserved by the legal supply and to consumers, such as youth, who are excluded from legitimate sources. With the exception of Alberta and Quebec, where the legal age to purchase cannabis is 18 years, every province has deemed that the legal age for purchasing cannabis is 19 years. Although consumers over these ages now have a legitimate option to purchase cannabis products, underage consumers will continue to present a profitable consumer-base for OCGs. Moreover, some jurisdictions offer a limited number of centrally located storefronts, which leaves rural or remote areas underserved and provides lucrative opportunities to illicit suppliers. Some municipalities are moving to prohibit the sale of recreational cannabis entirely, which will remove much of the competition for illicit suppliers.

Figure 12 – Breakdown of Provincial Regulations



*There will be no brick and mortar stores in Ontario until 2019
*Quebec will potentially increase minimum age of consumption to 21

2018-19 NCIE ILLICIT DRUGS

The rapid appearance of illicit dispensaries on First Nations Territories across the country, similar to the development of "smoke shacks" for tobacco in Southern Ontario and Quebec, points to the illicitly-sourced cannabis market emulating the contraband tobacco market by exploiting the tax exemptions extended to Indian Status card-holders and cannabis businesses. Although the illicit tobacco market is primarily concentrated in Southern Ontario, there is a strong potential for this production and distribution trend in the illicit cannabis market to expand to a national scale, due to the fact there are little geographical constraints and growing limitations for manufacturing cannabis plants, unlike tobacco plants. In addition, there will be a sizable portion of cannabis consumers who are price-sensitive and will sustain a demand for cheaper, tax-free cannabis products, similar to what drove the growth of the illicit tobacco market, and illicit retailers will respond to this demand.

With a lack of regulatory framework and jurisdictional conflicts for law enforcement, some First Nations Territories will likely be infiltrated by OCGs to exploit the manufacture and distribution of illicit cannabis. Several Indigenous groups have expressed their right to self-determination to oversee their own manufacture, distribution, and sale of cannabis outside of federal and provincial jurisdiction.

Exploiting the Continued Illegality of Higher-Concentration THC Products

OCGs will continue to profit from the sizeable portion of consumers who will seek to purchase higher-concentration THC cannabis products that remain illegal under current legislation. The growing popularity around higher THC products, such as concentrates, will continue to drive black market sales ahead of plans to introduce them into the legal market in the latter half of 2019. Solvent-based cannabis concentrates, which are currently illegal, will continue to be produced in clandestine labs by criminal elements. The volatility of solvents, like butane, that are used in the production of these types of concentrates poses significant dangers to public safety and has led to serious injuries, death, fires, and explosions in residential areas where some labs have been located.

The demand for higher-concentration THC products – such as Tetrahydrocannabinolic Acid (THCA) Crystalline – is likely to drive product innovation in underground spheres. Because of its high market price, Canadian OCGs and criminal entrepreneurs may expand into this market and begin to experiment with manufacturing to create THCA or products with similar purity levels, as cannabis concentrates with high purity levels remain illegal in Canada. In such cases, law enforcement may begin to encounter illicit cannabis clan labs. However, given that the process to manufacture THCA requires the use of large equipment, several steps that can take a number of days, and substantial quantities of cannabis to yield the purest concentration of THCA in copious amounts, only a limited number of Canadian OCGs may expand into its manufacture. OCGs are more likely to develop distribution networks to introduce and disseminate this new product across the country.

Exploiting Continued International Demand

In the longer term, OCGs producing cannabis with established export routes may increase the amount of cannabis shipped outside Canada to countries where cannabis is illegal and has a higher value, particularly if production exceeds domestic demand or if domestic demand of illicitly-sourced product decreases following legalization. Such high profits may also attract other OCGs not currently involved in illicit cannabis, thereby expanding the market.

As regulatory loopholes are closed and opportunities to exploit the legitimate market are minimized, the trend toward transnational OCGs establishing networks and bases of operation in jurisdictions in which cannabis is legal, such as was reported in Colorado, U.S., may be mitigated in Canada by the prevalence of licensed producers and the availability of legal cannabis in all provinces and territories. One of the key points of exploitation of legalized marijuana in the U.S. centers on the number of states where cannabis remains illegal. Transnational groups that move into states where cannabis is legal to set up production sites benefit from selling to an existing illicit market within the U.S., avoiding the risks associated with international cross-border smuggling. The export of marijuana from Canada remains illegal, unless a special permit is obtained; cross-border interdictions and seizures still present a risk to OCGs and criminal entrepreneurs exporting marijuana to the U.S. and other countries.

Future Considerations

Reporting on OCG involvement in the cannabis market over the next year will be complicated by a general shift from policing to regulation, with cannabis now classified as a controlled, legal substance. With this shift, a significant drop in reporting is anticipated from the law enforcement community as members adapt to their new roles. Additionally, other enforcement priorities may take precedence, which may further result in underreporting of OCG involvement in the cannabis market, in order to accurately assess the impact of cannabis legalization. However, criminal involvement in the cannabis market will require continued monitoring and assessment in order to ensure compliance with the legal regime and minimize the threat of OCG infiltration and exploitation.

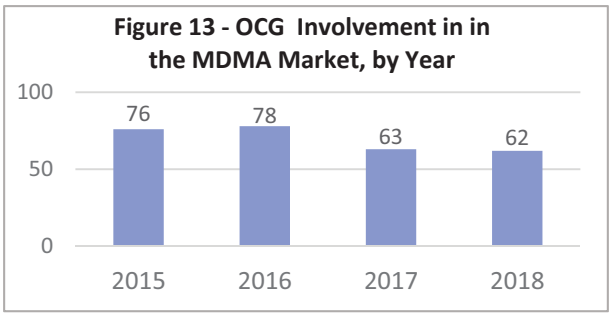
In the short term, OCGs will continue to fill the shortfall in the legitimate supply, try to undercut legal pricing, manufacture and traffic prohibited high-THC products, and increase exports to countries where cannabis remains illegal and more profitable. They are also likely to continue to sell cannabis illicitly via the dark web, exploit jurisdictional differences, fraudulently obtain cannabis licenses using nominees and proxies to produce and sell under the legal regime, and launder money through cannabis businesses they control. For those OCGs whose potential losses drive them away from the cannabis market, they are likely to continue to operate in the criminal marketplace in some other manner, given their propensity for already being involved in other drug markets.

In the longer term, if the regulatory framework surrounding cannabis is adjusted to prevent OCGs from exploiting vulnerabilities, it may result in a reduction in domestic illicit market share, although OCGs will continue to profit from the ensuing contraband cannabis market. If not, more OCGs may be attracted to the Canadian illicit cannabis market, opting to become involved in order to profit from higher demand for cannabis products, both domestically and internationally.

Other Illicit Drug Markets

MDMA

3,4-methylenedioxy-methamphetamine (MDMA) is a synthetic drug commonly known as "ecstasy" or "molly" which produces stimulant like and psychedelic effects. As a result MDMA is prominent in nightclubs and all night dance parties ("raves"). While MDMA is present across the country it remains a relatively small market and OCG involvement is on the decline (see Figure 13). Criminal groups are concentrated in British Columbia, Ontario and the Atlantic Provinces. Since the majority of these OCGs are involved in poly drug markets, MDMA is rarely the only drug being distributed. With the demand and profitability of other drugs, it is not anticipated this market will grow in the short-term.



MDMA is produced in Canada for both domestic consumption and for international distribution, primarily to the U.S. According to the DEA's 2018 National Drug Assessment, Canadian OCGs collaborate with U.S.-based Asian OCGs. There are also reports that Canadian OCGs will exchange MDMA for drugs like cocaine.

It is expected that Canadian OCGs will continue using precursors obtained domestically and internationally to produce MDMA and similar forms of it. For example, MDP2P is a common precursor chemical used in the production of MDMA. Despite increasing regulations on precursor chemicals, MDP2P and other MDMA precursors continue to make its way into Canada from China, Vietnam, and India.

Hydromorphone

Hydromorphone is the sixth controlled substance most often identified in Health Canada's DAS[6]. It is commonly sold under the brand name Dilaudid and is a semi-synthetic prescription opioid that is prescribed as a pain reliever that is five times more powerful than morphine. While hydromorphone is a pharmaceutical drug, it has become a popular street drug in some regions, mainly Saskatchewan, Quebec and Atlantic Canada, due to its high potency.

Canadian OCG involvement in hydromorphone is stable (approximately 16 assessed groups) with the majority of groups based in Atlantic Canada, where the user base is well-established and will likely continue to be in the medium- to long term. For example, OCGs in this region have successfully trafficked hydromorphone (e.g. Dilaudid) in Nova Scotia for the past decade without significant disruption. As such, this region continues to have a relatively stable supply of pharmaceutical opiates with users not likely to transition to alternative forms of opioids, including heroin or fentanyl. In Saskatchewan, the number of hydromorphone overdoses (83) have been approximately twice as high as the number of fentanyl-related deaths. Similarly, hydromorphone is the opioid most commonly identified in Quebec by Health Canada. However, the extent of OCG involvement in these provinces remains an intelligence gap.

Nonetheless, CISC does not consider this market to represent a significant threat and assesses OCG involvement to be minimal.

[6] See footnote on page 10.

New Psychoactive Substances

NPS are constantly evolving which presents new potential avenues for OCG and criminal entrepreneur involvement, as well as increased health and safety risks to users. NPS, also referred to as 'designer drugs' or 'legal highs', are synthetic substances that have been designed to mimic the effects of existing controlled substances. There are over 500 types of these substances and they are often unregulated and marketed as safe alternatives, counterfeited, contaminated or mixed into other substances without users` knowledge, which presents increased health risks to users. However, due to the diverse and quasi-legal nature of these substances they remain an intelligence gap.

The main source and transit countries for NPS are the Netherlands, China and Peru. However, these substances are difficult to detect and source as they are trafficked via the web (both dark and clear) and postal mode. Seizures are usually via postal (78 percent) and from the Netherlands (38 percent); potentially due to a large amount of dark web vendors operating in this country.

While NPS seizures have doubled in Canada from 2016 to 2017 and continue to increase in 2018, they remain low compared to other illicit drugs. The number of NPS seizures has increased 22 percent in 2018 in comparison to 2017 mid-year figures, and already exceeded 2017 year-end seizures. This increase in NPS could be explained by a lack of an illicit substance or precursor chemical for an illicit drug, more dealers targeting low income regions or users seeking less expensive non-scheduled alternative drugs that offer similar effects of illicit substances.

Dimethyltryptamine (DMT) and Harmaline accounted for the greatest proportion of sizeable NPS seizures in 2018, which suggests that these substances are being trafficked and may have OCG involvement. Most forms of NPS are seized in small quantities (averaging 16 grams or 22 doses) suggesting that they are predominantly used for personal consumption, rather than for trafficking purposes. Although there is a low number of seizures, the volume of these seizures exceeds the amount typically used for personal consumption suggesting that DMT and its additives are being trafficked into Canada.

Steroids

Steroids are generally prescribed to treat hormonal issues or to treat diseases that cause muscle loss, of which there are two types: corticosteroids and anabolic steroids. The most commonly abused steroids are anabolic. The muscle-building effects of these drugs make them appealing to athletes and bodybuilders. China is considered to be the world's main supplier for steroids, and the majority is imported into Canada via the postal mode. Law enforcement reporting on this market, however, is scant. While there has been a 33 percent increase in the number of OCGs (26 assessed groups) involved in this market between 2015 and 2018, the number of groups remains low. Most are poly-drug groups and steroids smuggling or trafficking is likely not their primary focus.

Ketamine

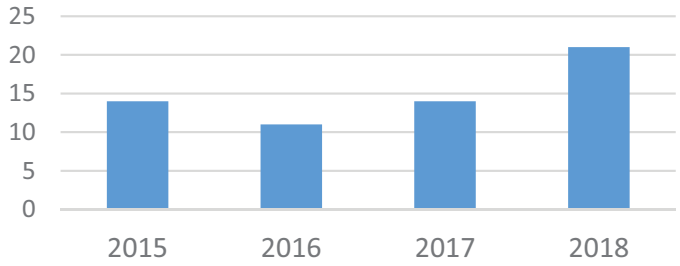
Ketamine, also known by street names Special K, Vitamin K, Ket, and Ketty is a fast-acting anesthetic and mind-altering drug which is used for medical purposes but also has become a popular recreational street drug. When sold illegally it often comes in a powder form that can be sniffed, smoked, dissolved into a liquid and injected, or mixed with a liquid and drunk. It may also be sold in tablet or capsule form.

There are currently 21 profiled OCGs involved in the ketamine market with most of these groups being concentrated in British Columbia, and to a lesser extent in Ontario and Quebec (See Figure 14). Notably, OCGs involved in this market within British Columbia have doubled over the past year with the number of reported groups increasing from 5 to 10. However, OCG involvement and the production of ketamine in clandestine labs remains an information gap due to law enforcement's focus on and targeting of larger drug markets such as fentanyl, cocaine and methamphetamine.

Most OCGs involved in ketamine are also involved in other illicit drug markets (e.g. methamphetamine, MDMA, cocaine, cannabis) and have numerous international and domestic connections.

Further information is required to accurately forecast the scale of this market. However, its reach, the degree of OCG involvement, seizure data and Health Canada reporting suggest that it poses a lesser threat than other illicit drug markets.

Figure 14 - OCG involvment in the Ketamine Market, by Year



GHB

Gamma hydroxybutyrate (GHB) acts as a depressant, slowing down activity of the nervous system. It is commonly referred to as the "date-rape drug" since the sedative component prevents victims from resisting the sexual assault. One trend that was reported was the use of GHB by methamphetamine users as a way to sleep following the alertness caused by the stimulant. Similarly, GHB is being increasingly seen as a "party" drug, which could present a health risk to users when mixing drugs and due to possible contamination from poly drug distributers. In 2018, there are only currently 18 assessed OCGs involved in the GHB market with most groups operating in Quebec, representing a slight increase from 2017. Nonetheless, this market is not assessed as a significant illicit drug market. Should OCG involvement become more pronounced and the threat increase in a measurable manner, separate standalone assessments or bulletins will be produced.

Opium

Opium is a highly addictive natural plant-based drug derived from the opium poppy plant and can be smoked, injected or taken in pill form. It was commonly used in Canada in the 1920s but is now supplanted by more potent opioids, such as morphine, heroin and fentanyl.

According to the UNODC, global opium supply increased by 65 percent from 2016 to 2017, primarily due to the rise in opium cultivation in Afghanistan. This growth will not impact the Canadian market, which does not represent a significant threat at this time. Opium's domestic user base, largely made up of diasporas based in British Columbia and Ontario, will remain relatively small, and it is unlikely that additional Canadian OCGs will shift to importing opium in the foreseeable future.

OCGs involved in importing opium are typically involved in importing heroin and rely on the same well-established transportation routes, modes and concealment methods. India is the main transit point for opium coming into Canada due to its proximity to major opium source countries, Afghanistan and Myanmar, and transit countries, Pakistan and Iran. Turkey is also a key opium transit point to Canada as it is located along the Balkan Route, which remains the most prominent opium and heroin trafficking route. The air cargo and postal modes are the venues most abused by OCGs to smuggle opium into Canada.