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

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

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.**

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.

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.

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.

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

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.

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

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.

(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.

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.**

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.

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.

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.

(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.

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."

- **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)."

> **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

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.

(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.

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.**

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).

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

"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

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*

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.