INTERNATIONAL MONETARY FUND

IMF Country Report No. 16/294

CANADA

DETAILED ASSESSMENT REPORT ON ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM

September 2016

This Detailed Assessment Report on Anti-Money Laundering and Combating the Financing of Terrorism for Canada was prepared by a staff team of the International Monetary Fund as background documentation for the periodic consultation with the member country. It is based on the information available at the time it was completed in August 2016.

Copies of this report are available to the public from

International Monetary Fund • Publication Services
PO Box 92780 • Washington, D.C. 20090
Telephone: (202) 623-7430 • Fax: (202) 623-7201
E-mail: publications@imf.org Web: http://www.imf.org
Price: $18.00 per printed copy

International Monetary Fund
Washington, D.C.

INTERNATIONAL MONETARY FUND

CANADA

DETAILED ASSESSMENT REPORT ON ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM

August 2016

Prepared By

Legal Department

This Detailed Assessment Report was prepared in the context of an IMF Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) assessment mission in Canada during November 3 to 20, 2015, led by Nadim Kyriakos-Saad, IMF and overseen by the Legal Department, IMF. Further information on the IMF's AML/CFT program can be found at:

[http://www.imf.org/external/np/exr/facts/aml.htm]

CONTENTS

Glossary

AMF	Autorité des Marchés Financiers
AML/CFT	Anti-Money Laundering and Combating the Financing of Terrorism
BC	British Columbia
CBCR	Cross-Border Currency Report
CBSA	Canada Border Services Agency
CDR	Casino Disbursement Report
CDSA	Controlled Drugs and Substances Act
CRA	Canada Revenue Agency
CRA-CID	Canada Revenue Agency—Criminal Investigations Directorate
CSIS	Canadian Security Intelligence Service
DAR	Detailed Assessment Report
DOJ	Department of Justice
DPMS	Dealers in precious metals and stones
DPRK	Democratic People's Republic of Korea
DNFBP	Designated Non-Financial Businesses and Professions
D-SIB	Domestic Systematically Important Bank
EFTR	Electronic Funds Transfer Report
FATF	Financial Action Task Force
FI	Financial Institution
FINTRAC	Financial Transactions and Reports Analysis Centre of Canada
FIU	Financial Intelligence Unit
FRFI	Federally Regulated Financial Institution
GAC	Global Affairs Canada
IAG	International Assistance Group
ICC	Interdepartmental Coordinating Committee on Listings
IMF	International Monetary Fund
IO	Immediate Outcome
IPOC	Integrated Proceeds of Crime Initiative

ISEDC	Innovation, Science and Economic Development Canada (former Industry Canada)
LCTR	Large Cash Transaction Report
LEA	Law Enforcement Agency
MSB	Money Service Business
ML	Money Laundering
MLA	Mutual Legal Assistance
NPO	Non-Profit Organization
NRA	National Risk Assessment
OPC	Office of the Privacy Commissioner
OSFI	Office of the Superintendent of Financial Institutions
PCMLTFA	Proceeds of Crime (Money Laundering) and Terrorist Financing Act
PCMLTFR	Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations
PEFP	Politically Exposed Foreign Persons
PEP	Politically Exposed Person
PF	Proliferation Financing
PIPEDA	Personal Information Protection and Electronic Documents Act
POC	Proceeds of Crime
PPSC	Public Prosecution Service of Canada
PS	Public Safety Canada (former Public Safety and Emergency Preparedness)
PSPC	Public Services and Procurement Canada (former Public Works and Government Services Canada)
RBA	Risk-Based Approach
RCMP	Royal Canadian Mounted Police
RE	Reporting Entity
RIUNRST	Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism
STR	Suspicious Transaction Report
TCSP	Trust and Company Services Providers
TF	Terrorist Financing

TFS	Targeted Financial Sanctions
UNSCR	United Nations Security Council Resolution
UNAQTR	United Nations Al-Qaida and Taliban Regulations
US	United States of America
VIR	Voluntary Information Record

EXECUTIVE SUMMARY

This report provides a summary of the anti-money laundering and combating the financing of terrorism (AML/CFT) measures in place in Canada as at the date of the onsite visit (November 3 to 20, 2015). It analyzes the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Canada's AML/CFT system, and provides recommendations on how the system could be strengthened.

KEY FINDINGS

1. The Canadian authorities have a good understanding of most of Canada's money laundering and terrorist financing (ML/TF) risks. The 2015 Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada (the NRA) is of good quality. AML/CFT cooperation and coordination are generally good at the policy and operational levels.

2. All high-risk areas are covered by AML/CFT measures, except legal counsels, legal firms, and Quebec notaries. This constitutes a significant loophole in Canada's AML/CFT framework.

3. Financial intelligence and other relevant information are accessed by Canada's financial intelligence unit, FINTRAC, to some extent and by law enforcement agencies (LEAs) to a greater extent, but through a much lengthier process. They are used to some extent to investigate predicate crimes and TF activities, and, to a much more limited extent, to pursue ML.

4. FINTRAC receives a wide range of information, which it uses adequately, but some factors, in particular the fact that it is not authorized to request additional information from any reporting entity (RE), limit the scope and depth of the analysis that it is authorized to conduct.

5. Law enforcement results are not commensurate with the ML risk and asset recovery is low.

6. Canada accords priority to pursuing TF activities. TF-related targeted financial sanctions (TFS) are adequately implemented by financial institutions (FIs) but not by designated nonfinancial business and professions (DNFBPs). Charities (i.e., registered NPOs) are monitored on a risk basis.

7. Canada's Iran and Democratic People's Republic of Korea (DPRK) sanction regime is comprehensive, and some success has been achieved in freezing funds of designated individuals, there is no mechanism to monitor compliance with PF-related TFS.

8. FIs, including the six domestic systemically important banks, have a good understanding of their risks and obligations, and generally apply adequate mitigating measures. The same is not true for DNFBPs. REs have gradually increased their reporting of suspicious transactions, but reporting by DNFBPs other than casinos is very low.

9. FIs and DNFBPs are generally subject to appropriate risk-sensitive AML/CFT supervision, but supervision of the real estate and dealers in precious metals and stones (DPMS) sectors is not

entirely commensurate to the risks in those sectors. A range of supervisory tools are used effectively especially in the financial sector. There is some duplication of effort between FINTRAC and the Office of the Superintendent of Financial Institutions (OSFI) in the supervisory coverage of federally regulated financial institutions (FRFIs) and a need to coordinate resources and expertise more effectively.

10. Legal persons and arrangements are at a high risk of misuse, and that risk is not mitigated.

11. Canada generally provides useful mutual legal assistance and extradition. The authorities solicit other countries' assistance to fight TF and, to a somewhat lesser extent, ML. Informal cooperation is generally effective and frequently used.

Risks and General Situation

12. Canada has a strong framework to fight ML and TF, which relies on a comprehensive set of laws and regulations, as well as a range of competent authorities.

13. It faces an important domestic and foreign ML threat, and lower TF threat. As acknowledged in the public version of the authorities' 2015 assessment of Canada's inherent ML and TF risks (the NRA), the main domestic sources of proceeds of crime (POC) are fraud, corruption and bribery, counterfeiting and piracy, illicit drug trafficking, tobacco smuggling and trafficking, as well as (to a slightly higher level than assessed) tax evasion. Canada's open and stable economy and accessible financial system also make it vulnerable to significant foreign ML threats, especially originating from the neighboring United States of America (U.S.), but also from other jurisdictions. The main channels to launder the POC appear to be the financial institutions (FIs), in particular the six domestic systemically important banks (D-SIBs) due to their size and exposure, as well as money service businesses (MSBs). While not insignificant, the TF threat to Canada appears lower than the ML threat. A number of TF methods have been used in Canada and have involved both financial and material support to terrorism, including the payment of travel expenses of individuals and the procurement of goods.

Overall Level of Effectiveness and Technical Compliance

14. Since its 2007 evaluation, Canada has made significant progress in bringing its AML/CFT legal and institutional framework in line with the standard, but the fact that AML/CFT obligations are inoperative for legal counsels, legal firms and Quebec notaries is a significant concern. In terms of effectiveness, Canada achieves substantial results with respect to five of the Immediate Outcomes (IO), moderate results with respect to five IOs, and low results with respect to one IO.

Assessment of Risks, Coordination and Policy Setting (Chapter 2—IO.1; R.1, R.2, R.33)

15. The authorities have a generally good level of understanding of Canada's main ML/TF risks. The public version of the 2015 NRA is of good quality. It is based on dependable evidence and sound judgment, and supported by a convincing rationale. In many respects, the NRA confirmed the authorities' overall understanding of the sectors, activities, services and products exposed to ML/TF

risk. While the NRA's findings did not contain major unexpected revelations, the process was useful in clarifying the magnitude of the threat, in particular the threat affecting the real estate sector and emanating from third-party money launderers. The authorities nevertheless may be underestimating the magnitude of some key risks, such as the risk emanating from tax crimes and foreign corruption.

16. All high-risk areas are covered by the AML/CFT regime, with the notable exception of the legal professions other than British Columbia (BC) notaries, which is a significant loophole in Canada's AML/CFT framework, and online casinos, open loop prepaid cards, and white label ATMs.

17. While supervisory measures are generally in line with the main ML/TF risks, more intensive supervisory measures should be applied in some higher risk areas such as the real estate and DPMS.

18. AML/CFT cooperation and coordination appear effective at the policy level, but in some provinces, greater dialogue between LEAs and the Public Prosecution Service of Canada (PPSC) would prove useful.

19. While FIs generally appear adequately aware of their ML/TF risks, the same does not apply in some DNFBP sectors, in particular the real estate sector.

Financial Intelligence, Money Laundering and Confiscation (Chapter 3—IOs 6–8; R.3, R.4, R.29–32)

20. Financial intelligence and other relevant information is collected and used to some extent only by competent authorities to carry out investigations into the predicate crimes and TF activities, and, to a more limited extent, to pursue ML. FINTRAC receives a range of information from REs and LEAs, which it adequately analyzes. Some factors nevertheless hamper its ability to produce more comprehensive intelligence products, in particular, the fact that FINTRAC is not authorized to obtain from any RE additional information related to suspicions of ML/TF. FINTRAC's analysis and disclosures are mainly prepared in response to the requests made by LEAs in Voluntary Information Records (VIRs). LEAs use these disclosures mainly to investigate the predicate offense, rather than to carry out ML investigations. FINTRAC also produces strategic reports that address the LEAs' operational priorities and advise them on new ML/TF trends and typologies. Information resulting from cross-border transportation of cash and other bearer negotiable instruments is not exploited to its full extent. The FIU and the LEAs cooperate effectively and exchange information and financial intelligence on a regular basis and in a secure way.

21. LEAs have adequate powers and cooperation mechanisms to undertake large and complex financial investigations. This has notably resulted in some high-profile successes in neutralizing ML networks and syndicates. However, current efforts are mainly aimed at the predicate offenses, with inadequate focus on the main ML risks other than those emanating from drug offenses, i.e., standalone ML, third-party ML and laundering of proceeds generated abroad. Some provinces, such as Quebec, appear more effective in this respect. LEAs' prioritization processes are not fully in line with the findings of the NRA, and LEAs generally suffer from insufficient resources and expertise to pursue complex ML cases. In addition, legal persons are not effectively pursued and sanctioned for

ML, despite their misuse having been identified in the NRA as a common ML typology. Criminal sanctions applied are not sufficiently dissuasive. The majority of natural persons convicted for ML are sentenced in the lower range of one month to two years of imprisonment, even in cases involving professional money launderers.

22. Overall, asset recovery appears low. Some provinces, such as Quebec, appear more effective in recovering assets linked to crime. Falsely and undeclared cross-border movements of currency and other bearer negotiable instruments are rarely analyzed by the FIU or investigated by the RCMP. As a result, the majority of the cash seized by the Canada Border Services Agency (CBSA) is returned to the traveler at the border.

Terrorist Financing and Financing Proliferation (Chapter 4—IOs 9–11; R.5–8)

23. The authorities display a good understanding of Canada's TF risk and cooperate effectively in CFT efforts. The intelligence services, LEAs and FINTRAC regularly exchange information, which notably contributes to support prioritization of TF investigations. Canada accords priority to investigations and prosecutions of terrorism and TF. There are a number of TF investigations, which resulted in two TF convictions. Canada also makes regular use of other disruption measures.

24. Implementation of TF-related targeted financial sanctions (TFS) is generally good but uneven. Large FIs implement sanctions without delay, but DNFBPs do not seem to have a good understanding of their obligations and are not required to conduct a full search of their customer databases on a regular basis. In practice, few assets have been frozen in connection with TF-related TFS, which does not seem unreasonable in the Canadian context.

25. Charities (i.e., registered NPOs) are monitored by the Canada Revenue Agency (CRA) on a risk basis, but the number of inspections conducted over the last few years does not reflect those TF risks. The NRA found the risk of misuse of charities as high, but only a small percentage of charities have been inspected. Nevertheless, to limit this risk, the CRA's charities division has developed an enhanced outreach plan which reflects the best practices put forward by the FATF.

26. Canada's framework to implement the relevant UN counter-proliferation financing sanctions is strong and, in some respect, goes beyond the standard, but does not apply to all types of assets listed in the standard. The current lists of designated persons are available on the OSFI websites, and changes to those lists are promptly brought to the attention of the FRFIs (i.e., banks, insurance companies, trust and loan companies, private pension plans, cooperative credit associations, and fraternal benefit societies). There is a good level of policy and operational cooperation between the relevant authorities including those involved in export control, border control, law enforcement and AML/CFT supervision. Some success has been achieved in freezing funds of designated persons. None of the Canadian authorities has an explicit mandate to monitor FIs' and DNFBPs' implementation of their counter-PF obligations but, in practice, OSFI has examined implementation by FRFIs of TFS for both TF and PF, and has also identified shortcomings and requested improvements.

Preventive Measures (Chapter 5—IO.4; R.9–23)

27. AML/CFT requirements are inoperative towards legal counsels, legal firms and Quebec notaries. These requirements were found to breach the constitutional right to attorney-client privilege by the Supreme Court of Canada on February 13, 2015. In light of these professionals' key gatekeeper role, in particular in high-risk sectors and activities such as real-estate transactions and the formation of corporations and trusts, this constitutes a serious impediment to Canada's efforts to fight ML.

28. FRFIs, including the six domestic banks that dominate the financial sector, have a good understanding of their risks and AML/CFT obligations. Supervisory findings on the implementation of the risk-based approach (RBA) are also generally positive. The large FRFIs conducted comprehensive group-wide risk assessments and took corresponding mitigating measures. In an effort to mitigate some of the higher risks, a number of FRFIs have gone beyond the Canadian requirements (e.g., by collecting information on the quality of AML/CFT supervision in the respondent bank's country).

29. Nevertheless, some deficiencies in the AML/CFT obligations undermine the effective detection of very high-risk threats identified in the NRA, such as corruption. This is notably the case of the current requirements related to politically exposed persons (PEPs). The identification of beneficial ownership also raises important concerns. Although the legal requirements have recently been strengthened, little is done by FIs to verify the accuracy of beneficial ownership information. DNFBPs are not required to identify the beneficial ownership nor to take specific measures with respect to foreign PEPs.

30. Most DNFBPs are not sufficiently aware of their AML/CFT obligations. This is in particular the case of real estate agents. Extensive work has been conducted by FINTRAC with relevant DPMS trade associations, to increase the DNFBPs' awareness, which is leading to some improvement in compliance. REs have gradually increased the number of STRs and other threshold-based reports filed with FINTRAC but reporting remains very low. The fact that no STRs have been filed by accountants and BC notaries, and the low number of STRs received from the real estate sector raise concern.

Supervision (Chapter 6—IO.3; R.26–28, R.34–35)

31. FINTRAC and OSFI supervise FIs and DNFBPs on a risk-sensitive basis. FINTRAC should, however, apply more intensive supervisory measures to DNFBPs. There is good supervisory coverage of FRFIs, but FINTRAC and OSFI need to improve their coordination to share expertise, maximize the use of the supervisory resources available and avoid duplication of efforts. FINTRAC has increased its supervisory capacity in recent years. It adopted an effective RBA in its compliance and enforcement program, but needs to further develop its sector-specific expertise and increase the intensity of supervision of DNFBPs, particularly in the real estate sector and with respect to DPMS, commensurate with the risks identified in the NRA.

32. There are good market entry controls in place to prevent criminals and their associates from owning or controlling FIs and most DNFBPs. There are, however, no controls for DPMS, and fitness and probity controls at the provincial level are not conducted on an ongoing basis (i.e., including after-market entry).

33. Supervisors appear generally effective. Remedial actions are effectively used and have been extensively applied by supervisors but the sanctioning regime for breaches of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (the PCMLTFA) has not been applied in a proportionate and/or sufficiently dissuasive manner. Supervisors have demonstrated that their actions have largely had a positive effect on compliance by FIs and some categories of DNFBPs. They have increased guidance and feedback to REs in recent years but further efforts are necessary, particularly with regard to the DNFBP sector. The exclusion of most of the legal professions (legal counsels, legal firms, and Quebec notaries) from AML/CFT supervision has a negative impact on the effectiveness of the supervisory regime as a whole.

Transparency of Legal Persons and Arrangements (Chapter 7—IO.5; R.24–25)

34. Canadian legal entities and legal arrangements are at a high risk of misuse for ML/TF purposes and that risk is not mitigated. This is notably the case with respect to nominee shareholding arrangements, which are commonly used across Canada and pose real obstacles for LEAs.

35. Basic information on legal persons is publicly available, but beneficial ownership information is more difficult to obtain. Some information is collected by FIs and to a limited extent DNFBPs, the tax authorities and legal entities themselves, but is neither verified nor comprehensive in all cases. LEAs have the necessary powers to obtain that information, but the process is lengthy. Information exchange between LEAs and the CRA is also limited by stringent legal requirements.

36. The authorities have insufficient access to information related to trusts. Some information is collected by the CRA as well as by FIs providing financial services, but that information is not verified, does not always pertain to the beneficial owner, and is even more difficult to obtain than in the case of legal entities.

37. LEAs have successfully identified the beneficial owners in limited instances only. Despite corporate vehicles and trusts posing a major ML and TF risk in Canada, LEAs do not investigate many cases in which legal entities or trusts played a prominent role or that involved complex corporate elements or foreign ownership or control aspects.

International Cooperation (Chapter 8—IO.2; R.36–40)

38. The range of mutual legal assistance (MLA) provided by Canada is generally broad, and countries provided—through the FATF—largely positive feedback regarding the responsiveness and quality of the assistance provided. Canada solicits other countries' assistance in relatively few instances in pursuit of domestic ML, associated predicate offenses and TF cases with transnational

elements. Some concerns were nevertheless raised by some Canadian LEAs about delays in the processing of incoming and outgoing requests. The extradition framework is adequately implemented. Informal cooperation is effective. Cooperation between LEAs, FINTRAC, the CBSA and OSFI and their respective foreign counterparts is more fluid, and more frequently used than MLA. Nevertheless, some weaknesses in Canada's framework (e.g., the impossibility for FINTRAC to obtain additional information from REs, and the low quantity of STRs from DNFBPs) negatively affects the authorities' ability to assist their foreign counterparts.

Priority Actions

- Ensure that legal counsels, legal firms, and Quebec notaries engaged in the activities listed in the standard are subject to AML/CFT obligations and supervision. Bring all remaining FIs and DNFBPs in the AML/CFT regime.
- Increase timeliness of access by competent authorities to accurate and up-to-date beneficial ownership information—consider additional measures to supplement the current framework.
- Increase timely access to financial intelligence—authorize FINTRAC to request and obtain from any RE further information related to suspicions of ML, predicate offenses and TF.
- Use financial intelligence to a greater extent to investigate ML and trace assets.
- Increase efforts to detect, pursue, and bring before the courts cases of ML related to all high-risk predicate offenses, third party ML, self-laundering, laundering of POC of foreign predicates, and the misuse of legal persons and trusts in ML activities.
- Ensure that asset recovery is pursued as a policy objective throughout the territory.
- Ensure compliance by all FIs with the requirement to confirm the accuracy of beneficial ownership in relation to all customers.
- Require DNFBPs to identify and verify the identity of beneficial owners and PEPs.
- Coordinate more effectively supervision of FRFIs by OSFI and FINTRAC to maximize the use of resource and expertise, and review implementation of the current approach.
- Ensure that FINTRAC develops sector-specific expertise, and applies more intensive supervisory measures to the real estate and the DPMS sectors.

Effectiveness and Technical Compliance Ratings

Effectiveness Ratings

IO.1 Risk, policy and coordination	**IO.2** International cooperation	**IO.3** Supervision	**IO.4** Preventive measures	**IO.5** Legal persons and arrangements	**IO.6** Financial intelligence
Sub.	**Sub.**	**Sub.**	**Mod.**	**Low**	**Mod.**
IO.7 ML investigation and prosecution	**IO.8** Confiscation	**IO.9** TF investigation and prosecution	**IO.10** TF preventive measures and financial sanctions	**IO.11** PF financial sanctions	
Mod.	**Mod.**	**Sub.**	**Sub.**	**Mod.**	

Technical Compliance Ratings

AML/CFT Policies and Coordination

R.1	R.2
LC	**C**

Money Laundering and Confiscation

R.3	R.4
C	**LC**

Terrorist Financing and Financing of Proliferation

R.5	R.6	R.7	R.8
LC	**LC**	**LC**	**C**

Preventive Measures

R.9	R.10	R.11	R.12	R.13	R.14
C	LC	LC	NC	LC	C
R.15	R.16	R.17	R.18	R.19	R.20
NC	PC	PC	LC	C	PC
R.21	R.22	R.23			
LC	NC	NC			

Transparency and Beneficial Ownership of Legal Persons and Arrangements

R.24	R.25
PC	NC

Powers and Responsibilities of Competent Authorities and other Institutional Measures

R.26	R.27	R.28	R.29	R.30	R.31
LC	C	PC	PC	C	LC
R.32	R.33	R.34	R.35		
LC	C	LC	LC		

International Cooperation

R.36	R.37	R.38	R.39	R.40
C	LC	LC	C	LC

DETAILED ASSESSMENT REPORT

Preface

This report provides a summary of the anti-money laundering and combating the financing of terrorism (AML/CFT) measures in Canada as at the date of the onsite visit. It analyzes the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Canada's AML/CFT system, and provides recommendations on how the system could be strengthened.

This evaluation was based on the 2012 FATF Recommendations, and was prepared using the 2013 Methodology as updated at the time of the onsite. The evaluation was based on information provided by Canada, and information obtained by the evaluation team during its onsite visit to Canada from November 3 to 20, 2015.

The evaluation was conducted by an assessment team consisting of: Nadim Kyriakos-Saad (team leader), Nadine Schwarz (deputy team leader), Antonio Hyman-Bouchereau (legal expert, IMF), Katia Bucaioni (financial sector expert, Unità di Informazione Finanziaria, Italy), Anthony Cahalan (financial sector expert, Central Bank of Ireland), Carla De Carli (legal expert, Regional Circuit Prosecution, Brazil), Gabriele Dunker (IMF consultant), John Ellis (IMF consultant), Sylvie Jaubert (law enforcement expert, Directorate of Intelligence and Customs Investigations, France), Amy Lam (law enforcement expert, Hong Kong Police). The report was reviewed by Emery Kobor (U.S.), Erin Lubowicz (New Zealand), Peter Smit (South Africa), Richard Berkhout (FATF Secretariat), and Lindsay Chan (Asia Pacific Group on Money Laundering—APG secretariat).

Canada previously underwent a FATF mutual evaluation in 2007, conducted according to the 2004 FATF Methodology. That evaluation concluded that Canada was compliant with 7 Recommendations; largely compliant with 23; partially compliant with 8; and non-compliant with 11. Canada was rated compliant or largely compliant with 13 of the 16 Core and Key Recommendations. Canada was placed in the regular follow-up process, and reported back to the FATF in February 2009, February 2011, October 2011, October 2012, and February 2013. The FATF February 2014 follow-up report found that overall, while some minor deficiencies remained, Canada had made sufficient progress with respect to the Core and Key Recommendations. Canada was therefore removed from the follow-up process in February 2014.

The 2008 mutual evaluation report (MER) and February 2014 follow-up report have been published and are available at http://www.fatf-gafi.org/countries/#Canada.

ML/TF RISKS AND CONTEXT

39. Canada extends from the Atlantic to the Pacific and northward into the Arctic Ocean, covering 9.98 million square kilometers (3.85 million square miles) in total, making it the world's second-largest country by total area (i.e., the sum of land and water areas) and the fourth-largest country by land area. Canada is a developed country and the world's eleventh-largest economy as of 2015 (approximately US$1.573 trillion). As of 2015, the population of Canada is estimated to be 35,851,774. The foreign-born population of Canada represented 20.6 percent of the total population in 2011, the highest proportion among the G7 countries.[1]

40. Canada is a federation of ten provinces and three territories[2] in the northern part of North America. Ottawa, in the province of Ontario, is the national capital. Canada is a federal parliamentary democracy and a constitutional monarchy, with her Majesty Queen Elizabeth II being the Head of State. The Governor General of Canada carries out most of the federal royal duties in Canada as representative of the Canadian crown.

41. Canada's Constitution consists of unwritten and written acts, customs, judicial decisions, and traditions dating from 1763. The composition of the Constitution of Canada is defined in subsection 52(2) of the Constitution Act, 1982 as consisting of the Canada Act 1982 (including the Constitution Act, 1982), all acts and orders referred to in the schedule (including the Constitution Act, 1867 and the Charter of Rights and Freedoms), and any amendments to these documents.

42. All provinces and territories within Canada follow the common law legal tradition, except Quebec, which follows the civil law tradition. In addition, all federal laws also follow the common law legal tradition and are applicable in every province and territory (Quebec's civil tradition only applies to provincial laws).

A. ML/TF Risks and Scoping of Higher-Risk Issues

Overview of ML/TF Risks

43. Canada faces important ML risks generated both domestically and abroad. Estimates of the total amount of POC generated and/or laundered in Canada vary: the Criminal Intelligence Service Canada (CISC) estimated in 2007 that POC generated annually by predicate crimes committed in Canada represent approximately three to five percent of Canada's nominal gross domestic product (GDP), or approximately US$47 billion. The RCMP estimated in 2011 that the amount of money laundered annually in Canada to be somewhere between US$5 billion and US$15 billion. The NRA

[1] *Immigration and Ethnocultural Diversity in Canada—National Household Survey, 2011,* Statistics Canada (2011). See https://www12.statcan.gc.ca/nhs-enm/2011/as-sa/99-010-x/99-010-x2011001-eng.cfm.

[2] The 10 provinces are Alberta, British Columbia, Manitoba, New Brunswick, Newfoundland and Labrador, Nova Scotia, Ontario, Prince Edward Island, Quebec, and Saskatchewan. The three territories are Northwest Territories, Nunavut, and Yukon.

indicates that profit-generating criminal activity generates billions of dollars in POC that might be laundered.

44. Organized Criminal Groups (OCGs) pose the greatest domestic ML risk, as they are involved in multiple criminal activities generating large amounts of POC. There are over 650 OCGs operating in Canada. The public version of the NRA does not include a detailed analysis of the risks associated with the methods and financial channels used to raise, collect or transfer funds for TF, due to reasons of national security. The classified version of the NRA includes specific ratings for the TF risks represented by each of the terrorist groups. However, this could not be shared and therefore not assessed by the assessors due to national security concerns.

45. Canada appears to be moderately exposed to PF risks, due primarily to the size of the Canadian financial sector. Canada produces a range of controlled military and dual-use goods, and while no estimates were provided regarding the value and volume of goods exported, they are understood to be relatively large. In addition, Canada appears vulnerable to being used as a transshipment or transit point for military controlled and dual-use goods produced in the U.S. There are no estimates of the financial flows between Canada and either Iran or the DPRK, but, due to the number of restrictions in place (see R.7 and IO.11), are understood to be low.

ML/TF Threats

46. POCs in Canada are mainly generated from: human smuggling, payment card fraud, tobacco smuggling and trafficking, mass marketing fraud, mortgage fraud, capital markets fraud, illicit drug trafficking, counterfeiting and piracy, corruption and bribery, and commercial trade fraud. Canada is exposed to very high ML threats of both local and foreign origin: (i) Fraud, including capital markets fraud, trade fraud, mass marketing fraud, and mortgage fraud, is a major source of POC in Canada. (ii) The proceeds of drug trafficking laundered in Canada are also significant, and derive predominantly from domestic activity controlled by OCGs. (iii) Third-party ML has started to pose a significant threat in recent years. The NRA found, and discussions onsite confirmed that large-scale and sophisticated ML operations in Canada, notably those connected to transnational OCGs, frequently involve professional money launderers[3] (i.e., individuals specialized in the ML of POC who offer their services for a fee), nominees or money mules. It also found that, of the three, professional money launderers pose the greatest threat both in terms of laundering domestically generated POC as well as laundering, through Canada, of POC generated abroad.[4]

47. The threat emanating from other countries is significant but less easily definable. While some countries have been identified as being the main source of POC laundered in Canada, the

[3] It is suspected that criminally-inclined real estate professionals, notably real estate lawyers, are used to facilitate ML. OCGs involved in mortgage fraud appear to launder funds through banks, MSBs, legitimate businesses and trust accounts.

[4] Public version of the NRA, p.22.

authorities' assessment of the foreign ML threat is less detailed and comprehensive than their analysis of the domestic threat.

48. The TF threat was assessed in relation to the terrorist organizations and associated individuals that have financing or support networks in Canada. In particular, the TF threat posed by the actors associated with the following 10 terrorist groups and foreign fighters was assessed: Al Qaeda in the Arabian Peninsula; Al Qaeda Core; Al Qaeda in the Islamic Maghreb; Al Shabaab; Hamas; Foreign Fighters/Extremist Travellers; Hizballah; Islamic State of Iraq and Syria; Jabhat Al-Nusra; Khalistani Extremist Groups; and Remnants of the Liberation Tigers of Tamil Eelam. Using rating criteria and currently available intelligence, the terrorist groups were assessed as posing a low, medium or high TF threat in Canada. The sectors and products exposed to very high TF risks are corporations, domestic banks, national full-service MSBs, small family-owned MSBs and express trusts. The NRA indicates the possible existence of TF networks in Canada suspected of raising, collecting and transmitting funds abroad to various terrorist groups.[5] The only domestically listed terrorist organizations that pose a TF threat to Canada are those that have financing or support networks in Canada.[6] Terrorism and TF have been increasing in the last two years and more resources were therefore shifted by the authorities to address these threats. As resources remain limited, these issues are putting additional pressures on the AML/CFT regime, and in particular LEAs. Additional funding for AML/CFT activities was authorized in Budget 2015, but these new resources have yet to be fully deployed.

Vulnerabilities

49. Canadian banks offer a number of inherently vulnerable products and services to a very large client base, which includes a significant amount of high-risk clients and businesses. In addition, banks are exposed to high-risk jurisdictions that have weak AML/CFT regimes and significant ML/TF threats. The main channels to launder the POC appear to be the FIs, in particular the D-SIBs due to their size and exposure, as well as MSBs. Terrorist financiers mostly use international and domestic wire transfers to move funds within Canada and/or abroad.

50. The legal profession in Canada is especially vulnerable to misuse for ML/TF risks, notably due to its involvement in activities exposed to a high ML/TF risk (e.g., real estate transactions, creating legal persons and arrangements, or operation of trust accounts on behalf of clients).[7]

[5] The TF methods that have been used in Canada include both financial and material support for terrorism, such as the payment of travel expenses and the procurement of goods. The transfer of suspected terrorist funds to foreign locations has been conducted through a number of methods including the use of MSBs, banks and NPOs as well as smuggling bulk cash across borders.

[6] Organizations posing a terrorist threat to Canada do not necessarily pose a TF threat to Canada. In such cases, the level of threat may not be the same.

[7] The use of trust accounts by lawyers has been recognized by the Department of Finance as a high vulnerability. See "Follow the Money: Is Canada Making Progress in Combatting Money Laundering and Terrorist Financing? Not really," Report of the Standing Senate Committee on Banking, Trade and Commerce, 2013, page A-26-Lawyers and legal firms. See www.parl.gc.ca/Content/SEN/Committee/411/BANC/rep/rep10mar13-e.pdf.

Following a February 13, 2015 Supreme Court of Canada ruling, legal counsels, legal firms, and Quebec notaries are not required to implement AML/CFT measures,[8] which, in light of the risks, raises serious concerns.

51. Businesses that handle high volumes of cash are highly vulnerable to ML/TF as they are attractive to launderers of drug proceeds. These include brick and mortar casinos, convenience stores, gas stations, bars, restaurants, food-related wholesalers and retailers, and DPMS (notably in the diamonds sector).[9]

52. The real estate sector is highly vulnerable to ML, including international ML activities, and the risk is not fully mitigated, notably because legal counsels, legal firms and Quebec notaries (who provide services in related financial transactions) are not required to implement AML. The sector provides products and services that are vulnerable to ML and TF, including the development of land, the construction of new buildings and their subsequent sale. Also, the real estate business is exposed to high-risk clients, including PEPs, notably from Asia[10] and foreign investors (including from locations of concern).

53. Other activities, such as the mining of diamonds, dealing in high value goods, virtual currencies and open loop prepaid cards, are subject to higher ML/TF vulnerability.[11][12] The NRA classifies the virtual currency sector as having high vulnerability, in particular convertible virtual currencies due to the increased anonymity that they can provide as well as their ease of access and high degree of transferability. White-label automated teller machine (ATM) operators are vulnerable to ML/TF. According to the RCMP, OCGs use white-label ATMs to launder POC in Canada. The money withdrawn has previously been deposed into a bank accounts controlled by OCGs through third parties.

54. Legal persons and legal arrangements are inherently vulnerable to misuse for ML/TF purposes to a high degree. There is no legal requirement for legal persons and entities to record and maintain beneficial ownership information. Accordingly, companies and trusts can be structured to conceal the beneficial owner and can be used to disguise and convert illicit proceeds. Privately-

[8] See Canada (Attorney General) v. Federation of law societies of Canada, 2015 SCC 7. See https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/14639/index.do.

[9] Ibid. p.63.

[10] For example, there are cases of Chinese officials laundering the PoC through the real estate sector, particularly in Vancouver, and the Chinese government has listed Canada as a country that it wishes to target for recovering the proceeds of Chinese corruption. Canada may be particularly vulnerable to such laundering, as there is no extradition treaty with China.

[11] See "ML and TF through Trade in Diamonds," FATF Report, October 2013 (p. 30 and 41): http://www.fatf-gafi.org/media/fatf/documents/reports/ML-TF-through-trade-in-diamonds.pdf.

[12] See "Developing a ML/TF Risk Assessment Framework for Canada," updated by the Public-Private Sector Advisory Committee (PPSAC) in May 2014. In this regard, AML/CFT requirements have not been extended to the other sectors (i.e., luxury goods, automobile, antiquities) when they engage in any cash transaction with a customer equal to or above a designated threshold.

held corporate entities can also be established relatively anonymously in Canada. Express trusts have global reach; Canadians and non-residents can establish Canadian trusts in Canada or abroad.

55. Full-service MSBs are vulnerable to ML/TF as they are widely accessible and exposed to clients in vulnerable businesses or occupations, and clients conducting activities in locations of concern. Drug traffickers are particularly frequent users of MSBs.[13]

International Dimension of ML/TF Vulnerabilities

56. Some of Canada's key attributes (e.g., political and economic stability, well-developed international trade networks, cultural environment, and highly developed financial system and regulatory environment)[14] also make it attractive to those seeking to launder money or finance terrorism. Canada's appeal as an investment setting also makes it an attractive destination for foreign POC.

57. Canada and the U.S. share the longest international border in the world, at over 8,800 kilometers. Some passages are unguarded and provide opportunity for criminals to move easily between both countries. OCGs in Canada and the U.S. actively exploit the border for criminal gain. Both countries endeavor to tackle this vulnerability through close cooperation and careful monitoring of threats.

58. Outflows of POC generated within Canada appear to be moderate in comparison with the inflows of POC. Illicit proceeds from cocaine sales in Canada are often smuggled into the U.S. Canadian individuals and corporations use tax havens and offshore financial centers to evade taxes, in particular those located in the Caribbean, Europe and Asia.

59. Canada's multiethnic and multicultural character also leaves the country vulnerable to exploitation by OCGs seeking to launder POC or terrorist organizations looking to conceal themselves within law-abiding diaspora communities to finance and promote terrorist activities. Some terrorist groups have also been known to use extortion to gain power over individuals to further their objectives, including by extorting funds from diaspora communities in Canada.[15] Moreover, informal diaspora remittances are open to criminal interference because they circumvent exchange controls and can therefore facilitate ML.

[13] Asia Pacific Group on Money Laundering Yearly Typologies Report, 2013.

[14] In response to such threats, Canada created the Illicit Financing Advisory Committee (IFAC) in September 2010. IFAC is responsible for advising the Department of Finance and its Minister about high-risk jurisdictions, and provides a formal mechanism to share information among Canadian government departments and AML/CFT agencies in order to identify and assess the ML/TF threats posed by foreign jurisdictions and entities to Canada.

[15] NRA, p.26.

Country's Risk Assessment and Scoping of Higher Risk Issues

60. The Canadian authorities recently undertook a comprehensive ML/TF NRA. They prepared a classified, restricted NRA report that was shared within the government, as well as a shorter, public version that was published in July 2015.

61. The NRA weighs ML/TF threats against the inherent vulnerabilities of sectors (i.e., to assess the likelihood of ML/TF) and then maps those inherent potential risk scenarios using ratings (i.e., very high, high, medium, low) of individual threat and vulnerability profiles. The threats analyzed included some related to sectors that are not currently subject to the PCMLTFA (e.g., check cashing businesses, closed-loop pre-paid access, financing and leasing companies). Ratings serve to illustrate the relative importance of various factors/elements/components relevant to ML/TF. Metrics were based on judgments and were heavily reliant on subject-matter experts' input and readily available information. Based on this approach, all assessed sectors and products were found to be potentially exposed to inherent ML risks while a more limited number of them were found to be exposed to inherent TF risks.

62. While the NRA findings did not contain major unexpected revelations regarding inherent ML or TF threats, the authorities reported that the exercise revealed the magnitude of the threat affecting the real estate sectors and arising from third-party money launderers.

Scoping of Higher Risk Issues

63. The assessment team gave increased attention to the following issues which it considered posed the highest ML/TF risk in Canada or warranted more thorough discussions:

- Third-party money launderers (e.g., professional money launderers): The NRA found that large-scale and sophisticated ML operations in Canada, notably those connected to transnational OCGs, frequently involve professional money launderers;
- Exposure of the Canadian economy to international ML/TF activities (i.e., deposit taking sector, real estate sector, and illicit outflows from Canada to so-called tax haven jurisdictions): A number of sectors are highly vulnerable to ML/TF linked to foreign countries, notably due to the openness of the Canadian economy, the volume of international migrants and visitors, a large and accessible financial system, and a well-developed international trading system;
- Inflows and outflows of POC (including with respect to fraud, corruption, OCG and tax evasion): A better understanding of the nature and magnitude of the inflows and outflows of POC was sought to analyze how Canadian regulators and banks are mitigating the risks of the banking system and to evaluate the effectiveness of international cooperation efforts;
- Sanctioning of ML activities (i.e., all ML offenses) and confiscation of POC: The team gathered information on the number and nature of investigations, prosecutions, sanctions

imposed and confiscations related to ML and the main predicate offenses in order to analyze trends since the 2008 MER; and

- Transparency of legal persons and trusts: The high level of vulnerability of Canadian legal persons and arrangements is reflected by the high level of threat of third-party ML, the inoperativeness of AML/CFT requirements to legal counsels, legal firms and Quebec notaries, and the frequent use of front companies by OCGs.

B. Materiality

64. Canada has a large and diversified economy, with assets totaling about 500 percent of GDP.[16] In 2014, 70 percent of the economy was devoted to services, while manufacturing and primary sectors accounted for the remaining 30 percent.[17] International trade represents more than 60 percent of Canada's GDP. Most of Canada's trade is with the U.S. (74 percent of export and 64 percent of import) followed by China and Mexico.[18]

65. Canada's financial system plays a key role in the Canadian economy and the global financial system. Canadian FIs provide substantial services to non-residents. The financial system is dominated by banks that total 42 percent of the financial sector assets, and by a handful of players in most sectors. The D-SIBs hold 93 percent of bank assets. The IMF's 2014 Financial Sector Assessment Program (FSAP) found that Canada's regulatory and supervisory framework demonstrates strong compliance with prudential international standards. Responsibility for supervision of FIs and markets is divided among federal and provincial authorities. The majority of the prudential supervision of the financial sector is regulated at the federal level by OSFI, though a significant segment is subject to provincial regulation.[19] In regard to prudential and business conduct, financial supervision is generally well coordinated across the federal oversight bodies.

Financial Sector and DNFBPs

66. There are approximately 30,000 REs subject to the PCMLTFA.

Table 1. Entities by Sector (as of November 2015)

Sector	Number of Entities	Subject to PCMLTFA (Y/N)
Domestic Systemically Important Banks (D-SIBs)	6	Y

[16] Canada is one of the 29 jurisdictions whose financial sectors are considered by the IMF to be systematically important: *Press Release NO 14/08* of January 13, 2014.

[17] See Canada's National Risk Assessment, p.27.

[18] CIA World Factbook, 2015.

[19] For more information on the financial sector, see IMF 2014 Financial Sector Stability Assessment of Canada (www.imf.org/external/pubs/ft/scr/2014/cr1429.pdf). Canada's NRA states that the banking sector is highly concentrated and holds over 60 percent of the financial system's assets.

Domestic Banks (other than D-SIBs)	22	Y
Foreign Bank Subsidiaries	24	Y
Foreign Bank Branches	29	Y
White-Label ATM Operators (Non-bank or financial institution)	43,100 (est.)	N
Mortgage Lenders	Not available	N
Leasing Companies	Over 200 (est.)	N
Life Insurance Companies	73 federal and 18 provincially-regulated	Y
Independent Life Insurance Agents And Brokers 1/	154,000 agents and 45,000 brokers (est.)	N
Trust and Loan Companies	63 federally-regulated trust companies and loan companies and 14 provincially-regulated	Y
Securities Dealers	3,487 (The D-SIBs own six of the securities dealers, accounting for 75 percent of the sector's transaction volume)	Y
Credit Unions and Caisses Populaires (CU/CPs)	696 CU/CPs9 that are provincially-regulated; 6 Cooperative Credit Associations and 1 Cooperative Retail Association that are federally-regulated	Y
Money Services Businesses (MSBs)	850 registered MSBs	Y
Check cashing businesses	Not available	N
Provincially-Regulated Casinos	39	Y
Ship-based casinos	0	N
Real Estate Agents and Developers	20,784	Y
Dealers in Precious Metals and Stones	642	Y
British Columbia Notaries	336	Y
Accountants	3,829	Y
Legal Professionals	104,938 lawyers, 36,685 paralegals and 3,576 civil law notaries	N (to legal counsels, legal firms and Quebec notaries)
Trust and Company Services Providers	8	N
Registered Charities	86,000 federally registered charities	N
1/ While independent insurance agents and brokers are not directly covered under the PCMLTFA, life insurance companies may use agents or brokers to ascertain the identity of clients on the basis of a written agreement or arrangement, which must conform to the requirements of PCMLTFR, s.64.1.		

67. The broader deposit taking sector includes trust and loan companies. Canada's largest trust and loan companies are subsidiaries of major banks. Some trusts have provincial charters and are

regulated at that level of government. Credit unions and caisses populaires are provincially incorporated and may not operate outside provincial borders. Relative to banks, these entities are minor participants in the deposit-taking sector. However, caisses populaires represent a large portion of the deposit-taking sector in the province of Quebec.

68. The insurance industry is an important player in the financial services sector, providing almost one-fifth of all financing to Canadian companies. Canadian-owned insurers take in more than 70 percent of total Canadian premium income. Canadian companies are also active abroad, especially in south-east Asia, generating more than half of their premium income from foreign operations.

C. Structural Elements

69. The key structural elements for effective AML/CFT controls are present in Canada. Canada is generally considered to be a very stable democracy. Political and institutional stability, accountability, the rule of law and an independent judiciary are all well established. There also appears to be a high-level political commitment to improve the effectiveness of Canada's AML/CFT regime, as evidenced by the Economic Action Plans 2014 and 2015.[20,21] However, LEAs' resources are generally insufficient to pursue complex ML cases.

70. Canada has an independent, efficient, and transparent Justice System. The judicial process is widely trusted and effective, as well as relatively quick.

71. Canada has a comprehensive legal framework that governs the protection of personal information of individuals in both the public and private sectors. The primary source of constitutionally enforced privacy rights is Section 8 of the Canadian Charter of Rights and Freedoms. The Office of the Privacy Commissioner (OPC) oversees compliance with both federal privacy laws (see Box 1 below). Every province has its own privacy law and the relevant provincial act applies to provincial government agencies instead of the federal legislation. The Canadian regime is implemented while seeking an appropriate balanced between privacy and security considerations. In

[20] Budget 2014 announced the Government's intention to take action to address the need to enhance the AML/CFT framework. As a result, the Government introduced in 2015 legislative amendments and regulations aiming to strengthen Canada's AML/CFT regime and improve Canada's compliance with international standards. This reform was based on the five-year review of the PCMLTFA undertaken by the Standing Senate Committee on Banking, Trade and Commerce in 2013. Economic Action Plan 2015 (Budget 2015) provides updates on these measures. The Government proposed to provide FINTRAC up to Can$10.5 million over five years and up to Can$2.2 million per year subsequently. The Government also proposed to provide up to Can$12 million on a cash basis over five years to improve FINTRAC's analytics system. This allocation intends to better meet the needs of Canadian law enforcement and other regime partners. See Budget 2014, www.budget.gc.ca/2014/docs/plan/pdf/budget2014-eng.pdf.

[21] Includes additional allocation of Can$292.6 million over five years in intelligence and law enforcement agencies for additional investigative resources to counter terrorism. See http://www.budget.gc.ca/2015/docs/plan/budget2015-eng.pdf.

that regard, in 2012 the OPC issued guidance for REs regarding reporting suspicions to FINTRAC, in light of their customers' privacy rights.[22]

Box 1. Legal Framework for Information and Data Protection in Canada

The primary source of privacy rights is Section 8 of the Canadian Charter of Rights and Freedoms, which provides protection against unreasonable search and seizure by authorities. This means, generally, that in situations where the person concerned has a reasonable expectation of privacy in relation to an object or document, in order for the state (i.e., government authorities such as LEAs) to have access to these items, prior judicial authorization will need to be obtained. Where such access is sought for the purposes of a criminal investigation, LEAs will generally seek to obtain a search warrant or a production order from a Canadian court. The latter is typically used for access to financial information held by a third party, such as a FI. "Reasonable grounds to believe" that an offense has been committed is the legal standard of proof in Canadian Law for the court to issue the appropriate order. In addition, it is necessary to demonstrate that evidence of the offense is to be found in the place to be searched. In certain cases, such as in relation to certain types of financial information, a lower legal standard of "reasonable grounds to suspect" applies.

At the federal level, Canada has two different privacy acts which are enforced by the Office of the Privacy Commissioner of Canada. The Privacy Act regulates the handling of personal information by federal government departments and agencies. The Personal Information Protection and Electronic Documents Act (PIPEDA) applies to the commercial transactions of organizations that operate in Canada's private sector. PIPEDA applies to all private sector entities in Canada, except in provinces that have enacted substantially similar legislation. Every Canadian province and territory has its own privacy law and the relevant provincial act applies to provincial government agencies instead of the federal legislation.

The Privacy Act lists 13 uses and disclosures that might be permissible without the consent of the individual (e.g., national security, law enforcement, public interest). Canadian law provides for lawful access to law enforcement and national security agencies to legally intercept private communications and the lawful search and seizure of information, including computer data, without the consent of either the sender or receiver to investigate serious crimes, including ML and threats to national security, such as terrorism. Lawful access is provided for in the CC, the CSIS Act, the Competition Act and other acts.

The Anti-Terrorism Act (ATA) provides law enforcement and national security agencies powers to obtain electronic search warrants. The ATA also allows Canadian intelligence agencies to intercept communications of Canadians in Canada, and allows the Attorney General to prevent the disclosure of information on the grounds of national security.

Under the PCMLTFA, FINTRAC receives detailed personal information through reports from REs, which can then be provided to the CRA (in cases which include tax matters), CSIS, CBSA, Citizenship and Immigration Canada (in cases which include immigration matters) or to LEAs (e.g., when the information is relevant to the investigation and prosecution of ML or TF offenses).

D. Background and other Contextual Factors

72. Canada ranks among the highest in international measurements of government transparency, civil liberties, quality of life, economic freedom, and education. It enjoys a high rate of

[22] *Privacy and PCMLTFA: How to balance your customers' privacy rights and your organization's anti-money laundering and anti-terrorist financing reporting requirements.* Office of the Privacy Commissioner Canada (2012). See www.priv.gc.ca/information/pub/faqs_pcmltfa_02_e.asp.

financial inclusion, with 96 percent of the population having an account with a formal FI. Canadian banks and other FIs operate an extensive network of more than 6,000 branches, and around 60,000 ATMs of which about 16,900 are bank-owned (the rest are white-label ATMs).[23]

73. The authorities have identified corruption as a high-risk issue for ML. Recent assessments of Canada's implementation of international anti-corruption conventions indicate a rather moderate range of positive outcomes in identifying and sanctioning cases of corruption and implementing structures and systems to prevent corruption.[24] Nevertheless, corruption does not appear to hinder the implementation of the AML/CFT regime. Canada is ranked as 9 out of 168 countries in Transparency International's 2015 Corruption Perception Index (with a score of 83/100).[25]

AML/CFT Strategy

74. As formulated in Budget 2014, the Government's priority in regards to AML/CFT is to improve the ability to trace and detect criminal funds in Canada. Besides law enforcement goals, this priority also aims to protect the tax base by supporting the Government's efforts to ensure tax compliance. Addressing this priority requires improving corporate transparency.

75. Canada does not have formal 'stand-alone' AML, CFT, or PF strategies. There is, however, a set of relevant policies and strategies: the National Identity Crime Strategy (RCMP 2011); National Border Risk Assessment 2013–2015 (CBSA); 2014–16 Border Risk Management Plan (CBSA); Enhanced Risk Assessment Model and Sector profiles (FINTRAC); AMLC Division AML and CFT Methodology and Assessment Processes (OSFI); Risk Ranking Criteria (OSFI); RBA to identify registered charities and organizations seeking registration that are at risk of potential abuse by terrorist entities and/or associated individuals (CRA) and CRA-RAD Audit Selection process. The RCMP recently developed its National Strategy to Combat ML.[26] These AML strategies and policies are linked to the *Canadian Law Enforcement Strategy on Organized Crime* adopted by senior police officials across Canada in 2011.

76. The Government's other main AML/CFT concerns are reflected in Finance Canada's Annual Report on Plans and Priorities,[27] which describes the AML/CFT regime's spending plans, priorities

[23] In Canada, "white label" or "no name" ATMs are those run by independent operators and not by major financial institutions. They are usually located in local small establishment retailers such as gas stations, bars/pubs, and restaurants and do not display labels from financial institutions on the machine.

[24] See 2014 review of the implementation by Canada of the Inter-American Convention against Corruption; 2013 Phase 3 report on implementation of the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transaction and the 2009 Recommendation of the Council for Further Combating Bribery of Foreign Public Officials in International Business Transactions.

[25] Transparency International's 2015 Corruption Perception Index. See http://www.transparency.org/cpi2015.

[26] 2015–16 Report on Plans and Priorities, Royal Canadian Mounted Police. See www.rcmp-grc.gc.ca/en/royal-canadian-mounted-police-2015-16-report-plans-and-priorities; this strategy was finalized in 2016.

[27] Report on Plans and Priorities 2014–15. Department of Finance Canada (2014). See www.fin.gc.ca/pub/rpp/2014-2015/index-eng.asp.

and expected results. Canada's CFT strategy policy guidance is derived from its 2012 Counter-terrorism Strategy.[28] This comprehensive Strategy guides more than 20 federal departments and agencies to better align them to address terrorist threats, including in regard to CFT activity and initiatives. The Minister of Public Safety and Emergency Preparedness, in consultation with the Minister of Foreign Affairs, is responsible for the Strategy's implementation. Similarly, the country's PF strategy forms part of the broader strategy to counter the proliferation of chemical, biological, radiological and nuclear weapons.

Legal and Institutional Framework

77. Canada's AML/CFT regime is organized as a horizontal federal program comprised of a large number of federal departments and agencies. Finance Canada is the domestic and international policy lead for the regime, and is responsible for its overall coordination, including guiding and informing strategic implementation of the RBA. It chairs the four main governing bodies of Canada's AML/CFT regime, namely:

- The interdepartmental Assistant Deputy Minister (ADM) Level Steering Committee, which was established to direct and coordinate the government's efforts to combat ML and TF activities. The ADM Committee and its working group consists of representatives of all partners;[29]

- The Interdepartmental Coordinating Committee (ICC), which provides a forum for government working-level stakeholders[30] to assess the operational efficiency and effectiveness of the regime;

- The National ML/TF Risk Assessment Committee (NRAC) provides a forum for regime and ad hoc partners to exchange information on risks and discuss about ML/TF risks in Canada and their mitigation; and

- The Public Private Sector Advisory Committee (PPSAC) which is a discussion and advisory committee, with membership from (federal public sector) regime partners and private sector REs, as well as provincial law enforcement.[31]

[28] Building Resilience Against Terrorism—Canada's Counter-Terrorism Strategy. Public Safety (2012). See http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rslnc-gnst-trrrsm/index-eng.aspx.

[29] The ADM Committee is composed of the following agencies: Finance Canada; Justice Canada; PPSC; Public Safety Canada; CRA; FINTRAC; RCMP; CBSA; OSFI; and CSIS.

[30] The ICC is composed of the following agencies: Finance Canada; PPSC; Public Safety Canada; CRA; FINTRAC; RCMP; CBSA; CSIS; OSFI; Privy Council Office (PCO); and Global Affairs Canada.

[31] This Committee consist of approximately 30 members, with more than half of the members coming from the private sector. The public sector participants generally consist of members who already participate in the Interdepartmental Steering Committee on this topic. The private sector participants will consist of participants from sectors covered by the PCMLTFA. This includes financial entities, life insurance companies, securities dealers, money service businesses, accountants, the notarial profession, the real estate sector, casinos, dealers in precious metals and stones, and home builders.

78. The AML/CFT regime operates on the basis of three interdependent pillars: (i) policy and coordination; (ii) prevention and detection; and (iii) investigation and disruption. On this basis, the following are the primary ministries, agencies, and authorities responsible for formulating and implementing Canada's AML/CFT policies (i.e., the regime partners):

Policy and Coordination

- **Finance Canada** is the lead agency of the regime, responsible for developing AML/CFT policy related to domestic and international commitments.
- **Department of Justice Canada (DOJ)** is responsible for the drafting and amending of statutory provisions dealing with criminal law and procedure, and to negotiate and administer mutual legal assistance (MLA) and extradition treaties.
- **Global Affairs Canada (GAC)**[32] is responsible for the designation of entities and individuals in Canada associated with terrorist activities listed by the United Nations 1267 Sanctions Committee or under Resolution 1373 of the United Nations Security Council. GAC also chairs the Counter-Proliferation Operations Committee, coordinating responses to threats within Canada.
- **Public Safety Canada (PSC, previously known as Public Safety and Emergency Preparedness)** chairs the Threat Resourcing Working Group and ensures coordination across all federal departments and agencies responsible for national security and the safety of Canadians, including on terrorist financing matters. It is responsible for the listing of terrorist entities under the Criminal Code and co-chairs the Interdepartmental Coordinating Committee on Terrorist Listings.

Prevention and Detection

- **Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)** is Canada's financial intelligence unit. It is also responsible for supervising and monitoring all REs' compliance with the PCMLTFA.
- **Office of the Superintendent of Financial Institutions Canada (OSFI)** prudentially supervises FRFIs.
- **Innovation, Science and Economic Development Canada (ISED, former Industry Canada)** collects information about business corporations, including the business name and address, and information about the directors.
- **Office of the Privacy Commissioner of Canada (OPC)** ensures that the necessary safeguards protecting privacy are upheld. The Privacy Commissioner has the ability to audit

[32] Global Affairs Canada's Anti-Crime and Counter-Terrorism Capacity Building programs (ACCBP and CTCBP) funding has been used to support the Regime's AML and CFT projects in a number of regions.

the public (e.g., FINTRAC) and private sector to ensure privacy laws are respected. The OPC is required to conduct a privacy audit of FINTRAC every two years.

Investigation and Disruption

- **Royal Canadian Mounted Police (RCMP)** is Canada's main law enforcement agency (LEA) responsible for investigating predicate offenses, ML and TF.
- **Public Prosecution Service of Canada (PPSC)** is responsible for prosecuting criminal offenses under federal jurisdiction. It also provides legal advice to the RCMP and other LEAs over the course of their investigations, and for undertaking any subsequent prosecutions.
- **Canada Revenue Agency (CRA)**—the CRA's Criminal Investigations Directorate (CID) investigates cases of suspected tax evasion/tax fraud and seeks prosecution through the PPSC where warranted. The CRA also has responsibility for administering the registration system for charities under the Income Tax Act through its Charities Directorate.
- **Canada Border Services Agency (CBSA)** enforces the physical cross-border reporting obligation.
- **Canadian Security Intelligence Service (CSIS)** collects, analyzes and reports to the Government of Canada information and intelligence concerning threats to Canada's national security.
- **Public Services and Procurement Canada (PSPC, previously Public Works and Government Services Canada)**, under the Seized Property Management Directorate (SPMD), is responsible for managing assets seized or restrained by law enforcement in connection with criminal offenses and for disposing and sharing the proceeds upon court declared forfeitures.

79. The AML/CFT regime is also supported by a number of other partners including: provincial, territorial and municipal LEAs, provincial and territorial financial sector regulators, and self-regulatory organizations.

80. Canada's AML/CFT framework is established in the PCMLTFA, supported by other key statutes, including the Criminal Code (CC). The Parliament of Canada undertakes a comprehensive review of the PCMLTFA every five years. The Government announced a series of measures to enhance the AML/CFT regime in Budget 2014, which received Royal Assent in June 2014. Accordingly, amended Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFR) were released in draft form for consultation by the Government on July 4, 2015.

Proliferation Financing

81. The principal legislation governing Canada's export control system is the Export and Import Control Permits Act (EIPA), which provides for the requirements for exporters to report goods to the

Government of Canada and for the enforcement of national control lists. The Customs Act and Canada Border Services Agency Act provide the CBSA with the authority to enforce Canada's export legislation. The country's efforts to combat the proliferation of weapons of mass destruction and, to some extent, its financing, are carried out by the following agencies: PSC (coordination of counter-proliferation policy and main operational partner); Global Affairs Canada (lead on international engagement on non-proliferation and disarmament and chairs the Counter-Proliferation Operations Committee); CBSA (law enforcement regarding the illicit export and proliferation of strategic goods and technology); Canadian Nuclear Safety Commission (licensing of nuclear-related activities); PWGSC (administers the Controlled Goods Program); FINTRAC (discloses financial intelligence that can assist in investigations and prosecutions); RCMP (enforces the counter-proliferation regime, investigates related criminal offenses, collects and analyzes evidence to support prosecutions in court); the Public Health Agency of Canada (national authority on biosafety and biosecurity for human pathogens and toxins); and Finance (responsible for safeguarding Canada's financial system from illegitimate use, through the PCMLTFA and associated regulations, and the overall coordination of Canada's AML/CFT regime domestically and internationally).

Preventive Measures

82. The legal framework relevant to the preventive measures includes the PCMLTFA, the OSFI Act and the FRFIs' governing legislation (i.e., the Bank Act, Trust and Loan Companies Act, the Cooperative Credit Associations Act and the Insurance Companies Act). The PCMLTFA is applicable to most of the financial activities and DNFBPs.

Legal Persons and Arrangements

a) Overview of Legal Persons

83. Canada's company law consists of federal, provincial and territorial frameworks. Legal entities may be established at the federal level under the Canada Business Corporation Act (CBCA); the Canada Not-for-Profit Corporations Act (NFP Act), or the Canada Cooperatives Act (CCA). A federally incorporated entity is entitled to operate throughout Canada. However, provincial and territorial law requires federal entities to register with the province or territory in which the entity is carrying out business. Incorporation on the federal level is carried out by Innovation, Science and Economic Development Canada (ISED, formerly Industry Canada) is responsible for the incorporation of federal corporate entities, while each province has its own system for incorporating and administering legal entities.

84. There are over 2.6 million corporations incorporated in Canada, including almost 4,000 publicly-traded companies. About 91 percent of corporations are incorporated at the provincial or territorial levels and the remaining 9 percent at the federal level. Bearer shares are permitted in most provinces and at the federal level, but seem to be rarely used. There is also a relatively small market for stock warrants. All companies are obliged to file tax returns with the CRA on an annual basis. Provincial legal entities incorporated in Alberta and Quebec must also file tax returns with the provincial tax authorities.

85. Partnerships are created under provincial law only and, other than limited partnerships, are created under the rules of the common law although subject to laws that codify and regulate certain aspects of the partnership. In contrast, limited partnerships are created under statute and subject to ongoing registration requirements.

b) Overview of Legal Arrangements

86. The only form of legal arrangement that exists in Canada is the trust in form of testamentary or *inter vivos* trust. There is no general requirement for trusts to be registered, but Canadian resident trusts and certain foreign-resident trusts are subject to obligations to file information under the income tax laws. Specific-purpose trusts such as unit or mutual fund trusts are also subject to the securities laws of the relevant province. Trusts created under the laws of Quebec are required to register in some instances. According to the NRA, the total number of Canadian trusts is estimated in the millions. As of 2007, only 210,000 trusts filed tax returns with the CRA.

c) International Context for Legal Persons and Arrangements

87. According to the UNCTAD 2014 World Investment Report, Canada ranks amongst the top ten countries both with respect to inflowing and outflowing foreign direct investment, with much of the activity taking place in the manufacturing and oil and gas sectors. Canada received over US$53 billion of foreign direct investment in 2014 coming mostly from the EU, the U.S., and China. On the outflow, Canada invested approximately US$52 billion abroad in 2014, mostly in the EU and the U.S. While detailed figures are not available with respect to foreign ownership of Canadian companies, the statistics provided by the UNCTAD leads to the conclusion that foreign ownership of Canadian legal entities is significant. Canada is not perceived as an international center for the creation or administration of legal persons or arrangements.

d) Supervisory Arrangements

88. Financial regulation is shared by a number of government bodies in Canada. The Bank of Canada has overall responsibility for financial stability, as well as for the conduct of monetary policy and the issuance of currency. As mentioned above, OSFI supervises and regulates FRFIs (banks and insurance companies, trust and loan companies, cooperative credit associations, fraternal benefit societies, and private pension plans). All banks, including branch operations of foreign banks, are regulated solely at the federal level. The securities sector including in respect of mutual funds, is currently regulated on a province by province basis with connections between the provinces through the Canadian Securities Administrators Association. Markets for securities and collective investments are overseen by provincial securities commissions, which coordinate their activities through the Canadian Securities Administrators.[33]

[33] Canada is currently developing a Cooperative Capital Markets Regulatory System (CCMRS), a new joint federal and provincial initiative. Under this system, the provinces and the federal government would delegate their regulatory functions to the CCMR, which may be useful in regard to the identification of systemic risk and criminal enforcement.

89. In March 2013, FINTRAC and OSFI entered into an agreement to conduct concurrent examinations to improve the effectiveness and cohesion of supervision and allocation of resources, and to reduce the regulatory burden on FRFIs. FINTRAC and OSFI thus concurrently assess FRFIs' AML/CFT compliance and risk management regimes using a RBA. FINTRAC and OSFI mutually share information under a MoU was signed in 2004 with respect to FRFIs. At the provincial level, FINTRAC conducts AML/CFT supervision on non-FRFIs with the cooperation of other national and provincial supervisors under various MOUs.

NATIONAL AML/CFT POLICIES AND COORDINATION

A. Key Findings

The Canadian authorities have a good understanding of the country's main ML/TF risks and have an array of mitigating measures at their disposal. Canada's NRA is comprehensive, and also takes into account some activities not currently subject to the AML/CFT measures.

All high-risk areas are covered by AML/CFT measures, except activities listed in the standard performed by legal counsels, legal firms and Quebec notaries, which is a significant loophole in Canada's AML/CFT framework, and online casinos, open loop prepaid cards, and white label ATMs.

FIs and casinos have a good understanding of the risks. Other DNFBPs, and in particular those active in the real estate sector, do not have a similarly good understanding.

Law enforcement action focus is not entirely commensurate with the ML risk emanating from high-risk offenses identified in the NRA.

Cooperation and coordination are good at both the policy and operational levels, except, in some provinces, in the context of the dialogue between LEAs and the PPSC.

Communication of the NRA findings to the private sector was delayed, but is in progress.

B. Recommended Actions

Canada should:

- Mitigate the risk emanating from legal counsels, legal firms, and Quebec notaries in their performance of the activities listed in the standard.
- Strengthen policies and strategies to address emerging ML risks (in particular white label ATMs and online casinos).
- Review LEAs' priorities in light of the findings of the NRA.
- In the context of the update of the NRA, examine more closely ML linked to tax evasion, corruption, legal persons and arrangements, third-party ML and foreign sources of POC and use results to implement mitigating actions.

The relevant Immediate Outcome considered and assessed in this chapter is IO.1. The recommendations relevant for the assessment of effectiveness under this section are R.1–2.

C. Immediate Outcome 1 (Risk, Policy and Coordination)

90. As indicated in Chapter 1 above, Canada completed in 2015 a national assessment of the inherent ML/TF risks that it faces. The process and main findings of the NRA are described above.

Country's Understanding of its ML/TF Risks

91. The authorities' understanding of ML/TF risks has been forged through the development of several national threat and risks assessments undertaken by different governmental agencies over the past decade on related matters (see Criterion 2.1). The Parliament's Standing Senate Committee on Banking, Trade and Commerce undertakes a comprehensive review of the PCMLTFA every five years. As a result of the most recent review (completed in 2013),[34] the Government introduced legislative amendments in 2014 to address the Committee's recommendations (e.g., including measures to strengthen CDD requirements, improve compliance, monitoring and enforcement and enhance information sharing). The authorities demonstrated a sound understanding of the issues highlighted in Chapter 1, including a good understanding of the linkages between the threats and inherent vulnerabilities of the different sectors and the domestic and foreign offenses that are a source of most of the ML/TF[35] in the country. The NRA process has also contributed to a deeper understanding of the powers, resources and operational needs of all regime partners. NRAC ensures that all regime partners generally have a similar level of understanding of the ML/TF risks.

92. Following the publication of the NRA in July 2015, the NRAC concluded a gap analysis in September 2015 to categorize the residual risks (i.e., the risk remaining after the mitigation of the identified threats and inherent vulnerabilities) and identify and prioritize the actions required to mitigate the risk. The review and updating of the NRA is expected to be finalized by the fall of 2016. The authorities indicated that as new, improved controls are put in place, the residual risk will be an indicator of the areas that remain pending to be addressed. As of the date of the onsite visit, it was not possible to establish if the publication of the NRA has led to improvements of the RE's level of compliance with AML/CFT requirements.

National Policies to Address Identified ML/TF Risks

93. The adjustment of the national policies and strategies related to the identified ML/TF risks is in its early stages and no updates have been completed. The authorities have been addressing the inherent risks identified in different ways including through ongoing policy coordination through NRAC, the discussion of draft amendments to the PCMLTF Regulations, adjusted supervisory

[34] *Follow The Money: Is Canada Making Progress in Combatting Money Laundering and Terrorist Financing? Not Really*—Report of the Standing Senate Committee on Banking Trade and Commerce. Senate of Canada (March 2013). See www.parl.gc.ca/Content/SEN/Committee/411/banc/rep/rep10mar13-e.pdf.

[35] As elaborated in Chapter 1, the classified version of the NRA, which was not shared with the assessment team, ranks in greater detail the TF risks associated with terrorist groups.

priorities, more focused police investigations, and amendments to the law regarding the seizure of illicit assets, among others.

94. On the basis of the NRA, a package of regulatory amendments was issued in July 2015 for public comment. The government is now moving forward with final publication and the Regulations will come into force one year after registration of the regulations. Canada is preparing a second package of regulatory amendments based on the NRA, including measures to cover pre-paid payment products (e.g., prepaid cards), virtual currency as well as money service businesses without a physical presence in Canada in the AML/CFT Regime. The authorities are also revisiting the PCMLTFA provisions relating to legal counsels, legal firms and Quebec notaries, in order to bring forward new provisions for the legal professional that would be constitutionally compliant. Furthermore, also informed by the NRA results, FINTRAC and OSFI are reviewing their RBA to supervision, the RCMP developed its Money Laundering Strategy, and the CBSA is reviewing its Cross-Border Currency Reporting program.

95. As discussed in Chapter 1, Canada's CFT strategy policy guidance is derived from its 2012 Counter-Terrorism Strategy. The PS coordinates Canada's counter-proliferation policy approach across the government, which includes PF.

Exemptions, Enhanced and Simplified Measures

96. Canada's AML/CFT framework does not provide for simplified CDD measures, but the PCMLTFR provide a small number of exceptions to REs based on the risk circumstances and products (see Criterion 10.18). These exemptions correspond to lower-risk scenarios that are consistent with the NRA findings in regard to FIs (i.e., in regard to life insurance companies, brokers, or agents).

Objectives and Activities of Competent Authorities

97. FINTRAC and OSFI objectives and activities are largely consistent with the ML and TF risks in Canada, as detailed in the NRA. With the exception of the legal professions (other than BC notaries), the supervisory coverage is adequate.

98. Law enforcement action is focused on LEAs current priorities, which include drug-related offenses and OCGs, but is not commensurate with the ML risk emanating from these and other types of offenses.

99. In terms of the resources required, the Government's Economic Action Plans for 2014 and 2015 included a commitment to ensuring that law enforcement and security agencies have the investigative resources and tools to address the threats presented by OGCs, ML and terrorism and to further their understanding of Canada's ML/TF risks. Nevertheless, the authorities advised the assessors that all regime partners are under significant pressures at the working level given the increased terrorist threats and combined with the increased threat of professional ML with transnational organized crimes and the number competing priorities.

National Coordination and Cooperation

100. AML/CFT policy cooperation and coordination to address Canada's ML/TF risks is adequate—with the exception of the dialogue between LEAs and the PPS in some provinces, which is currently insufficient—and constitutes an essential strength of the Canadian AML/CFT framework, as evidenced by the organization and process of the NRA. Canada has wide-ranging arrangements in place for AML/CFT coordination and cooperation at both the policy and operational levels, including with respect to strategic and tactical information sharing (see R.2). Coordination and cooperation at the policy design platform is exceptional.

101. The NRA has allowed the identification and inclusion of new partners for AML/CFT (e.g., Defence Research and Development Canada and Environment Canada), and to reconsider the roles and responsibilities of traditional partners that gained a more prominent role in the fight of ML/TF over the years given enhanced understanding of ML/TF risks (e.g., Industry Canada). Overall, the public version of the NRA is of good quality and is drafted in an accessible language. Moreover, the assessment process has yielded reasonable findings that broadly reflect the country's ML/TF context and risk environment.

Private Sector's Awareness of Risks

102. The public version of the NRA had not been circulated widely at the time of the onsite visit, due to a broader prohibition on the federal public service undertaking consultations with private sector stakeholders during the August to October 2015 federal election campaign. However, the public NRA has been made available on Finance Canada's, OSFI's and FINTRAC's website since July 2015.[36] The report was also shared with the PPSAC. As of the dates of the onsite visit, the authorities had not formally presented the results of the communication strategy for the broader private sector, but were in the process of reaching out to selected FIs. FINTRAC also provides access to guidelines, Interpretation Notices reports on current and emerging trends and typologies in ML and TF on its website to assist FIs and DNFBPs.

Overall Conclusions on Immediate Outcome 1

103. Canada has achieved a substantial level of effectiveness for IO.1.

[36] The NRA has since been made available on several websites (e.g., OSFI, Investment Industry Organization of Canada, among others).

LEGAL SYSTEM AND OPERATIONAL ISSUES

A. Key Findings

IO.6

Financial intelligence and other relevant information are accessed by FINTRAC to some extent, and by LEAs to a greater extent but through a much lengthier process.

They are then used by LEAs to some extent to investigate predicate crimes and TF, and, to a more limited extent, to investigate ML and trace assets.

FINTRAC receives a wide range of information, which it uses adequately to produce intelligence. This intelligence is mainly prepared in response to Voluntary Information Records (VIRs; i.e., LEAs' requests) and used to enrich ongoing investigations into the predicate offenses. FINTRAC also makes proactive disclosures to LEAs, some of which have prompted new investigations.

Several factors significantly curtail the scope of the FIU's analysis—and consequently the intelligence disclosed to LEAs—in particular: the impossibility for FINTRAC to request from any RE additional information related to suspicions of ML/TF or predicate offense, the absence of reports from some key gatekeepers (i.e., legal counsels, legal firms, and Quebec notaries), and the inability for FINTRAC to access to information detained by the tax administration. This is compensated by LEAs in their investigations to some extent only due to challenges in the identification of the person or entity who may hold relevant information.

FINTRAC also produces a significant quantity of strategic reports that usefully advise LEAs, intelligence agencies, policy makers, REs, international partners, and the public, on new ML/TF trends and typologies.

FINTRAC and the LEAs cooperate effectively and exchange information and financial intelligence in a secure way.

IO.7

Canada identifies and investigates ML to some extent only. While a number of PPOC cases are pursued, overall, the results obtained so far are not commensurate with Canada's ML risks.

LEAs have the necessary tools to obtain information, including beneficial ownership information, but the process is lengthy.

In some provinces, such as Quebec, federal, provincial, and municipal authorities are relatively more effective in pursuing ML.

Nevertheless, overall, as a result of inadequate alignment of current law enforcement priorities with the findings of the NRA and of resource constraints, LEAs' efforts are aimed mainly at drug

offenses and fraud, with insufficient focus on the other main ML risks (corruption, tobacco smuggling, standalone ML, third-party ML, ML of foreign predicate offenses). In addition, investigations generally do not focus on legal entities and trusts (despite the high risk of misuse), especially when more complex corporate structures are involved.

There is a high percentage of withdrawals and stays of proceedings in prosecution.

Sanctions imposed in ML cases are not sufficiently dissuasive.

IO.8

Canada has made some progress since its last evaluation in terms of asset recovery, but the fact that assets of equivalent value cannot be recovered hampers Canada's recovery of POC.

Confiscation results do not adequately reflect Canada's main ML risks, neither by nature nor by scale.

Results are unequal, with some provinces, such as Quebec, being significantly more effective, and achieving good results with adequately coordinated action (both at the provincial level and with the RCMP) and units specialized in asset recovery.

Administrative efforts to recover evaded taxes appear more effective.

Sanctions are not dissuasive in instances of failure to properly declare cross-border movements of currency and bearer negotiable instruments.

B. Recommended Actions

Canada should:

IO.6

- Increase timely access to financial intelligence. Authorize FINTRAC to request and obtain from any RE further information related to suspicions of ML, predicate offenses and TF in order to enhance its analysis capacity.
- Use financial intelligence to a greater extent to investigate ML and trace assets.
- Analyze and, where necessary, investigate further information resulting from undeclared or falsely declared cross-border transportation of cash and bearer negotiable instruments.
- Ensure that LEAs and FINTRAC can identify accounts and access records held by FIs/DNFBPs in a timely fashion.
- Consider granting FINTRAC access to information collected by the CRA for the purposes of its analysis of STRs.

IO.7

- Increase efforts to detect, pursue, and bring before the courts cases of ML related to high-risk predicate offenses other than drugs and fraud (i.e., corruption and tobacco smuggling), as well as third-party ML, self-laundering, laundering of POC of foreign predicate offenses, and the misuse of legal persons and trusts in ML activities.
- Ensure that LEAs have adequate resources (in terms of number and expertise) for ML investigations.
- Engage prosecutors at an earlier stage for securing relevant evidence for ML/PPOC prosecutions in order to limit instances where charges are dropped at the judicial process and minimize waste of resources in ML investigations.
- Ensure that effective, proportionate, and dissuasive sanctions for ML are applied.

IO.8

- Ensure that asset recovery is pursued as a policy objective throughout the territory.
- Make a greater use of the available tools to seize and restraint POC other than drug-related instrumentalities and cash (i.e., including other assets, e.g., accounts, businesses, and companies, property or money located abroad), especially proceeds of corruption, including foreign corruption, and other major asset generating crimes.
- Amend the legal framework to allow for the confiscation of property of equivalent value.
- Consider increasing the sanctions and seizures related to falsely declared or undeclared cross-border movements of currency and bearer negotiable instruments.

The relevant Immediate Outcomes considered and assessed in this chapter are IO.6–8. The recommendations relevant for the assessment of effectiveness under this section are R.3, R.4, and R.29–32.

C. Immediate Outcome 6 (Financial Intelligence ML/TF)

Use of Financial Intelligence and other Information

104. Financial intelligence derives from a wide range of information collected by LEAs and received by FINTRAC. Both processes are closely linked. FINTRAC's main financial intelligence product takes the form of disclosures made in response to LEAs' requests (i.e., voluntary information records, VIRs). FINTRAC also disseminates information to LEAs spontaneously (i.e., through "proactive disclosures").

105. LEAs request and obtain financial information held by the private sector either through a court warrant or a production order, when they can establish (as per the CC) that assets are POC. To

obtain this judicial authorization, LEAs must identify the FI/DNFBP or entity that holds the information (i.e., account or assets owned or controlled, financial transactions or operation). Various methods are available (see TCA criterion 24.10) and used in practice, such as "grid searches," VIRs to FINTRAC, and consultation of other sources of information as well as use of a range of investigative activities. In Ontario (where the major D-SIBs have their headquarters), "grid searches" are frequently conducted: LEAs send a request to the six D-SIBs (as they dominate about 80 percent of the deposit-taking market) inquiring whether a particular person is amongst their customers. If there is indication that this person is in business relationships with another FI or with a DNFBP, a request will be sent to that RE as well. Once a D-SIB (or other RE) confirms that a specific person is its customer, the LEAs apply for a court order requiring the D-SIB to produce the relevant account and beneficial ownership information, as well as transaction records. If necessary, the production is staged to expedite the procedure (i.e., the specific information stated in the order is produced first, and the remainder of the information is provided at a later stage). Nevertheless, the D-SIBs typically take up to several weeks to provide basic and beneficial ownership information to the LEA. As result of the time required at the initial stage (i.e., identification of the relevant RE that may hold the information), as well as the time imparted to implement the production order, it frequently takes 45-90 days before LEAs can obtain the initial transaction records of potential POCs. If the culprit uses numerous layering techniques before integration, it takes LEAs several months or even years to trace POCs. The outlined process is useful only if the persons under investigation bank with the D-SIBs or one of the other large FIs. In cases where a targeted person or entity is in a business relationship with a smaller FI or a DNFBP, the tracing of assets is far more burdensome; given the size of Canada and its financial and non-financial sectors, it is not possible for LEAs to check with each FI and DNFBP individually whether it holds relevant information. In these instances, the identification of the relevant FI or DNFBPs relies on other potentially lengthier methods (e.g., surveillance).

106. LEAs frequently obtain financial information and intelligence from FINTRAC, with or without prior judicial authorization. Most often, they request the information by sending VIRs (which do not require prior judicial authorization). This provides LEAs with a quicker access to the information they need to obtain the judicial authorization (but timeliness of production of requested information remains a challenge). The number of VIRs has increased steadily over the years.[37] This indicates a greater appetite for and appreciation of FINTRAC's reports.[38] Most LEAs expressed their satisfaction with the richness of FINTRAC's responses to VIRs and mentioned that these responses adequately supplement their ongoing investigations.[39] In 2011, the Canadian Association of Chiefs

[37] Number of VIRs received: 2010–2011: 1,186; 2011–2012: 1,034; 2012–2013: 1.082; 2013–2014: 1,320; 2014–2015: 1,380.

[38] The Canadian authorities were not able to provide additional information regarding the proportion of predicate offense investigations that lead to a VIR.

[39] The Canadian authorities provided examples of written testimonies of some agencies' satisfaction with FINTRAC's response to their VIRs. E.g., "*The disclosure was very impressive in its detail and scope. Shortly after receiving it, our General Investigation Service Unit generated a file resulting in a large seizure of drugs. The individuals mentioned in the disclosure were identified as involved*" (RCMP 'G' Division Federal Investigations Unit); "*The information obtained led us to start a new investigation focused on the money trail—namely the illegal means used by the accused to launder the money they obtained in this case*" (Sûreté du Québec); "*Quick turnaround time was appreciated. The disclosures*

of Police also recognized the contribution of financial intelligence, and called on all Canadian LEAs to include financial intelligence in their investigations and share their targets with FINTRAC.[40]

107. FINTRAC also provides information to LEAs on a spontaneous basis, through proactive disclosures, both in instances linked to ongoing investigation and in cases that identify new potential targets. Between January 1, 2010 and November 31, 2015, the RCMP received 2,497 FINTRAC disclosures, 867 of which were proactive.[41] Of these proactive disclosures, the authorities indicated that 599 generated a new investigation.[42] Very few resulted in ML charges (see IO.6.3 and IO.7). The cases communicated to and discussed with the assessors highlighted that FINTRAC information (in response to VIRs and/or shared proactively) is used by LEAs mainly as a basis for securing search warrants, aiding in the selection of investigational avenues (including the identification of targets, associates, and victims) and providing clarification of relevant domestic and international bank accounts and cash flows.

108. Additional relevant information is used to varying degrees: (i) The RCMP and other LEAs receive relevant information from provincial Securities Commissions and recognize the value of such information in combating ML/TF in the context where corporations are identified as very highly vulnerable to be abused for ML/TF. In Toronto and Montreal, the RCMP now includes personnel from the Securities Commission (Joint Securities Intelligence Unit—SIU) to facilitate intelligence gathering, analysis, and dissemination functions. The Canadian authorities provided examples of the use of information communicated to LEAs by the "Autorité des marches financiers" (AMF) (including Project Carrefour detailed below, as well as projects Convexe, Jongleur, Incitateur, and Ilot). In these cases, the financial intelligence was used to develop the financial part of the investigation into the predicate offense, not to investigate potential ML activities. (ii) The CRA-CID also uses financial intelligence to identify potential tax evasion. (iii) The CBSA forwards to FINTRAC and to the RCMP all Cross-Border Currency reports (CBCRs) submitted by importers or exporters. It also forwards seizure reports to FINTRAC. It seems that both FINTRAC and the RCMP use the CBSA information to supplement ongoing analysis and investigations[43] and that they analyze or, in the case of LEAs, investigate the CBSA information to a very limited extent, namely only when it has no link to existing

provided new information of potential interest along with account numbers not previously known. The Service was further able to identify additional relationships, which assisted our national security investigation. The information in the electronic funds transfers was found to provide valuable intelligence" (Canadian Security Intelligence Service).

[40] Canadian Association of Chiefs Police (Resolution #06-2011).

[41] FINTRAC also makes disclosures to other LEAs.

[42] According to the authorities, 297 completed feedback forms indicated that FINTRAC proactive disclosures prompted a new investigation in 53 cases between January 1, 2008 and November 31, 2015. In 92 cases a proactive disclosure provided the names of, or leads on, previously unknown persons or businesses/entities, 90 provided new information regarding persons or businesses of interest, 53 triggered a new investigation and 17 provided intelligence that may generate a future investigation. Only one of the 53 new investigations prompted following a proactive disclosure was shared with the assessors.

[43] RCMP indicated that of all ML, PPOC, and TF investigations and cross-border currency reporting have been used in 331 cases.

cases (see IO.7). Two cases originating from this intelligence have been communicated to the assessors, including project Chun (see Box 4 in IO.7).

Box 2. Project Carrefour

In December 2008, the Montreal Integrated Market Teams (IMET) Program[44] initiated an investigation based on an AMF referral. The AMF is mandated by the government of Quebec to regulate the province's financial markets and provide assistance to consumers of financial products and services. The referral indicated that individuals' Registered Retirement Savings Plans (RRSPs) and other types of retirement savings accounts were being emptied using methods that avoided attention from regulatory and fiscal authorities. The scheme consisted of attracting the attention of investors, through classified ads, with RRSPs and/or other types of retirement savings accounts looking for financial aid. In order for the investors to receive that aid, they had to give up full control of their accounts. The operators of the schemes would then empty those accounts to use the funds to transact on a variety of publicly traded companies under their control, hence engaging in market manipulation. On February 15, 2011, eleven Montréal and Toronto residents were charged with various fraud related offenses committed against 120 investors. They were also charged with fraudulent manipulation of stock exchange transactions estimated at US$3 million.

109. In sum, financial intelligence is used to some extent to develop evidence and trace criminal proceeds. While a great deal of information provided by REs and others (i.e., in STRs and CBCRs) is used by FINTRAC for tactical analysis, strategic analysis, and to take supervisory action, a large part of this information is not further used by its partners for tactical cases, until it appears relevant for an ongoing investigation. Moreover, a relatively small portion of the intelligence is used for the specific purpose of pursuing ML activities.

110. Financial intelligence and other relevant information are, however, more frequently used to pursue TF. FINTRAC, in consultation with some of the other competent authorities, published advisories that assisted the FIs in their efforts to identify potential ISIL and TF-related activities and funding. Financial intelligence is accessed and used in TF investigation (see below and IO.9), and the onsite discussions as well as the authorities' submissions indicate that FINTRAC's proactive disclosures and responses to VIRs are appreciated by LEAs in their TF efforts.[45]

STRs Received and Requested by Competent Authorities

111. FINTRAC receives a significant quantity of information in various reports (see table below), which it uses to develop its financial intelligence.

Table 2. Types of Reports Received by FINTRAC (excluding terrorist property reports)

	2010–2011	2011–2012	2012–2013	2013–2014	2014–2015

[44] The objective of the IMET program is to effectively enforce the law against serious criminal capital market fraud offenses in Canada. The authorities involved in the program are the RCMP, ODPP, DOJ, and Finance Canada.

[45] "*FINTRAC is considered a key partner and has provided valuable financial intelligence on an ongoing basis that contributed to "terrorist financing investigations." FINTRAC through their disclosures identified new linkages/nexus between entities and/or individuals through financial transactions which surfaced new avenues of investigation. FINTRAC has always responded in a timely fashion to our priority VIRs*" (RCMP Anti-Terrorist Financing Team, National Security Criminal Operations, Headquarters, Ottawa. FINTRAC 2012 Annual Report, p.11, Document 102).

Large Cash Transaction Reports	7,184,831	8,062,689	8,523,416	8,313,098	8,445,431
Electronic Funds Transfer Reports	11,878,508	10,251,643	10,993,457	11,182,829	12,348,360
STRs	58,722	70,392	79,294	81,735	92,531
Cross-Border Currency Reports /Cross-Border Seizure Reports	40,856	35,026	31,826	42,650	47,228
Casino Disbursement Reports	102,438	109,172	116,930	130,141	155,185
Total	19,265,355	18,528,922	19,744,923	19,750,453	21,088,735

112. With respect to STRs, the authorities indicated that the quality of reporting has improved over the years—notably as a result of FINTRAC's efforts to reach out to REs—and that the information filed is particularly useful for the analysis of individual behaviors and transactional activity. Half of the STRs are sent by MSBs. Banks and credit unions and caisses populaires have submitted more STRs to the FIU in the last two years, but the number of STRs filed by DNFBPs other than casinos, while it has increased as a result of FINTRAC's outreach efforts, remains very low (278 in 2014–2015), including those filed by the real estate sector despite the very high ML risk that it faces.[46]

113. The wide range of systematic reports of transactions above Can$10,000 that FINTRAC receives constitutes an important source of information which has allowed FINTRAC to detect unusual transactions, make links between suspected persons and/or detect bank accounts and other assets held by these persons.

114. Despite the important amount of information received, several factors limit the scope and depth of the analysis that the FIU can do, namely: (i) the fact that some REs listed in the standard are not required to file STRs (in particular legal counsels, legal firms and Quebec notaries)—as a result, FINTRAC does not receive information from key gatekeepers which would otherwise prove useful to its analysis and/or highlight additional cases of potential ML; (ii) the fact that some REs, such as those active in the real estate sector, file few STRs—as a result, information on some areas of high risks is limited; (iii) delays in reporting (FINTRAC supervisory findings seem to confirm that STRs are not filed promptly but within 30 days); and (iv) the fact that FINTRAC is not authorized to request

[46] Regarding the real estate sector, the authorities indicated that an important part of STRs received from banks and credit unions and caisses populaires over the last three years related to suspicions of ML activities in real estate transactions. This compensates partially but not fully the lack of reporting from legal professionals—other than BC notaries (who, although subject to AML/CFT reporting requirements had not filed STRs at the time of the assessment)—who are directly involved in these transactions. Real estate brokers, sales representatives, and developers (when carrying out certain activities) have filed STRs but in very small numbers.

additional information related to suspicions of ML, predicate offenses or TF from any REs—as a result, FINTRAC is largely dependent on what is reported. These factors entail that it is challenging for FINTRAC to follow the flows of potential POC in certain cases. For example, when an STR indicates that suspicious funds have been transferred to another FI, FINTRAC can only follow the trail of particular activities or transactions if other intermediaries and/or the final FI have also filed an STR or another report above the required threshold. This is particularly acute when the funds transferred are divided into multiple transfers below Can$10,000. Enabling FINTRAC to request additional information from REs would considerably facilitate and strengthen the analysis and development of financial intelligence.

Operational Needs Supported by FIU Analysis and Dissemination

115. FINTRAC nevertheless provides a significant amount of financial intelligence to LEAs. Over the years, it has increased the number of disclosures sent to regime partners, both in response to VIRs and proactively. In 2014–15, the FIU sent 2,001 disclosures to partners including the RCMP, CBSA, CRA, CSIS, municipal and provincial police, as well as foreign FIUs. Of these, 923 were associated to ML, while 228 dealt with cases of TF and other threats to the security of Canada. 109 disclosures had associations with all three. Additional statistics provided showed that FINTRAC's disseminations of financial information are appropriately spread between the different provinces.

Table 3. FINTRAC Disclosures to Regime Partners 2/

Year	Municipal Police	Provincial Police	CRA	CSIS	CBSA	CSEC	RCMP	Total
2012–13	182	144	149	164	96	32	580	**1347**
2013–14	207	135	153	243	139	33	703	**1613**
2014–15	331	214	173	312	169	23	779	**2001**

2/ A number of disclosures may have been sent to more than one regime partner.

116. The main predicate offenses highlighted in the disclosures are drugs-related offenses (27 percent of the cases disseminated), frauds (30 percent), and tax evasion (11 percent). Between FY 2010–2011 and 2013–14, the type of predicates was stable.[47] In FY 2014–2015, FINTRAC also provided information pertaining to potential other predicate offenses to ML (namely crimes against persons, child exploitation, prostitution, weapons and arms trafficking, cybercrimes, and illegal gambling).[48] These predicate offenses are in line with the main domestic sources of POC identified in the NRA, except corruption and bribery, counterfeiting and piracy and tobacco smuggling and

[47] The range of predicate offenses related to the cases disclosed were: drugs, fraud, "unknown," i.e., unspecified, tax evasion, corruption, customs/excise violations, theft, human smuggling/trafficking.

[48] The percentage were the following: crimes against persons, 4 percent; child exploitation, 1 percent; prostitution/bawdy houses, 1 percent; weapons/arms trafficking, 1 percent; cyber crimes, 0.3 percent; illegal gambling, 0.3 percent.

trafficking. FINTRAC's disclosures have assisted LEAs in their ongoing investigations in a number of instances, such as in the case of project Kromite described below.

Box 3. Project Kromite

In May 2013, the RCMP participated in an international investigation which focused on significant amounts of heroin being imported from source countries (Afghanistan, Pakistan and Iran) to Tanzania and South Africa. The investigation determined that the heroin was transported through various methods to destinations in Europe, South America, the Far East, Australia, the United States, and Canada. Profits from the distribution and sale of illicit drugs were being collected in Canada and disbursed back to the criminal organization in South Africa and Tanzania.

The RCMP sent VIRs to, and received financial disclosures from FINTRAC. The disclosures were able to identify accounts, businesses owned by the subjects and transactions which led to the identification of relevant banking information and, ultimately, to the identification of targets. The financial intelligence was used by the RCMP to collaborate with the DOJ and the PPSC to draft and issue judicial authorizations. Authorizations took various forms including four MLATs, which were issued to three foreign jurisdictions to provide a formal release of information, and Production Orders and Search Warrants that were used to trace and seize POC, both assets and funds. Formal drug-related charges under the Canada's Controlled Drugs Substances Act were laid. The ML-related component of the investigation has been concluded and potential ML/PPOC-related charges were being prepared at the time of the assessment, but no charges had been laid.

117. FINTRAC tailors its analysis to the LEAs' operational priorities. It focuses mainly on answering the VIRs and also discloses intelligence related to LEAs' priorities. Regular operational meetings[49] and discussions are conducted with disclosure recipients to discuss investigative priorities, analytical processes, the development of indicators, and to provide assistance regarding the use of FINTRAC intelligence. The CSIS Financial Intelligence Center (FIC), which is in charge of all financial Intelligence related to national security investigations and linked notably to terrorism and proliferation, also interacts with FINTRAC on a regular basis.

118. FINTRAC's financial intelligence products include its analysis of all relevant information collected: the information contained in STRs, EFTRs, LCTRs, other reports and other information received or accessed by the FIU are all an integral part for developing case disseminations. As mentioned above, LEAs generally consider that FINTRAC's disclosures provide useful supplements to their investigations and generally meet their operational needs. FINTRAC also uses the information gathered in the exercise of its AML/CFT supervisory function, as well as information from a fair range of law enforcement and administrative databases maintained by—or on behalf of—other authorities, and information from open and public sources. While this broad range of information is undeniably useful, it does not necessarily provide FINTRAC with sufficient information about the suspected person's financial environment. In this context, it would prove particularly useful to ensure that FINTRAC has adequate access, for the purposes of the analysis of STRs, to information collected by the CRA, as this would assist FINTRAC with information that could strengthen its analysis further,

[49] Seventy-six meetings have been laid in 2014–2015 between FINTRAC and different LEAs agencies, including municipal, provincial, and federal agencies, as intelligence services.

such as information about a person's or entity's income and assets, as well as information on trust assets and trustees (see IO.5).

119. In addition to disclosures in response to VIRs and proactive disclosures, FINTRAC produced from FY 2010/11 to 2014/15, 62 strategic intelligence and research products, which identify ML/TF methods and techniques used by listed terrorist groups and criminal networks, emerging technologies, as well as vulnerabilities in different sectors. These reports support the operational needs of competent authorities and many of them are developed in collaboration with the Canadian and international security, intelligence and law enforcement communities. FINTRAC's classified strategic financial intelligence assessments address the nature and extent of ML/TF activities inside and outside of Canada. Canadian authorities provided testimonies of some partners' satisfaction with FINTRAC's strategic intelligence reports.[50]

120. FINTRAC provides a significant amount of disclosures on TF to a variety of LEAs. FINTRAC sent 234 disclosures related to TF and other threats to the security of Canada in 2013–14, and 228 disclosures in 2014–15. These disclosures were communicated to a variety of partner agencies, including CBSA, CRA, CSIS, CSE and RCMP, as well as to municipal and provincial police, and other FIUs, and generated 40 new RCMP TF investigations in 2014 and 126 in 2015. FINTRAC has increased its disclosures regarding TF to 161 for the first six months of FY 2015–2016, of which 82 were proactive disclosures. This increase in the number of disclosure shows the involvement of the FIU in analyzing and disseminating information regarding TF.

Cooperation and Exchange of Information/Financial Intelligence

121. Most agencies adequately cooperate and exchange information including financial intelligence. FINTRAC meets with partners on a regular basis, as seen above, and the FIU focuses on priority investigations to support the LEAs' operational needs. In particular, VIRs constitute an important channel for cooperation and information sharing between FINTRAC and LEAs, as well as between LEAs. FINTRAC may send a single disclosure to multiples agencies simultaneously, which informs LEAs that another agency is working on a case. A LEA can further disseminate a disclosure that was based on another agency's VIR, provided that it obtains the permission from the source agency to further disseminate to the requester. In 2014–2015, FINTRAC was authorized by the source agency to disseminate further its disclosures to another LEA in some 41 percent of cases.

[50] FINTRAC's report, Mass Marketing Fraud: "*Money Laundering Methods and Techniques, is helpful to Canadian law enforcement and government agencies in understanding the complexity and international scope of mass marketing fraud impacting Canada. The CAFC has been able to leverage this report to provide insight into the prominent money laundering techniques used by criminal organizations engaged in mass marketing fraud*" (Canadian Anti-Fraud Centre); "*FINTRAC's report (on terrorism financing risks related to a particular group) … have contributed to AUSTRAC's understanding of the topic … FINTRAC and AUSTRAC have been able to collaborate on analytical products, supporting a multilateral approach to information sharing*" (Australian Transaction Reports and Analysis Centre); "*Public Safety Canada benefits from strategic financial intelligence reports on ML and TF provided by FINTRAC to inform the overall analysis of national security and organized crime issues. Strategic financial intelligence helps Public Safety to identify the nature and extent of money laundering and terrorism* financing and its potential links to *Canada, international conflicts, crimes, sectors and/or organizations, and the growing links between transnational organized crime and terrorism*" (Public Safety Canada).

122. In addition, FINTRAC has direct and indirect access to LEAs and Security (i.e., intelligence services) databases. The authorities indicated that FINTRAC regularly queries LEA databases in the course of its normal work. FINTRAC and LEAs have established privacy and security frameworks to protect and ensure the confidentiality of all information under FINTRAC's control (including information collected, used, stored and disseminated). In October 2013, FINTRAC strengthened its compliance policies and procedures to increase further the protection of the confidentiality of the information it maintains.

123. Where necessary, LEAs also share information indirectly via FINTRAC by highlighting the disclosures that should be disclosed to other agencies: In this respect, the RCMP has, in specific cases, flagged some files with cross border features to the FINTRAC for disclosure to the CBSA where cross border elements. Similarly, the CBSA has advised FINTRAC to disclose the results of certain VIRs to another regime partner where it determined that further investigations should be carried out.

124. Additionally, the CRA—Charities shares information with other government departments, including RCMP, CSIS and FINTRAC, when there are reasonable grounds to suspect the information would be relevant to an investigation of a terrorism offense or a threat to the security of Canada. Similarly, CSIS shares information on security issues with a range of domestic partners, including FINTRAC, on a regular basis. The sharing of intelligence includes financial intelligence.

Overall Conclusions on Immediate Outcome 6

125. Canada has achieved a moderate level of effectiveness for IO.6.

D. Immediate Outcome 7 (ML Investigation and Prosecution)

ML Identification and Investigation

126. ML cases are primarily identified from investigations of predicate offenses, human sources (e.g., informants, victims, suspects, informers, etc.), intelligence (including FINTRAC responses to VIRs), coercive powers, and, in fewer instances, FINTRAC's proactive disclosures, as well as referrals from other government departments without ML investigative powers. LEAs mentioned that they examine all cases with a financial component and assess whether a concurrent financial investigation is warranted. The decisions on whether to investigate a case and how much resources should be devoted to a specific investigation are guided by the LEAs' prioritization processes.[51] As a result,

[51] In the case of the RCMP: The Prioritization Process is designed to aid the judgment of RCMP management in the application of its investigative resources against the most important (priority) criminal threats and activities facing the country. It takes into consideration a series of variables designed to gauge the overall profile of the investigation (or project), its targets, the expected impact against those targets, as well as the expected cost in terms of investigative resources and the length of time they will be dedicated to the project. Prioritization criteria include: economic, political and social integrity of Canada, strategic relevance to RCMP, links to other GoC and partner priorities, etc. Investigations are scored in three tiers (Tier 1 being the highest priority). Highest priority files afforded resources as required to successfully conduct the investigations.

LEAs principally investigate the financial aspects of ML[52] or PPOC[53] occurrences in serious and organized crime cases, and in less serious investigations pursue PPOC charges if proceeds are seized through the predicate investigation.

Table 4. ML and PPOC-Related "Occurrences" 3/
(numbers extracted from all police services' records management systems across Canada)

	2010	2011	2012	2013	2014	Total
ML-Related Occurrences	684	716	596	593	608	3197
PPOC-related Occurrences	42,261	38,796	38,638	37,521	36,012	193,228
Total	**42,945**	**39,512**	**39,234**	**38,114**	**36,620**	**196,425**

Source: Statistics Canada's Uniform Crime Reporting Survey (2015)

3/ The basic unit of this data capture system is an "incident", which is defined as the suspected occurrence of one or more criminal offense(s) during one single, distinct event. During the onsite visit, authorities explained that the ML/PPOC related occurrences are classified when the offenses or incidents fall into the definitions of PPOC/ML under the CC. E.g., a simple theft case can be regarded as a PPOC incident; and if the thief further transfers the stolen good, it will be a ML occurrence.

Table 5. ML/PPOC Occurrences Handled by the RCMP 4/

	2010	2011	2012	2013	2014	Total
ML-Related Occurrences	945	844	692	619	664	3,764
PPOC-Related Occurrences	12,753	11,408	11,573	12,299	14,177	62,210
Total	**13,698**	**12,252**	**12,265**	**12,918**	**14,841**	**65,974**

Source: RCMP

4/ The RCMP figures could be greater than that of all police forces as RCMP figures include "Assistance files," i.e., assistance provided to foreign agency files.

127. The ML/PPOC occurrences handled by RCMP (unlike the numbers provided in the table for all police forces) include 1,599 ML- and 13,179 PPOC-related "assistance files," i.e., cases where the RCMP rendered assistance to foreign agencies. In practice, requests from foreign counterparts are used to a limited extent to identify potential ML cases in Canada. In particular, requests from foreign countries seeking information regarding Canadian bank accounts suspected of receiving or transferring POC are generally only acceded to and a ML investigation initiated when the account holder(s) is/are subject to ongoing investigation(s) in Canada, or there is clear indication of a predicate offense having been committed in Canada. Although Canada has identified third-party ML as one of the very high ML threat, it does not focus sufficiently on foreign requests that may reveal the presence, in Canada, of third-party launderers.

128. As mentioned in IO.6, FINTRAC provides a significant amount of information to LEAs. FINTRAC responses to VIRs (which constitute the majority of FINTRAC's disclosures) and proactive disclosures that have a link with an existing file and/or target are adequately used by LEAs. LEAs

[52] ML encompasses the CC: ss.462.31(1) and (2) for laundering property and proceeds of property.

[53] PPOC includes CC s.354 possession of property of proceeds obtained by crime.

mentioned that due to time and resources considerations, in line with their prioritization process, fewer investigations are initiated on the basis of a proactive disclosure which has no link to an ongoing investigation. Between 2010 and 2014, FINTRAC made 867 proactive disclosures to the RCMP, of which 599 led to new ML/PPOC related occurrences for further investigations.

129. While the CBSA may investigate fiscal crimes, it does not have the powers to investigate related ML/PPOC cases, and in instances where it considers that there are reasonable grounds to suspect that a person is or has been engaging in ML activities, it reports the case to the RCMP. The latter recorded that between 2010 and 2014 there were 444 ML/PPOC occurrences related to cross border currency reporting. The authorities provided one case ("Project Chun," described in the Box below) of a successful ML investigation started in 2002 on the basis of a CBSA referral. Whilst the assessment team was also shown several ML cases involving parallel investigations arising from CBSA's enquiries into smuggling or customs related offenses, no other cases arising from CBSA's cross-border declaration/seizure reports were provided. It therefore appears that, in practice, information collected at the border is analyzed or investigated with a view to pursuing ML activities to a very limited extent only. The cross-border declaration system is not adequately used to identify potential ML activities.

Box 4. Case Study: Project Chun

In October 2002, a male was intercepted at the Montreal International Airport with US$600,000 cash in his hand luggage. In the absence of a valid explanation, the money was seized and the case was referred to RCMP which initiated an investigation to determine the source and destination of the money. Extensive enquiries unveiled that the male and his wife owned two currency exchange companies in Canada and in 2000 they made an agreement with a drug trafficker to assist the latter in laundering proceeds deriving from drug trafficking activities. The laundering included use of various financial services and an elaborate scheme for the transfer of money to a bank in Cambodia that was owned and controlled by the couple. The precise amounts involved in these activities are estimated at more than Can$100 million. Information received from FINTRAC indicated that the couple dealt in large sums of cash and that their bank account activities did not fit their economic profiles. Travel records of one of the accomplice money launderers were received from Cuba through MLAT requests. The accomplice, who was detained in custody in the U.S., was later transferred from the U.S. to Canada to provide testimony for the prosecution. Canadian investigators had travelled to Israel and Cambodia for tracing after and restraining the crime proceeds. The couple applied delaying tactics during the prosecution and the Canadian authorities eventually convicted the couple with six counts of Money Laundering and seven counts of tax offenses. In March 2015, the couple was each sentenced to eight years of imprisonment and ordered to pay fines of Can$9 million. Two real properties, US$600,000 and the shares of a bank in Cambodia were forfeited.

130. Canada's main law enforcement policy objective is to prevent, detect and disrupt crimes, including ML, but in practice, most of the attention is focused on securing evidence in relation to the predicate offense and little attention is given to ML, as evidenced by the discussions held as well as by the case studies provided. LEAs focus on criminal actions undertaken by OCGs (i.e., mainly drug-related offenses and fraud). Cases studies and figures provided by LEAs demonstrated that they also investigate other high-risk offenses (e.g., corruption and tobacco smuggling), but to a limited extent only. Insufficient efforts are deployed in pursuing the ML element of predicate offenses and pursuing ML without a direct link to the predicate offense (e.g., third-party/professional money

launderers). Since 2010, when tax evasion became a predicate offense to ML, none of the tax evasion cases finalized by the CRA have included sanctions for ML. There are, however, ongoing investigations that contemplate the ML activities.

131. The various LEAs adequately coordinate their efforts, both at the strategic level and at the operational and intelligence levels, through working groups and meetings. Within the RCMP, a centralized database is used to minimize the risk of duplicative investigative efforts against the same groups or persons. Direct exchanges regularly occur during relevant LEAs meetings, as well as through specific joint projects: in particular, the CRA-CID and the RCMP have entered into special projects (i.e., Joint Forces Operations, JFOs) for a specific duration, to identify targets of potential criminal charges including ITA/ETA offenses. Between 2010 and 2015, 10 JFOs were conducted. In these cases, the JFO agreements do not supersede or override the confidentiality provisions of the ITA/ETA, but they, nevertheless, enable the CRA to provide tax information to the RCMP if this is reasonably regarded as necessary for the purposes of the administration and enforcement of the Acts.

132. LEAs regularly seek the production of a court order to obtain banking (or other relevant) information for the purposes of their investigations. However, as detailed in R.31.3 and IO.6, the length of the process leading to the identification of relevant accounts considerably delays the tracing of POC in ML/PPOC investigations.

133. The LEAs also access tax information (outside JFOs) with prior judicial authorization. During the period April 1, 2013 to December 31, 2015, the CRA CID received in excess of 2500 LEA requests for taxpayer information. One RCMP unit indicated that this information is obtained in all significant cases by way of letter under s.241 of ITA when charges are laid or by CC authorization of Tax order. The RCMP sent 91 tax letters from 2010 to 2016.

134. LEAs also regularly consult public registries of land and companies, but the paucity of accurate basic and beneficial ownership information in these registries limit the usefulness of the information obtained. Investigations in Canada typically do not focus on complex ML cases involving corporate structures (and/or involving transnational activities). LEAs stated that, in the few cases where legal entities were under investigation, the beneficial ownership information was typically obtained from FIs, in particularly the D-SIBs. Investigators are aware of the risk of misuse of corporate entities in ML schemes, but, in some provinces, do not investigate such cases to the extent that they should mainly because of a shortage of adequate resources and expertise. As a result, some targets are not pursued or bank accounts investigated (e.g., in instances where multiple targets and accounts are involved), and LEA efforts are focused on easier targets where the chances of the investigations being cost effective are greater.

Consistency of ML Investigations and Prosecutions with Threats and Risk Profile, and National AML Policies

135. According to the NRA, fraud, corruption, counterfeiting, drug trafficking, tobacco smuggling, and (although a recent phenomenon) third-party ML pose very high ML threats in

Canada. The LEAs generally agreed with the NRA findings and have prioritized their resources on OCGs, which are mostly involved in drug and fraud related offenses (see table below). As described above, LEAs, in particular the RCMP, have a prioritization process, which is continually evolving to address the current threats, taking into account a number of factors. At the time of the assessment, that process did not take the NRA's findings sufficiently into account.

Prosecuted ML-Related Cases	**2010**	**2011**	**2012**	**2013**	**2014**	**Total**	**%**
Money Laundering (CC s.462.31)	88	86	130	108	114	526	51.2%
Fraud	12	27	57	61	53	210	20.4%
Drug Offenses	14	18	9	14	14	69	6.7%
Others	27	52	45	51	47	222	21.6%
Total	**141**	**183**	**241**	**234**	**228**	**1027**	**100.0%**
Source: Statistics Canada's Uniform Crime Reporting Survey (UCR)—all police services' records							

Prosecuted PPOC-Related Cases	**2010**	**2011**	**2012**	**2013**	**2014**	**Total**	**%**
PPOC (CC 354, 355)	11930	11955	11179	10904	10292	56260	37.7%
Drug Offenses	4260	4351	4504	4020	3889	21024	14.1%
Fraud	3013	2690	2467	2352	2144	12666	8.5%
Others	13144	12602	12079	11656	9638	59119	39.7%
Total	**32347**	**31598**	**30229**	**28932**	**25963**	**149069**	**100%**
Source: Statistics Canada's Uniform Crime Reporting Survey (UCR)—all police services' records							

136. The authorities provided in the above tables the number of prosecution cases, broken down by the most serious offense (MSO) of the case, in which at least one ML or PPOC charge was laid in 2010 to 2014.[54] This information does not distinguish third-party ML from self-laundering. These statistics show that high-threat predicate offenses, i.e., drug trafficking and fraud, account for 27.1 percent of ML or 22.6 percent of PPOC prosecutions only, which does not match the ML threats and risks identified in the NRA (which suggest that a higher percentage would be necessary to mitigate the risks). The figures provided do not show related prosecutions in the context of corruption, counterfeiting, and tobacco smuggling cases, but these cases could be embedded in the "others," "ML," or "PPOC" categories, when they were not the MSO. Canada provided further information to show that there were 68 counterfeiting related ML/PPOC cases, examples of tobacco smuggling related ML cases and one case (Project LAUREAT highlighted below) of a successful prosecution of corruption-related[55] ML cases.

[54] RCMP also provided that between 2010 and 2014, it laid 130,630 PPOC charges against 35,600 persons and 1904 ML charges against 503 persons.

[55] Two other corruption-related ML cases, Project Ascendant and Project Assistance, were provided but both cases were under court proceedings.

Box 5. Case Study: Project LAUREAT

In 2010, in order to obtain the Can$1.3 billion contract of modernization of a Health Centre ("HC"), the president ("P") and vice-president ("VP") of an engineer company ("EC") had bribed the top officials, "Y" and "Z," of the HC to get the award. Upon the announcement of the award to EC, the VP transferred a total of Can$22.5 million to the shell companies in foreign countries owned by Y and Z. Y further transferred the crime proceeds to the accounts of his wife's (Y's wife) shell companies. Numerous MLAT requests were executed and bank accounts in nine other countries, worth more than Can$8.5 million, were blocked. Y, Z, P, VP were also extradited from other countries. The syndicate was charged with corruption, fraud, ML along with other offenses. For Y's wife, who has only been involved in laundering the Can$22.5 million, was sentenced to 33 months of imprisonment.[56] Upon her conviction, seven buildings (value at Can$5.5 million) were confiscated.

137. While Project LAUREAT was relatively successful, overall, on the face of the statistics and cases provided as well as of the discussions held onsite, it was not established that Canada adequately pursues ML related to all very high-risk predicate offenses identified in the NRA.

138. As indicated in the statistics on standalone ML/PPOC prosecutions below, there were 35 (3.4 percent) and 14,271 (9.6 percent) standalone ML and PPOC concluded respectively in the last five years. As professional money launderers are mostly involved in ML (rather than PPOC) cases, the fact that Canada only led 35 prosecutions and obtained 12 convictions of single-charge ML cases in the last five years is a concern. It is possible and, according to the authorities, very likely that a professional money launderer would also be charged with another charge such as conspiracy, fraud, or organized crime in addition to ML, but the numbers nevertheless appear too low in light of the risk.

Table 6. Results of Single Charge ML Cases

	2010	2011	2012	2013	2014	Total	%
Guilty	2	2	4	3	1	12	34.3%
Acquitted	0	0	0	0	1	1	2.9%
Stayed	0	1	3	1	0	5	14.3%
Withdrawn	2	4	4	2	2	14	40.0%
Other decisions	0	0	1	0	2	3	8.6%
Total	**4**	**7**	**12**	**6**	**6**	**35**	**100%**

Source: Statistics Canada's Integrated Criminal Court Survey (ICCS)

Table 7. Results of Single Charge PPOC Cases

	2010	2011	2012	2013	2014	Total	%
Guilty	1332	1199	1108	1017	947	5603	39.3%
Acquitted	115	84	76	127	98	500	3.5%
Stayed	589	642	640	611	581	3063	21.5%
Withdrawn	1158	1077	1022	904	806	4967	34.8%

[56] The sentence of Y's wife expires in December 2016, but she was granted full parole in September 2015.

Other decisions	53	23	24	23	15	138	1.0%
Total	**3247**	**3025**	**2870**	**2682**	**2447**	**14271**	**100%**
Source: Statistics Canada's Integrated Criminal Court Survey (ICCS)							

139. Canada's NRA also identified very high ML vulnerabilities in the use of trusts and corporations. LEAs confirmed that corporate vehicles and trusts are misused to a relatively large extent for ML purposes. As the case study Dorade (below) indicates, the authorities have been successful in identifying the legal persons and arrangements involved in the ML schemes and in confiscating their assets in some instances. However, overall, it was clear from the discussions held with police forces and prosecutors that legal persons are hardly ever prosecuted for ML offenses, mainly because of a shortage of adequate resources and expertise. Investigators are nevertheless aware of the risk of misuse of corporate entities in ML schemes and that more focus should be placed on this risk.

Box 6. Case Study: DORADE

During the investigation of a fraud syndicate, it was revealed that the director of a loan company had set up, with the assistance of various professional accomplices, foreign shell companies located in tax havens for receiving the crime proceeds and lending the sum back to loan company for its legitimate loan business, thereby facilitating the director to evade tax payment and recycle crime proceeds. It was estimated, between 1997 and 2010, a total of Can$13 million of tax was evaded. With the assistance of MLAT requests, the syndicate members were identified and the proceeds, whether domestic or abroad, were restrained and eventually confiscated. The director and the professionals were convicted of fraud and ML and sentenced to 36–84 months of imprisonment. However, all the ML charges attracted an imprisonment term of less than 18 months and to be served concurrently with the Fraud sentence.

140. Overall, while there are exceptions, law enforcement efforts are not entirely in line with Canada's NRA risk profiles. As previously noted, LEAs' prioritization processes place strong attention to National Security investigations, OCGs, and, to a lesser extent, more recently third-party ML in an international context. Other instances of high threat predicate offenses, especially fraud, corruption, counterfeiting, tobacco smuggling, and related ML, as well as laundering activities in Canada of the proceeds of foreign predicate offenses, third-party ML and ML schemes involving corporate structures are not adequately ranked in the prioritization process and, consequently, are not pursued to the extent that they should.

Types of ML Cases Pursued

141. Different types of ML and PPOC cases are prosecuted, but there is insufficient focus on the types of ML that are more significant in Canada's context, i.e., ML related to high-risk predicate offenses. In addition, prosecutions of ML-related cases focus on the predicate offenses, with the ML charge(s) often withdrawn or stayed after plea bargaining and re-packaging of charges. The number of standalone ML cases is comparatively low, indicating few investigations and hence prosecutions of third-party ML and foreign predicate offenses despite their high ranking in the NRA. According to the authorities, as far as third-party ML is concerned, the low number of investigations and prosecutions is that the magnitude of the threat has only recently reached a high level. Finally, legal

persons are frequently misused for ML purposes, but not often pursued for ML offenses. The tables below show the results of ML cases brought before the courts and the charges laid in these cases.

Table 8. Results of ML-Related Cases

	2010	2011	2012	2013	2014	Total	%
Guilty	82	108	140	136	146	612	59.6%
Acquitted	2	0	0	4	7	13	1.3%
Stayed	8	12	15	26	18	79	7.7%
Withdrawn	49	63	74	64	53	303	29.5%
Other Decisions	0	0	12	4	4	20	1.9%
Total	**141**	**183**	**241**	**234**	**228**	**1027**	**100%**

Source: Statistics Canada's Integrated Criminal Court Survey (ICCS)

Table 9. Results of ML-Charges

	2010	2011	2012	2013	2014	Total	%
Guilty	38	21	35	31	44	169	9.4%
Acquitted	5	1	8	6	9	29	1.6%
Stayed	17	26	144	45	31	263	14.6%
Withdrawn	132	190	366	327	294	1309	72.7%
Other Decisions	2	2	14	7	5	30	1.7%
Total	**194**	**240**	**567**	**416**	**383**	**1800**	**100%**

Source: Statistics Canada's Integrated Criminal Court Survey (ICCS)

142. Between 2010 and 2014, a total of 1,800 ML charges were concluded in 1,027 cases. Although about 60 percent of these cases were led to convictions, only 169 ML charges (i.e., some 9 percent) resulted in a conviction. Some 87 percent of the ML charges were either withdrawn or stayed. The reasons provided for the withdrawal of the ML charges included insufficient evidence, the lack of public interest in the pursuit of the charges, the avoidance of overcharging, as well as repackaging of charges and plea bargaining (as the ML/PPOC charge will not normally add any additional sentence to the defendant and it is easier for the defendant to accept the guilty plea of the predicate offenses in order to contribute to a fair and efficient criminal justice system). The consultation with prosecutors at an earlier stage of the ML cases is clearly useful in securing the necessary evidence and avoiding a waste of investigative efforts. The length of criminal proceedings in ML cases is also a concern. Proceedings may take a number of years during which the subjects of the investigation and prosecution may continue their unlawful businesses and dispose of the POCs (as was the case in Project Chun for example).

143. Over the last years, although 68.4 percent of PPOC cases resulted in convictions, 74.6 percent of the PPOC charges were withdrawn/stayed or dealt with by other means, and the defendants were only charged with and convicted of the predicate offenses.

Table 10. Results of PPOC-Related Cases							
	2010	**2011**	**2012**	**2013**	**2014**	**Total**	**%**
Guilty	22,974	21,728	20,525	19,611	17,191	102,029	68.4%
Acquitted	388	349	339	404	391	1871	1.3%
Stayed	2,769	3,193	3,157	3,148	2,857	15,124	10.1%
Withdrawn	5,961	6,140	6,021	5,606	5,380	29,108	19.5%
Other Decisions	255	188	187	163	144	937	0.6%
Total	**32,347**	**31,598**	**30,229**	**28,932**	**25,963**	**149,069**	**100%**
Source: Statistics Canada's Integrated Criminal Court Survey (ICCS)							

Table 11. Results of PPOC-Related Charges							
	2010	**2011**	**2012**	**2013**	**2014**	**Total**	**%**
Guilty	13,493	12,782	11,178	10,996	10,072	58,521	23.6%
Acquitted	736	715	1,716	674	817	4,658	1.9%
Stayed	9,178	9,715	9,183	9,132	6,894	44,102	17.8%
Withdrawn	28,776	28,388	27,402	27,375	25,130	137,071	55.2%
Other decisions	1,120	912	883	753	416	4,084	1.6%
Total	**53,303**	**52,512**	**50,362**	**48,930**	**43,329**	**248,436**	**100%**
Source: Statistics Canada's Integrated Criminal Court Survey (ICCS)							

144. Overall, of the 1,027 ML-related cases and 102,029 PPOC-related cases that entered the court system, over 60 percent resulted in convictions, though most of the defendants were convicted of the predicate offenses rather than the ML or PPOC charges. This indicates that Canada is able to investigate and prosecute predicate offenses in ML/PPOC-related cases and disrupt some of the ML/PPOC activities. One hundred sixty-nine ML charges were led to a conviction in the past five years (i.e., 33.8 charges on average annually), which appears very low in light of the magnitude of the ML risks identified. Canada does not pursue the ML charges sufficiently.

Effectiveness, Proportionality and Dissuasiveness of Sanctions

145. The totality principle[57] always applies in the sentencing, and a ML/PPOC sentence is usually ordered to be run concurrently with the predicate offenses. The statistics below indicate the sanctions imposed for ML in instances where the ML charges were the most serious offenses (MSO). The vast majority of natural persons (i.e., 89 percent) convicted for ML have been sentenced in the lower range of one month to two years of imprisonment or awarded non-custodial sentences.[58] This is proportionate with the type of ML activities most frequently pursued in Canada. However,

[57] Totality principle is a common law principle, which applies when a court imposes multiple sentences of imprisonment. Section 718.2(c) of the CC stipulates that when a court that imposes a sentence shall take into consideration of, amongst others, where consecutive sentences are imposed, the combined sentence should not be unduly long or harsh.

[58] A breakdown of sanctions for third-party ML cases and against legal persons is not available.

although this is not made evident in the statistics provided, it is apparent from the case examples provided, and in Projects Dorade and Laurent mentioned above, that many sanctions imposed on money launderers are low even in the (relatively few) cases of complex ML schemes and/or of professional launderers brought before the courts. None of the PPOC convictions attracted a sentence of more than two years. In these circumstances, the sanctions applied do not appear to be of a level dissuasive enough to deter criminals from ML activities.

Table 12. Sanctions in ML Cases Where ML was the Most Serious Offense, from 2010 to 2014 5/

	Number	Percentage
Custodial Sentence	80	55.2%
• Less than 12 months	47	32.4%
• 12 to 24 months	17	11.7%
• More than 24 months	16	11.0%
Conditional sentence, probation, fine, restitution	65	44.8%
Total	**145**	**100.0%**

5/ There are other undisclosed cases where the ML offense runs concurrently with another MSO.

Extent to Which Criminal Justice Measures are Applied Where Conviction is Not Applicable

146. Information provided under IO.8 reveals that non-conviction based forfeiture amounted to 17 percent of the total forfeiture. Whilst it is not encouraged to drop the criminal charges during the judicial process, Canada's use of civil confiscation is not to be discounted. Plea bargaining and repackaging of charges have also been used in the prosecution stage for shortening the length of court proceedings.

Overall Conclusions of Immediate Outcome 7

147. Canada has achieved a moderate level of effectiveness for IO.7.

E. Immediate Outcome 8 (Confiscation)

148. Since its last assessment, Canada improved its ability to collect information on seizures and confiscations and produce related statistics. It uses both criminal and civil (non-criminal based) proceedings to confiscate proceeds and property related to an unlawful activity. At the Federal level, there is an agency to manage seized and confiscated assets (SPMD). At the provincial level, the management of these assets rests with the prosecution services. Canada also confiscates with no terms of release any undeclared currency and monetary instruments from travelers entering and exiting the country when there is reasonable ground to suspect they are from illicit origin or that the funds are intended for use in the financing of terrorist activities. It shares confiscated assets with countries with which it has a sharing agreement.

Confiscation of Proceeds, Instrumentalities and Property of Equivalent Value as a Policy Objective

149. While confiscation of criminal proceeds and instrumentalities is a policy objective, that objective is pursued to some extent only. Canada is not able to confiscate property of equivalent value; instead, it imposes fines in lieu. As a result of the deficiencies described in IO.7 confiscation relate mainly to proceeds of criminal activities and offence related property conducted by OCGs, in particular drug offenses, fraud, theft, and to the proceeds of tax evasion.

150. Canada's Integrated Proceeds of Crime (IPOC) Initiative aims at the disruption, dismantling, and incapacitation of OCGs by targeting their illicit proceeds and assets. It brings together the CBSA, CRA, PPSC, Public Safety Canada, PSPC (more specifically, its Forensic Accounting Management Group, and the Seized Property Management Directorate), and the RCMP, which cooperate and share information to facilitate investigations. According to the authorities, the IPOC is a distinct program and a corner stone of the AML/CFT regime as a whole as modified in 2000. However, it is not identified as one of the key goals of the latest articulation of the AML/CFT program.

151. The RCMP's Federal Policing Serious and Organized Crime/Financial Crime Teams (which investigate ML cases) target the proceeds of organized crime for seizure. The return of frozen or seized POC and instrumentalities to the defendant is avoided in the context of a plea bargain; in line with the PPSC policy, both POC and instrumentalities must be sought.[59] According to the authorities, the accused normally agree with the confiscation request when they plead guilty. At the provincial level, measures aimed at tracing and seizing assets in view of confiscation are in some cases conducted jointly by the RCMP and the provincial LEA. In the province of Quebec, for instance, the cooperation between the RCMP and the relevant provincial police, i.e., the Sûreté du Quebec, has shown a number of cases of successful recovery of assets. At the municipal level, the Service de Police of the City of Montreal has a unit specialized in the recovery of POC and in the investigation of ML (Unité des produits de la criminalité—Programme UPC-ACCEF). The priority of the investigations in Quebec and in Montreal in particular is clearly to identify assets for confiscation, especially in cases involving OCGs. These clear priorities and effective specialized units have resulted in greater recovery of POC and instrumentalities by criminal law means both in scope and in type of assets, including in more complex ML cases. Other provinces rely more on non-conviction based forfeiture, where roughly Can$100 million have been confiscated, nationally, during the relevant period.

152. As a general rule, however, LEAs in other provinces and at the federal level do not seem to adopt a "follow the money" approach in practice, nor to initiate a parallel financial investigation,

[59] According to the PPSC Deskbook, Guideline issued by the Director under Section 3(3)(c) of the Director of Public Prosecutions Act, Chapter 5.3 Proceeds of Crime, in the context of ORP, "partial forfeiture is not a negotiation tool. If the facts justify and application for total forfeiture, Crown counsel may not, as part of negotiations, suggest partial forfeiture."

notably because of resource constraints. Overall, as a result of the shortcomings explained under IO.6 and IO.7, asset recovery is pursued to a limited extent only.

Confiscations of Proceeds from Foreign and Domestic Predicates, and Proceeds Located Abroad

153. The total amounts recovered yearly have increased significantly since the previous assessment,[60] but, nevertheless, appear to be low in the Canadian context (see table below). This is likely to be due to the lack of focus on asset recovery mentioned above and the shortcomings mentioned in IO.6 and IO.7, as well as the length of time needed to bring cases to closure: The delays encountered (especially at the tracing stage) are likely to encourage and facilitate the flight of assets.

Table 13. Amounts Forfeited in Canada 6/

	Criminal Federal Forfeiture	Federal Fines in Lieu	CBSA Cash Forfeitures	Civil Forfeiture Results (Nationally)	Québec Criminal Provincial Forfeiture	Total
2009/10	46,368,327	101,600	5,277,676	7,600,000	---	59,347,604
2010/11	58,872,881	71,650	4,698,404	12,400,000	9,070,456.	85,113,392
2011/12	77,698,566	31,700	1,960,038	18,900,000	10,905,959	109,496,264
2012/13	83,935,230	105,939	3,468,888	41,700,000	11,498,811	140,708,870
2013/14	75,997,602	312,178	4,054,089	18,900,000	12,453,244	111,717,114
2014/15	72,869,240	314,217	4,076,586	---	---	77,260,044
Total In Can$	$415,741,848	$937,285	$23,535,683	$99,500,000	$43,928,471	$583,643,289

6/ The table is a consolidation of statistics maintained by different authorities, using different criteria and does not include forfeitures undertaken by federal departments that do not involve or are not reported to the SPMD. At the provincial level, figures were provided for Quebec only (federal criminal results for Quebec appear in the first column). They do not differentiate domestic from foreign predicate offenses (though IO.2 shows that there have been forfeitures based on the direct enforcement of foreign orders) and proceeds which have moved to other countries. According to the authorities, the link between seized and forfeited assets cannot easily be made, as these actions occur over multiple years.

154. Different types of assets are seized or restrained in federal criminal proceedings (see table below) but, overall, Canada does not restrain businesses, company shares—despite the high risk of misuse of legal entities—or property rights.[61] In general, Canadian authorities seem to be managing effectively the seized and confiscated assets on both federal and provincial levels. Assets are generally not sold before the conclusion of the criminal proceeding to maintain their value or

[60] An average of Can$27 million a year were forfeited from 2000 to 2007 (2008 MER, page 62).

[61] The only exception appears to be a golf course seized on behalf of another country.

reduce the costs of management of the property, unless they are rapidly depreciating or perishable, or the accused authorizes their disposal.

Table 14. Federally Seized/Restrained Assets by Appraisal Value						
Asset Type	**2009/2010**	**2010/2011**	**2011/2012**	**2012/2013**	**2013/2014**	**2014/2015**
Aircraft	$108,000	$ -	$15,000	$ -	$250,000	$0
Cash	$20,878,443	$21,456,803	$22,665,264	$28,833,075	$18,036,703	$21,680,932
Financial Instruments	$365,247	$961,557	$5,938,052	$732,443	$26,924,056	$723,834
Hydroponics	$6,291	$2,748	$808	$1,240	$259	$12
Other Property (incl. jewelry)	$138,410	$684,780	$605,054	$274,601	$203,956	$269,866
Real Estate	$52,785,401	$54,220,901	$37,336,935	$25,445,169	$26,532,406	$16,758,250
Vehicle	$5,940,355	$5,947,937	$6,256,389	$4,839,410	$4,479,067	$4,433,720
Vessel	$311,200	$156,101	$79,296	$121,661	$39,700	$518,000
Grand Total	**$80,533,349**	**$83,430,829**	**$72,896,801**	**$60,247,601**	**$76,466,149**	**$44,384,616**

155. Revenue agencies, both at the federal and provincial level, have been successful in recovering evaded taxes, including in instances where the monies were held offshore. In FY 2013/2014, Revenue Quebec alone recuperated over Can$3.5 billion of evaded taxes, both by criminal sanctions and civil compliance actions. During the same period, FY 2013/2014 the CRA recuperated Can$10.6 billion in its criminal and civil actions. As a result of the CRA's investigations into suspected cases of tax evasion, fraud and other serious violations of tax laws, and recommendations to the PPSC, Canada secured convictions for tax crimes for Can$162.3 million and levied a total of Can$70.7 million in criminal fines. However, it should be noted that these figures do not solely represent confiscations related to the proceeds of crime, and that the Canadian authorities were unable to provide such separate figures.

156. Between 2008 and 2015, in an effort to recover proceeds that have been moved to other countries, Canada sent 135 requests for tracing assets (bank or real estate records) to other countries 43 requests for restraint of funds or assets and 4 requests for forfeiture. Discussions with the authorities and the cases provided nevertheless established that the authorities pursue assets abroad to some extent only, notably because such actions require resources that are currently dedicated to other priorities. The fact that LEAs seem to have little expertise in pursuing complex international ML schemes or in the investigation of professional money launderers also explain the relatively low level of effort in seeking the recovery of assets abroad. Considering that there is no possibility for the authorities to seize property of equivalent value, when POC cannot be forfeited, fines in lieu are ordered, in addition to the custodial sentence. The total fines collected by the

federal Crown are Can$937,285.95 for 2009–2015. The authorities share parts of the confiscated assets with their foreign counterparts, both in criminal and civil actions, when the property is in Canada, the foreign country assisted Canada in the case and there is a signed sharing agreement. This would be the case when the offense was committed partly or entirely abroad and laundered in Canada.[62] The major part of the sharing occurred with the U.S., which appears justified in the Canadian context, and property was also shared with Cuba and the U.K.

Confiscation of Falsely or Undeclared Cross-Border Transaction of Currency/BNI

157. CBSA agents seize monies when there is a suspicion that the latter are POC or funds intended to be used to fund terrorism. As indicated in the table below, between 2009 and 2015, Canada seized about Can$263 million at the border, of which less than 9 percent were confiscated and more than 91 percent were returned to the travelers. In the latter cases, according to the authorities, there was no suspicion of ML, TF, or other illicit activities; therefore, the monies were returned to the traveler and an administrative fixed fine (of Can$250, Can$2,500, or Can$5,000) levied. In practice, however, falsely or undeclared cross-border movements of currency and other bearer negotiable instruments are analyzed by the FIU, or investigated by the RCMP to a very limited extent, namely only when they pertain to an ongoing analysis or investigation (see IO.6). Moreover, the level of the sanctions for noncompliance with the obligation of disclosure of cross-border movements and the frequency which it is applied does not seem effective, proportionate nor dissuasive.

FY	Seized Amount	Returned at Seizure by CBSA	Final Penalty Amount Forfeited	Cash Seizures Forfeited	Amount Returned by SPMD[63]
2009/2010	$99,430,742	$94,448,985	$2,150,500	$5,277,676	$731,782
2010/2011	$12,447,605	$6,277,108	$223,000	$4,698.404	$1,458,233
2011/2012	$4,361,463	$1,871,650	$50,750	$1,960,038	$522,035
2012/2013	$28,273,318	$23,949,256	$545,500	$3,468,888	$853,173
2013/2014	$52,508,920	$47,564,857	$1,340,000	$4,054,089	$873,782
2014/2015	$65,989,388	$61,808,579	$1,732,000	$4,076,586	$1,328,046
Total	$263,011,436	$235,920,435	$6,041,750	$23,535,681	$5,767,054

[62] Canada shared the following amounts: 2007/2008: Can$199,390; 2008/2009: Can$75,620; 2009/2010: Can$357,844; 2010/2011: Can$0; 2011/2012: Can$93,013; 2012/2013: Can$237,577; 2013/2014: Can$244,846.

[63] This column contains only the amounts for closed cases where an appeal or other legal means of challenging are no longer available to the travelers.

Consistency of Confiscation Results with ML/TF Risks and National AML/CTF Policies and Priorities

158. Law enforcement actions, including asset recovery efforts focus mostly on illicit drug trafficking, fraud, and theft.[64] While drug-related offense and fraud are identified as very high ML threats in Canada's NRA, theft is not. In addition, the recovery of proceeds of other very high threats identified in the NRA is pursued, but not to the same extent (this is notably the case for proceeds of corruption and bribery, third-party ML, and tobacco smuggling, although some success was achieved in a case of tax evasion perpetrated from 1991 to 1996 in relation to a large scale tobacco smuggling operation.)[6566] As a result, Canada's confiscation results are not entirely consistent with ML/TF risks or national AML/CFT policy.

Overall Conclusions on Immediate Outcome 8

159. Canada has achieved a moderate level of effectiveness in Immediate Outcome 8.

[64] As stated in the Research Brief-Review of Money Laundering Court Cases provided by FINTRAC, p.1 and the Authorities Submissions to IO.7, p.12 and 13. This is consistent with the assessor's findings after the interviews with Canadian authorities during the onsite.

[65] Project Oiler, where charges of tax fraud (through smuggling) and the possession of proceeds of crime were laid in 2003 and ultimately a plea of guilty accepted for violations of the Excise Tax Act in 2008 and 2010. This case resulted in the imposition of criminal fines and penalties totaling Can$1.7 billion.

[66] The authorities provided the assessment team with a table showing the seizures in relation to the offenses (Seizures by Act), from 2009 until 2015. The higher values are related to the Controlled Drug and Substance Act, followed by the offense of Possession of property obtained by crime, laundering of proceeds, PCMLTFA, tax offenses and conspiracy. The values seized in relation to bribery of officers are insignificant (except in one case where some Can$4 million were confiscated). It is not possible to identify third-party ML in the statistics provided. Seizures for possession of tobacco appear only in fiscal years 2012/2013 and 2013/2014, and seizure for bribery of officers appear only in FY 2010/2011, 2011/2012 and 2013/2014. In FY 2009/2010, 2012/2013 and 2014/2015 the value of seizures in relation to bribery is zero.

TERRORIST FINANCING AND FINANCING OF PROLIFERATION

A. Key Findings

IO.9

The authorities display a good understanding of TF risks and close cooperation in CFT efforts. The intelligence services, LEAs and FINTRAC regularly exchange information, which notably contributes to support prioritization of TF investigations.

Canada accords priority to pursuing terrorism and TF, with TF investigation being one of the key components of its counter-terrorism strategy.

The RCMP duly investigates the financial components of all terrorism-related incidents, considers prosecution in all cases and the prosecution services proceed with charges when there is sufficient evidence and it serves the public interest. Two TF convictions were secured since 2009. Sanctions imposed were proportionate and dissuasive.

Canada also makes frequent use of other measures to disrupt TF.

IO.10

Implementation of TF-related targeted financial sanctions (TFS) is quite effective for FIs but not for DNFBPs.

Canada takes a RBA to mitigate the misuse of NPOs (i.e., charities). A specialized division within CRA-Charities focuses specifically on concerns of misuse of organizations identified as being at greatest risk. In addition, CRA-Charities has developed an enhanced outreach plan, which reflects the best practices put forward by the FATF.

In practice, few assets have been frozen in connection with TF-related TFS.

IO.11

Canada's Iran and DPRK sanction regimes are very comprehensive and in some respects go beyond the UN designations.

Cooperation between relevant agencies is effective and some success has been achieved in identifying and freezing the funds and other assets belonging to designated individuals.

Large FIs have a good understanding of their TFS obligations and implement adequate screening measures but some limit their screening to customers only. DNFBPs, however, are not sufficiently aware of their obligations and have not implemented TFS.

There is no formal monitoring mechanism in place; while some monitoring does occur in practice, it is limited to FRFIs and is not accompanied by sanctioning powers in cases of non-compliance.

B. Recommended Actions

Canada should:

IO.9

- Pursue more and different types of TF prosecutions.

IO.10

- Require DNFBPs to conduct a full search of their customer databases on a regular basis.
- Consider increasing the instances of proactive notification of changes to the lists to REs other than FRFIs.
- Consider enhancing the number of seizures and confiscations related to TF offenses.

IO.11

- Monitor and ensure FIs' and DNFBPs' compliance with PF-related obligations.
- Conduct greater outreach. This should include information on the PF-risk that can be published without compromising Canada's security, as well as more detailed guidance on the implementation of TFS and indicators of potential PF activity.

The relevant Immediate Outcomes considered and assessed in this chapter are IO.9–11. The recommendations relevant for the assessment of effectiveness under this section are R.5–8.

C. Immediate Outcome 9 (TF Investigation and Prosecution)

Prosecution/Conviction of Types of TF Activity Consistent with the Country's Risk-Profile

160. The RCMP investigates all occurrences of TF. This includes investigations into a wide range of TF activities, such as the collection of funds and their movement and use by individual, entities or wider organizations. The RCMP lays TF charges when approved by PPSC based on sufficient evidence and when the prosecution would best serve the public interest. Between 2010 and 2015,

charges were laid against one individual, resulting in a conviction for TF in 2010 (see Box 7 below). Charges were also laid in another case, but subsequently withdrawn for tactical and operational enforcement reasons.

Box 7. R v. THAMBITHURAI 2008

It came to the knowledge of the RCMP's Integrated Security Enforcement Team (INSET) that a man was in the process of collecting funds from his place of residence and businesses for the Liberation Tigers of Tamil Eelam (LTTE), a listed terrorist entity in Canada. The person was arrested in Vancouver. INSET found various materials in his possession, including donation forms for the LTTE which were used for a Can$600 donation and a Can$300 pledge. The accused was charged with four counts of "Providing or making available property for a terrorist organization" under CC 83.03, three of which were later withdrawn. He pled guilty in 2010 and was sentenced to six months of imprisonment.

161. LEAs actively pursue the threat of individuals radicalized to violence, and in particular, those seeking to travel abroad for terrorist purposes. The RCMP's priority is to pursue charges that are in the best interest of public safety, and to mitigate the possible threat of terrorist activity as efficiently as possible. TF charges are not always determined to be the most appropriate means to mitigate threat. In these instances, alternative measures are used. The below case showed that while a boy obtained funds by robbery for travel abroad to join a terrorist organization, RCMP had pursued terrorism and criminal charges instead of TF charges.

Box 8. Young Foreign Terrorist Fighter

In 2014, a 15-year-old boy who had become radicalized to violence became determined to travel abroad to join a terrorist organization. He had previously tried unsuccessfully to purchase an airline ticket for Syria with his father's credit card. In October 2014, the father discovered Can$870, a knife, and a balaclava in the boy's backpack. Feeling suspicious of money might have been stolen, the father made a report to police. Investigation revealed that the boy had committed an armed robbery in order to purchase ticket for Syria. The boy was charged and convicted of armed robbery. Additional national security investigation by C-INSET resulted in the youth being convicted of attempting to leave Canada to participate in the activity of a terrorist group (CC 83.131) and commission of an offense for a terrorist group (83.2). He was sentenced to 24 months in youth custody plus one-year probation, consecutive to the sentence of armed robbery.

162. This and other cases discussed establish the authorities' ability to pursue TF activities. However, the results obtained so far are not entirely commensurate with Canada's risk profile, which, as assessed in the NRA, points to more frequent and diverse TF occurrences. As a result, Canada has demonstrated to some extent that it pursues the different types of TF activities that it faces.

TF Identification and Investigation

163. The RCMP investigates the financial component of all terrorism-related incidents. It employs various avenues to identify and investigate potential TF activities including human source or intelligence, referrals from international or domestic partners (e.g., the U.S. Federal Bureau of Investigations (FBI), FINTRAC, CRA, and CSIS, direct reporting from Canadian FIs), and national security investigations.

164. FINTRAC regularly provides proactive disclosures and responses to VIRs on TF cases, which supports the prioritization of TF investigations. It mostly disseminates disclosures related to TF to CSIS, but also to the RCMP, CBSA, CRA, municipal and provincial police, and foreign FIUs. According to FINTRAC, roughly half of TF disclosures were proactive, and half in response to VIRs. The authorities do not keep figures on the results of TF investigations arising from proactive disclosures.

Table 15. TF-Related VIRs and FINTRAC Disclosures (from and to RCMP only)

	2010-11	2011-12	2012-13	2013-14	2014-15	Total
Number of TF Disclosures	100	110	125	188	206	729
Number of TF-Related VIRs	26	65	78	84	61	314

165. LEAs and FINTRAC accord priority to TF investigations, although there are exceptions where priority would be accorded to other terrorism files, as highlighted in the Project Investigation below. In urgent cases, FINTRAC provides TF-related financial intelligence to the RCMP within hours. In normal circumstances, it may take days or weeks to respond to the VIRs. In one of the cases provided, which dated back more than 10 years, timely intelligence from FINTRAC was instrumental in identifying domestic and foreign accounts, as well as in establishing the foundations for the necessary judicial authorization applications.[67] The CBSA also assists in the identification of an investigation into TF activities.

166. For example, in the case of Project Investigation, a person was intercepted by the CBSA at a Canadian airport for carrying undeclared currency in excess of Can$10,000. CBSA notified the RCMP, which assumed control of the investigation because of the nexus to TF. The investigation revealed that funds destined to a foreign country to support an organization listed by Canada as a terrorist entity had been collected across Canada by multiple individuals. Information received from FINTRAC resulted in the identification of the funding networks of the entity and of its key members. Due to operational and resource constraints imposed by higher priority national security investigations, the RCMP was unable to proceed further with the file. A different approach was therefore adopted: the suspect was charged under PCMLTFA for not reporting the importation or exportation of currency or monetary instruments. He pleaded guilty and was fined Can$5,000, and the funds previously seized were forfeited to the Crown.

[67] The case in question was the Project Saluki: In 2002, the RCMP conducted a TF investigation to determine whether monies were being raised in Canada by a front organization, the World Tamil Movement (WTM), for the LTTE in Sri Lanka. Financial Intelligence provided by FINTRAC and banking records from FIs obtained by a court order indicated that funds were being sent from a bank account in Canada to a bank account in a foreign country registered to a legal entity. With the assistance of the foreign country, the RCMP gathered the bank documents of the foreign account and identified the holders and the persons associated with or who maintained control over the account, which involved a private deed of trust as well as a list of the appointed trustees. RCMP officers went to the foreign country, interviewed the trustees and signatories of the foreign bank account and determined details of their involvement and position with the legal entity. No person was charged upon the conclusion of the investigation. The PPSC applied for civil forfeiture and in 2010 the Court ordered forfeiture of the WTM building in Montreal and other property under terrorism legislation.

167. All TF investigations are conducted by the RCMP's INSET field units. These units are located in Vancouver, Edmonton, Calgary, Toronto, Ottawa, and Montreal, and are comprised of officers deployed from other partners (including municipal and provincial LEAs and the CSIS) in numbers that fluctuate depending on operational needs. They are tasked by FPCO, which it is responsible for the prioritization of investigations. TF activities are investigated in proportion with their scope and complexity. As investigations become more complex and require more resources, the RCMP uses a management tool to ensure that investigations align with national security priorities. Between 2009 and 2013, it identified five investigations as major TF cases, which led to two charges being laid (see previous core issue).

Table 16. TF Investigations

	2010	2011	2012	2013	2014	Total
Assistance Files 7/	235	162	117	201	179	**894**
Participate/Contribute to Terrorist Group Activity	40	29	33	45	52	**199**
Provide/Collect Property for Terrorist Activity	31	26	17	21	9	**104**
Information Files 8/	30	31	15	25	34	**135**
Crime Prevention 9/	0	2	1	2	79	**84**
Facilitate Terrorist Activity	15	3	6	10	15	**49**
Make Available Property/Service for Terrorist Act	10	15	8	5	8	**46**
Suspicious Person/Vehicle/Property	0	1	6	9	2	**18**
Use/Possess Property for Terrorist Activity	4	1	2	1	0	**8**
National Security Survey Codes 10/	1	1	0	4	0	**6**
Instruct/Commit Act for Terrorist Group	2	3	0	1	3	**9**
Others (Criminal Intelligence, Fraud, etc.)	5	3	6	5	4	**23**
Total	**373**	**277**	**211**	**329**	**385**	**1575**

7/ An Assistance file is created when assisting domestic or foreign non-PROS/SPROS units or agencies.

8/ Information File is information received is not a call for service, or the person or agency supplying the information does not expect police action.

9/ Crime Prevention are activities directed toward the tangible objective of preventing a specific type of crime, e.g., breaking and entry, approved or accepted community-based policing program such as Drug Abuse Resistance Education (DARE).

10/ National Security Survey Codes are the combined collection of two different survey types: Threat Assessments and VIP/Major Events.

TF Investigation Integrated with—and Supportive of—National Strategies

168. CFT is an integral part of Canada's strategy to combat terrorism. The RCMP confirms that it assesses the existence of a TF component in every national security investigation. Cases provided (including IRFAN-CANADA described in IO.10) showed that the authorities use TF investigations to identify the structures, key persons, and activities of terrorist organizations. TF investigations are integrated with, and used to support, national counter-terrorism strategies and investigations.

Effectiveness, Proportionality and Dissuasiveness of Sanctions

169. Canada successfully pursued and convicted two individuals on TF charges. The first case (R v. THAMBITHURAI described above) only attracted a six-month imprisonment despite PPSC appealing against the sentence. In the second case (R v. KHAWAJA, see Box 9 below), the Court sentenced the defendant to two years' imprisonment for TF and to life imprisonment for "developing a device to activate a detonator."

Box 9. R v. KHAWAJA

In 2004, Canada initiated an investigation into a Canadian citizen linked to a terrorist group under investigation in the United Kingdom (U.K.) for planning a fertilizer bomb attack targeting pubs, nightclubs, trains and utility (gas, water and electric) supply stations in the U.K. The evidence collected indicated that the Canadian subject attended a training camp in Pakistan in July 2003 and transferred on three occasions a total of about Can$6,800 to his associates in the U.K. with the help of a young woman to avoid suspicion of link. His parents were persuaded to evict tenants from their residence in Pakistan so that the subject may make the facility available for use by the group's members. He also planned 30 devices to strap explosives onto model airplanes with remote triggers. He was arrested by the RCMP in 2004, detained, and charged in 2008 with seven counts of offenses under the CC, including one count of TF under 83.03(a). MLA requests were sent to the U.S. authorities for the subject's Internet Service Provider and payment records as well as the testimony of a U.S. witness. In December 2010, upon the appeal by the PPSC, the subject was sentenced to life imprisonment for "developing a device to activate a detonator" and 24 years of imprisonment for the other offenses, including two years' imprisonment for TF.

170. While low, the number of instances prosecuted appears in line with Canada's threat profile and considering the alternative mitigating measures taken (see below). Sanctions applied appear to be proportionate with the amounts involved and dissuasive. No legal person has been convicted of TF offenses. No designations were made to the relevant UN bodies but Canada has been co-sponsor to a number of designations.

Alternative Measures Used Where TF Conviction is Not Possible (e.g., Disruption)

171. Canada's primary goal in counter terrorism efforts is to maintain public safety, and Canada places a strong focus on disrupting terrorist organizations and terrorist acts before they occur. The RCMP defines disruption in national security matters as the interruption, suspension or elimination, through law enforcement actions of the ability of a group(s) and/or individual(s) to carry out terrorist or other criminal activity that may pose a threat to national security, in Canada or abroad. It includes disruption of TF activities

172. During national security investigations, activities of participants and peripheral participants may be tactically disrupted for a variety of reasons, including triggering reactions or behavioral changes of the main targets. TF investigations therefore do not always result in TF charges, if other charges for terrorism or other offenses are being laid and the evidence is most cogent and appropriate or would best serve the public interest. The authorities shared several cases (including Project Smooth below) where despite clear evidence to substantiate a TF charge, other means were preferable to ensure the public interest.

Box 10. Project SMOOTH

In August 2012, CSIS reported to RCMP that a male ("CE") residing in Montreal had met another male ("RJ") in Toronto. RJ was known to the RCMP for recently distributing pro Al-Qaeda propaganda. Investigation, including the use of an undercover U.S. FBI agent who had gained the trust of CE and RJ, revealed that the two men had plotted to cut a hole in a railway bridge to derail the Canadian Via Rail passenger train between Toronto and New York. The FBI agent had surreptitiously recorded their conversations, which made up the bulk of the case's evidence, including CE's description on the hierarchical structure and mode of communication of a terrorist group and that CE was receiving orders from Al Qaeda through a middleman. It was also unveiled during the investigation that CE had or intended to finance a total of Can$4,200 to the terrorist group. In 2013, CE and RJ were arrested. CE and RJ were both charged with four offenses: conspiring to damage transportation property with intent to endanger safety for a terrorist organization, conspiring to commit murder for a terrorist group, plus two counts of participating or contributing to a terrorist. CE was found guilty of all four charges plus another he faced alone for participating in a terrorist group. RJ was convicted of all charges except that of "conspiring to damage transportation property with intent to endanger safety for a terrorist organization." In March 2015, both men were sentenced to life imprisonment.

173. In other cases, TF prosecutions were not possible, especially in cases based largely on intelligence that may fall short of the evidentiary threshold required by criminal courts. In instances where prosecution is not deemed to be the best avenue to protect the public or human sources, or is not possible, a wide-range of disruption techniques is employed. Such techniques typically include: arrests; search-and-seizure raids; "intrusive surveillance" (in which police make it obvious to the suspects that they are being watched); civil forfeiture; inclusion of specific persons in Canada's no fly list (which is particularly relevant considering the growing threat of foreign fighters); revocation of the charitable status of NPOs identified as having been used for TF purposes; listing of terrorist entity under the CC, barring of individuals who pose a threat to the security of Canada and prohibition from entering or obtaining status in Canada or from obtaining access to sensitive sites, government assets or information; and extradition. Canada frequently uses other criminal justice and administrative measures to disrupt TF activities when a prosecution for TF is not practicable.

Overall Conclusions on Immediate Outcome 9

174. Canada has achieved a substantial level of effectiveness for IO.9.

D. Immediate Outcome 10 (TF Preventive Measures and Financial Sanctions)

Implementation of Targeted Financial Sanctions for TF without Delay

175. Canada implements UNSCR 1267 and UNSCR 1373 (and their successor resolutions) through three separate domestic listing mechanisms: United Nations Al-Qaeda and Taliban Regulations (UNAQTR); the Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism (RIUNRST); and the CC. Canada plays an active role in co-sponsoring the listing of new terrorist entities, as appropriate, and delisting defunct entities. The lists of entities whose assets are to be frozen under UNSCR 1267 and its successor resolutions are automatically

incorporated into Canadian law by reference through UNAQTR. Accordingly, UNSC decisions to list or delist an individual are given immediate effect in Canada; no additional action by Canadian authorities is needed to give legal effect to a designation. These decisions are rapidly brought to the attention of FRFIs, but not of other REs.

176. The CC is Canada's primary listing mechanism, and allows it to satisfy the obligations under UNSCR 1373. While the RIUNRST also satisfies UNSCR 1373, no listings have been added to the RIUNRST since 2006. In practice, this CC process entails a criminal intelligence report prepared by the RCMP or a security intelligence report prepared by the CSIS, which is subjected to a legal review by independent counsel to ensure that it meets the CC listing threshold (i.e., reasonable grounds to believe), as well as interdepartmental consultations. The authorities can list an entity to Canada's domestic list (under the CC) in an expedited manner if necessary.[68] The Canadian authorities provided a concrete example (IRFAN Canada, below) of the domestic listing of a NPO.

Box 11. IRFAN-Canada

In 2010, CRA-Charities suspended the receipting privileges of IRFAN-Canada. The suspension was based on the organization's failure to provide and maintain records, which interfered with CRA-Charities' ability to carry out the audit that began in 2009. CRA-Charities continued with the audit during the period of suspension and ultimately revoked IRFAN-Canada's charitable registration in 2011. It shared information regarding IRFAN-Canada's possible association with the listed organization, Hamas, with partner organizations, including the RCMP. A CRA-Charities analyst seconded to the RCMP was able to provide expertise to facilitate the sharing of information, as authorized by legislation. The RCMP collaborated with and received financial intelligence from FINTRAC.

In 2014, the RCMP officially opened the investigation, which resulted in an RCMP recommendation to PS Canada to have IRFAN-Canada listed as a terrorist organization. The financial intelligence provided by FINTRAC also served to inform deliberations on the listing of IRFAN. The RCMP, PS Canada, and the DOJ worked together to prepare the documentation required for the Government to make a decision as to the listing. In April 2014, IRFAN-Canada was listed as a terrorist entity by the Government of Canada. Following the listing, criminal investigations were initiated by the RCMP's INSETs in Ontario and Quebec, and were still ongoing at the time the assessment.

177. Third-party requests from foreign jurisdictions are considered under the CC framework. Canada has received numerous requests from foreign jurisdictions since the establishment of the regime and has given effect to both formal and informal requests, though it does not keep records on the number of third-party requests for listing under the CC. The authorities also indicated that they were able to list an entity on an expedited manner when necessary, following third-party requests.

178. As of April 7, 2015, 54 entities were listed pursuant to the CC and 36 terrorist entities under the RIUNRST. Once an entity has been listed, PS issues a news release advising of the new listing and provides a notification on its sanctions website, and the listings are published in the Canada Gazette, approximately two weeks after listing. To assist FIs search their list of customers against these listed

[68] Several factors may be considered, as for example: operational imperative to list more quickly to freeze known assets; nexus to Canada; national security concerns; allied concerns, etc.

terrorist names, OSFI maintains on its website a database of all terrorist names (and known identifiers) subject to Canadian laws, and notifies FIs without delay by posting instantly a notification to its website and by notifying all its e-mail subscribers each time a new terrorist name is listed under Canadian law, or there are changes to existing information. FRFIs are also required to report to OSFI monthly that they have conducted the name screening and report any terrorist property that they have identified and frozen. FINTRAC also provides a link to OSFI's website on its own website, as well as guidance to REs on the reporting requirements related to terrorist property. Other than in the case of OSFI, the mechanism for informing the private sector about listed entities appears to be rather passive, as it relies on REs consulting the Official Gazette and the websites of the competent authorities and/or, when they are aware of this possibility, subscribing to RSS feeds (or the UN notification system).

179. The FRFIs met during the onsite had a good understanding of their screening obligation regarding targeted financial sanctions (TFS) and implemented sanctions without delay. DNFBPs, however, do not have a good understanding of their obligations (see IO.4). Furthermore, while they are required to check the listings at the beginning of a business relationship, they are not required to conduct a full search of their customer databases on a regular basis, which is a major limitation to an effective implementation of TFS.

180. Persons listed in Canada may apply for revocation of the designation under the framework detailed in R.6.[69] Examples of delisting were shared with the assessors. One entity was delisted in December 2012.

181. Canada has not proposed a designation to the UN Sanctions Committees, but acted as co-sponsor on several occasions.

Targeted Approach, Outreach and Oversight of At-Risk Non-Profit Organizations

182. The Canadian NRA concluded that registered charities present a high risk of TF, due to the fact that a large number of the financial transactions that charities conduct may be performed via delivery channels with a high degree of anonymity and some level of complexity (i.e., multiple intermediaries are involved). The NRA also highlights that the significant use of cash may make it difficult for the authorities to establish the original source of funds, and that it may be difficult to know how the funds or resources will be used once transferred to partner organizations or third parties.

183. Canada has implemented a targeted approach regarding the NPO sector vulnerability to TF. In 2015, the CRA, which regulates charities under the Income Tax Act, conducted a review in addition to the NRA, to examine the size, scope and composition of the NPO sector in Canada and to determine which organizations, by virtue of their activities and characteristics, were at greater risk

[69] Under the Criminal Code regime, there are several ways an entity could be delisted. The Minister of Public Safety and Emergency Preparedness can recommend to the Governor in Council that an entity be delisted at any time, the entity could be recommended for delisting as part of the two-year review, or an entity can apply for delisting as per the process outlined under section 83.05(2).

of being abused for terrorist support purposes. The CRA found that, in Canada, the organizations at greatest risk of terrorist abuse because of the nature of their activities and characteristics are charities. As a result, the authorities concluded that, in the Canadian context, NPOs that fall within the FATF definition are charities. Four reports had previously been published regarding the sector, notably a "Non-Profit Organisation Risk Identification Project" in 2009. Canada has a large NPO sector, comprising of approximately 180,000 organizations. The sector can be divided into two groups: charities and NPOs, depending on their legal structures. While both are exempt from paying taxes, federally registered charities (of which there are approximately 86,000) receive additional fiscal privileges and submit annual information returns, which include notably the names of the directors or trustee, a description of its activity and financial information, including sources of funding. Non-charity NPOs (of which there are approximately 94,000) having assets in excess of Can$200,000 or annual investment income exceeding Can$10,000 are not required to register, but must file an annual NPO Information Return with the CRA.[70] In addition, non-charity NPOs incorporated provincially or federally would be required to file certain information with the provincial or federal governments on an annual basis depending on the statute under which the organization is formed. This typically includes information related to address, directors, and the date of the last general meeting. In certain cases, organizations may have to provide detailed financial information depending on value of assets or fund received.

184. CRA-Charities reviews all applications for charitable registration and conducts audits of registered charities. From 2008–2014, CRA-Charities completed approximately 5,000 audits in total; 16 these audits comprised a national security concern, eight of which resulted in revocation of registration.[71] If an applicant charity does not meet the requirements of registration, e.g., due to terrorism concerns, the CRA denies its application.[72] Through its work, CRA-Charities may take administrative action to disrupt an organization's activities where it has identified a risk of terrorist abuse, and/or relay the information to LEAs. If a registered charity no longer complies with the requirements of registration, for any reason including connections to terrorism, the division can apply a range of regulatory interventions and, in the most the serious cases, may revoke the registration.

185. CRA-Charities conducts outreach to advise charities of their legislative requirements and how to protect themselves from terrorist abuse. This includes general guidance on topics related to sound internal governance, accountability procedures, and transparent reporting, as well as specific tools such as a checklist on avoiding terrorism abuse and a web page on operating in the international context. CRA-Charities will build on this existing outreach through its enhanced

[70] The annual NPO Information Return includes information about their activities, assets, and liabilities.

[71] Two led to penalties totaling Can$440,000; four led to compliance agreements with the charity involved; and two resulted in education letters.

[72] The Income Tax Act requires that charities devote their resources to charitable purposes and activities. An organization that supports terrorism would be denied registration for carrying on activities contrary to public policy, which would not qualify as charitable. Additionally, the Charities Registration (Security Information) Act provides a prudent reserve power to deny or revoke registration when terrorist connections are suspected.

outreach plan. CRA-Charities has begun consultations with the sector to educate them on the risk of terrorist abuse and to gain a better understanding of their needs in terms of outreach and guidance.

186. National coordination has been enhanced. The CRA shares information with relevant partners where there are concerns that a charity is engaged in providing support to terrorism. If the division encounters information that is relevant to a terrorism investigation when carrying out its regulatory duties, it shares that information with national security partners and LEAs. The division shared information with domestic national security partners in support of their mandate in 47 cases. Similarly, the division received information from partners in 51 cases to assist with its analysis, in 2014/2015. In addition, to facilitate the sharing of information, a secondment program between the CRA and its partners has been instituted: CRA employees are seconded to the partner agencies and employees from the partner agencies are seconded to the CRA.

187. According to the CRA's NPO Sector Review of 2015 the 86.000 registered charities represent 68 percent of all revenues of the NPO sector and nearly 96 percent of all donations (see R.8). CRA registered charities also account for a substantial share of the sector's foreign activities as about 75 percent of internationally operating NPOs are registered as charities. In addition, as detailed above, all registered charities, regardless of the value of their assets, and all NPOs with assets in excess of Can$200,000 or annual investment income exceeding Can$10,000 must file an annual information return with the CRA, which includes the provision of financial information. In addition, registered charities with revenue in excess of $100,000, and/or property used for charitable activities over Can$25,000, and/or that have sought permission to accumulate funds, must provide more detailed financial information. The authorities identify charities as being the organizations falling under the FATF definition of NPOs and reviewed the NPO's sector (see Box 12).

Box 12. Canadian NPO's Sector Review

The national regulator of registered charities, i.e., the CRA, conducted a domestic review of the entire NPO sector in Canada in order to identify which organizations, by virtue of their activities and characteristics, were at greater risk of being abused for terrorist support purposes. The review aimed to ensure that Canada (i) is not taking an overly broad interpretation of the FATF definition of NPO, (ii) focuses on those organizations that are at greatest risk, and (iii) does not burden organizations that not at risk with onerous reporting requirements for TF purposes.

The CRA reviewed existing publications and research by governmental, academic, and non-profit organizations related to the non-profit sector, including reports by Statistics Canada on non-profit institutes, consultations on regulations affecting the sector, and studies on trends in charitable giving and volunteering. In addition, it looked at existing laws and reporting requirements affecting NPOs. To determine where there is risk, NPOs were categorized based on shared characteristics such as purpose, activities, size and location of operation. The CRA compared those characteristics with the elements of the FATF definition of NPO. It also took into consideration the findings of the FATF typologies report Risk of Terrorist Abuse in NPOs to identify features that put organizations a greater risk.

The CRA found that, in Canada, the organizations at greatest risk of terrorist abuse are charities. As a result, the authorities concluded that, in the Canadian context, only charities fall within the FATF definition of NPO. While organizations at greatest risk are charities, not all charities are at risk. The insight obtained from the sector review allowed Canada to focus on charities as the starting point for its NRA.

Source: FATF Best practices paper on combating the abuse of NPOs—October 2015.

188. The registered charity met during the assessment is large and has a number of international connections. It has a good understanding of its vulnerability to TF and has implemented adequate measures to mitigate that risk, without disrupting legitimate NPO activities.

Deprivation of TF Assets and Instrumentalities

189. As of February 2015, the total amount of frozen assets belonging to designated entities is Can$131,235 in 12 bank accounts, Can$29,200 in six life insurance policies, nine house insurance policies, and one automobile insurance policy, totaling Can$3,248,612 frozen. The number of entities that had their assets frozen was not provided.

190. Despite the high number of TF occurrences (see IO.9), no assets and instrumentalities related to TF were seized or confiscated in circumstances other than designations. There are several reasonable explanations for this. LEAs indicated that, in several cases, no assets or instrumentalities were found. In others cases, the lack of confiscation can be due to the fact that TF investigations do not always result in TF charges and other means of disruption (see IO.9). The authorities also provided cases of TF investigations unrelated to the UN designations where the RCMP seized some assets and instrumentalities,[73] but did not proceed to seek their confiscation.

Consistency of Measures with Overall TF Risk Profile

191. While the terrorist threat has grown in the recent years, in particular in light of an increased number of Canadian nationals who have joined terrorist groups abroad,[74] not all terrorist entities identified have financing or support in Canada. In October 2014, Canada was victim of two terrorist attacks in Saint-Jean-sur-Richelieu and Ottawa, perpetrated by two Canadian citizens who intended to travel abroad for extremist purposes, but had been prevented from doing so. The TF investigation related to these events was still ongoing at the time of the assessment. In other instances, the authorities detected the transfer of suspected terrorist funds to international locations. These transfers had been conducted through a number of methods, including the use of MSBs, banks, and NPOs, as well as smuggling bulk cash across borders.

192. Canada has demonstrated to some extent only that it pursues the TF threat that it faces (see IO.9). The system suffers from inadequate implementation of UNSCRs by DNFBPs. Nevertheless, it must also be noted that, in some respect, Canada goes beyond the standard—this in particular the case with respect to the CC terrorist list, which Canada reviews every two years to ensure that the legal threshold for listing continues to be met for each entity listed.

[73] The assets seized included over Can$10,000 in cash, in one case, and tractor trailers in another.

[74] As stated by the Director of CSIS following his appearance at the Senate Committee on National Security and Defence, as of the end of 2015, the Government was aware of approximately 180 individuals with Canadian a nexus who were abroad and suspected of engaging in terrorism related activities. The Government was also aware of a further 60 extremist travelers who had returned to Canada.

Overall Conclusions on Immediate Outcome 10

193. Canada has achieved a substantial level of effectiveness for IO.10.

E. Immediate Outcome 11 (PF Financial Sanctions)

Implementation of Targeted Financial Sanctions Related to Proliferation Financing without Delay

194. Canada's framework to implement the relevant UN CFP sanctions relies on three main components: (i) a prohibition to conduct financial transactions to Iran and the DPRK, with a few regulated exceptions, (ii) an obligation to freeze assets of designated persons; and (iii) an obligation to notify the competent authorities of any frozen assets.

195. Canada implemented the UNSCR 1737 and 1718 obligations, including part of the freezing obligations, by issuing within the UN-requested timeline two regulations dealing with Iran and the DPRK respectively. Both regulations impose freezing obligations that are generally comprehensive (see R.7). The lead agency for their implementation is GAC. Canada also went beyond the standard by imposing additional unilateral sanctions under the Special Economic Measures Act (SEMA). As a result of its Controlled Engagement Policy towards both countries, the Canadian Government does not engage in active trade promotion with Iran and the DPRK, and, with almost all commercial financial transactions between Canada and Iran prohibited, the volume of existing bilateral trade with both countries has dropped considerably. Canada also ensured that the exceptions to the general prohibition of conducting financial transactions[75] do not apply with respect to designated persons and entities.

196. Decisions taken by the UNSC under 1737 and 1718 take immediate effect in Canada. The current lists of designated persons and entities are published on the OSFI website. To facilitate the implementation of the TFS, guidance is provided on the GAC and OSFI website.[76] In addition, OSFI notifies the FRFIs of any changes to the lists on the same day as the changes occur, or on the day that follows the receipt of the note verbale. It also reminds FRFIs on a monthly basis of their screening and freezing obligations, either per web post or per email. Its guidance requires FRFIs to search their records for designated names in two ways: (i) by screening new customers' names against the official lists at the time such customers are accepted; and (ii) by conducting a full search of all customers' databases "continuously," which the guidance defines as "weekly at a minimum." No other authorities provide notifications to other REs of changes made to the lists. As a result, while the legal obligations to implement PF-related TFS are the same across the range of REs, swift

[75] Examples of these exceptions include: non-commercial remittances to the DPRK; financial banking transactions of Can$40,000 and under between family members in Canada and family members in Iran; and other transactions permitted on a case-by-case basis, at the discretion of the Minister of Global Affairs. In practice, exceptions have been granted mainly in the case of prospective Iranian immigrants for the purposes of immigration fees and related transactions.

[76] See www.international.gc.ca/sanctions/countries-pays/iran.aspx?lang=eng; www.international.gc.ca/sanctions/countries-pays/korea-coree.aspx?lang=eng.

action is actively facilitated in the case of FRFIs only. REs may nevertheless subscribe to the RSS feeds on the GAC website, or to the UN notification system, in order to be notified of changes to the Iran and DPRK regulations.

Identification of Assets and Funds Held by Designated Persons/Entities and Prohibitions

197. Canada has had some success in identifying funds and other assets of designated persons, and preventing these funds from being used, as indicated in the table below. Two of the larger banks, as well as one provincial FI and two life insurers have identified assets of designated persons, frozen those assets (where available), and reported the case to the RCMP, OSFI, and FINTRAC. The assets were detected through timely screening of the FIs' customers' (but not other parties such as the beneficial owner, despite OSFI's guidance in this respect) against the UN lists. While the freezing are occurrences are low, they nevertheless indicate that FIs and in particular D-SIBs are taking measures to prevent their potential misuse for PF activities. No information was provided on the timing of the freezing measures.

Table 17. Assets Reported Under the Regulations Implementing the United Nations Resolutions on both Iran and the DPRK, as of September 2015

Reporting Entity	Number of Accounts/Contracts	Assets Frozen		Assets Reported but Not Frozen (no cash surrender value) in Can$
		Can$ equivalent of amounts in foreign currencies	Amounts in Can$	
Bank X (DTI)	1		78,838	
Bank Y (DTI)	2	591.2	845	
Provincial FI	4		30,647	
Total re. Accounts	**7**	**591.2**	**110,330**	
Federal Life Insurer X	6			29,200
Life Insurer Y	10			3,248,612
Total re. Insurance Contracts	**16**			**3,277,812**

198. Canada went beyond the UN listings by investigating the financial components of proliferation activities detected on their territory. The authorities successfully prosecuted one individual for the export of prohibited dual-use goods. The enforcement function is shared between the RCMP and the CBSA, with the former taking the lead in instances that include a potential nexus with national security or OCGs, and the CBSA taking the lead in other instances. So far, the investigations revealed no need for freezing measures: the individuals had little assets, most of which had been used to purchase unauthorized dual use goods.

199. Through the analysis of STRs and other information, FINTRAC has detected potential violations of the SEMA and import-export legislation which it disclosed to the CBSA and CSIS.[77] The analysis of STRs notably pointed to some instances of potential wire stripping and sanctions evasion. No figures were provided as the system does not keep track of STRs that also mention suspicion of PF. According to the authorities, in most instances, the REs may not specifically refer to suspicions of PF, but simply highlight that the transactions does not make economic sense. FINTRAC has discussed some of these cases with its partner agencies in the operation meetings of the Counter-Proliferation Operations Committee.

FIs and DNFPBs' Understanding of and Compliance with Obligations

200. Large FIs, and in particular the D-SIBs, have a good understanding of their freezing obligations, including with respect to PF. They generally have staff dedicated to the implementation of TFS that regularly check the UN lists. They are also aware of the risk of wire stripping and have reported instances of potential wire stripping to FINTRAC. Smaller FRFIs have a relatively good understanding of their obligations, although several do not distinguish the PF-related from the TF-related sanctions. DNFBPs, however, are far less aware of their PF-related obligations, so far, none of them have frozen assets belonging to designated persons.

201. Some outreach has been conducted, notably by the RCMP, with a view to increase the general public's awareness of the proliferation risk. Although some of the outreach activities include information on red flags for potentially suspicious PF activities, these efforts have, so far, mainly focused on proliferation activities rather than the implementation of related TFS.

Competent Authorities Ensuring and Monitoring Compliance

202. There is no formal mechanism for monitoring and ensuring compliance by FIs and DNFBPs with PF-related obligations. Nevertheless, some monitoring does take place in practice with respect to FRFIs: OSFI, in the exercise of its general functions, has examined the systems put in place by FRFIs to implement the sanctions regimes for both TF and PF. It has also identified shortcomings (in particular the lack of screening of persons other than the customer) and requested improvements in the screening processes. As a result of a sanction recently imposed by the U.S. regulator on a foreign bank with subsidiary operations in Canada and the U.S. for violations of the PF-related sanctions, OSFI increased its dialogue with and monitoring of that specific bank. Ultimately, it was satisfied that the activities conducted in Canada were different than those conducted in the U.S. and that the risk was limited in Canada. OSFI is not, however, habilitated to sanction any potential breach of PF-related obligations.

[77] While FINTRAC does not have an explicit mandate to receive reports of suspicions of PF, it is required by law to disclose financial intelligence to assist in investigations and prosecutions for ML, TF and other threats to the security of Canada, which could include PF.

203. While this ad hoc monitoring by the OSFI is proving helpful with respect to FRFIs and useful in identifying shortcoming in their implementation of TFS, it does not entirely compensate the lack of a more comprehensive monitoring system.

Overall Conclusions on Immediate Outcome 11

204. Canada has achieved a moderate level of effectiveness with IO.11.

PREVENTIVE MEASURES

A. Key Findings

Several, but not all REs listed in the standard are subject to Canada's AML/CFT framework:

- AML/CFT requirements were found to breach the constitutional right to attorney-client privilege by the Supreme Court of Canada, and, as a result, are inoperative with respect to legal counsels, legal firms, and Quebec notaries. The exclusion of these professions is not line with the standard and raises serious concerns (e.g., in light of these professionals' key gatekeeper role in high-risk activities such as real estate transactions and formation of corporations and trusts).

- TCSPs (other than trust companies), non-FI providers of open loop pre-paid card, factoring companies, leasing and financing companies, check cashing business and unregulated mortgage lenders, online gambling, and virtual currencies do not fall under the AML/CFT regime, but legislative steps have been taken with respect to online gambling, open-loop pre-paid cards and virtual currencies.

FIs including the D-SIBs have a good understanding of the ML/TF risks and of their AML/CFT obligations. While a number of FIs have gone beyond existing requirements (e.g., in correspondent banking), technical deficiencies in some of the CDD requirements (e.g., related to PEPs) undermine the effective detection of some very high-risk threats, such as corruption.

Requirements—on FIs only—pertaining to beneficial ownership were strengthened in 2014 but there is an undue reliance on customers' self-declaration for the purpose of confirming beneficial ownership.

Although REs have gradually increased the number of STRs and threshold-based reports filed, the number of STRs filed by DNFBPs other than casinos remains very low.

With the exception of casinos and BC notaries, DNFBPs—and real estate agents in particular—are not adequately aware of their AML/CFT obligations.

B. Recommended Actions

Canada should:

- Ensure that legal counsels, legal firms, and Quebec notaries are subject to AML/CFT obligations when engaged in the financial transactions listed in the standard.

- Ensure that TCSPs (other than trust companies) open loop pre-paid cards, including non FI providers, virtual currency and on line gambling to AML/CFT requirements.

- Require DNFBPs to identify and verify the identity of beneficial owners and PEP in line with the standard.
- Require FIs to implement preventive measures with respect to PEPs, and wire transfers in line with the FATF standards, and monitor (e.g., through targeted inspections) and ensure compliance by all FIs of their obligation to confirm the accuracy of beneficial ownership in relation to all customers.
- Enhance the dialogue with DNFBPs other than casinos to increase their understanding of their respective ML/TF vulnerabilities and AML/CFT obligations, in particular with real estate agents, dealers in precious metals and stones (DPMS) (with greater involvement of the provincial regulators and the relevant trade and professional associations). Update ML/TF typologies and specific red flags addressed to the different categories of DNFBPs to assist in the detection of suspicious transactions.
- Consider introducing a licensing or registration regime, or other controls for DPMS.
- Monitor and ensure DNFBPs' and small retail MSBs' compliance with TFS obligations.
- Issue further guidance, especially to non-FRFIs, on the new requirements related to domestic PEPs.
- Strengthen feedback to small banks and the insurance sector on the use of STRs.
- Issue guidance for all REs to facilitate the detection of the possible misuse of open loop prepaid cards in ML and TF schemes.

The relevant Immediate Outcome considered and assessed in this chapter is IO.4. The recommendations relevant for the assessment of effectiveness under this section are R.9-23.

C. Immediate Outcome 4 (Preventive Measures)

Understanding of ML/TF Risks and the Application of Mitigating Measures

205. The level of understanding of ML/TF risks and AML/CFT obligations, as well as the application of mitigating measures vary greatly amongst the various REs.

206. FIs are aware of the main threats and high-risk sectors identified in the NRA, as well as of the level of ML/TF vulnerabilities associated to their activities. Recent trends in the FIs' understanding of risks and AML/CFT obligations is not immediately apparent in the supervisory data (because the latter aggregates as "partial deficiencies" both minor and more severe failures), but, according to the authorities, have been positive. The major banks have developed comprehensive group-wide risk assessments and implement mitigating measures derived from detailed consideration of all relevant risk factors (including lines of business, products, services, delivery channels, customer profiles). Several other FIs stated that their risk assessment and mitigating

measures are already in line with the findings of the NRA. Specific attention is paid to cash (including potentially associated to tax evasion) and to the geographic risk (which, especially in the case of large banks, takes into account the index of corruption developed by relevant international organization and includes offshore financial centers). Some FIs also consider trust accounts held by lawyers and other legal professions as presenting a higher risk and, as a result, conduct enhanced monitoring of these accounts. Specific products associated to real estate transactions, such as mortgage loans, are also considered as high-risk products. Over the last three fiscal years, a total of 9,556 STRs were filed with FINTRAC regarding suspected ML/TF activities in relation to real estate, which represents 3,8 percent of the overall amount of STRs received, with most STRs coming from banks, credit unions, caisses populaires, and trust and loan companies. The main typologies identified in this respect range from the use of nominees by criminals to purchase real estate or structuring of cash deposits to more sophisticated schemes where, for example, loan and mortgage schemes are used in conjunction with the use of lawyer's trust account.

207. In some instances, however, the regulator's onsite inspections revealed issues with the quality and scope of the risk assessments, especially in relation to the elements taken into account as inherent risk of individuals, and to the consistency among business-lines. Smaller FRFIs display a weaker understanding of ML/TF risks, and tend to regard AML/CFT obligations as a burden.

208. The life insurance sector appears to underestimate the level of risk that it faces. According to FINTRAC supervisory findings, life insurance companies and trust and loan companies that are non-FRFIs show the highest level of deficiency in their risk assessment, as well as the weakest understanding of their AML/CFT obligations. Non-federally regulated life insurance companies have a weak understanding of their ML/TF risks than federally regulated companies, and appear particularly refractory to improving AML/CFT compliance.

209. The representatives of the securities sector recognized the high risk rating of their activities, but also noted that the higher level of risk lie mainly in smaller security firms and individuals. Firms not involved in cross-border activities seem to underestimate their vulnerability to ML risk, having a limited notion of geographic risk, as mainly referred to offshore countries. Overall, securities dealers have a good understanding of their AML/CFT obligations, although supervisory findings highlight that the level of understanding is weaker in more simplified structures and that internal controls are a recurring area of weakness.

210. MSBs' level of awareness of AML/CFT obligations is consistent with their size and level of sophistication of their business model. MSBs that operate globally as part of larger networks are aware of the specific ML/TF risks that they face (i.e., risks emanating mainly from the fact their activity is essentially cash-based). They have developed specific criteria to evaluate certain risk (e.g., the risks posed by their agents) to enable them to determine the appropriate level of controls. While the assessment team did not have an opportunity to meet with representative from the smaller

independent MSBs,[78] representatives from other private sector entities as well as FINTRAC confirm that smaller MSBs are far less aware of their AML/CFT obligations and their vulnerabilities to ML/TF. According to FINTRAC, community-specific MSBs are reluctant to apply enhanced due diligence to higher risk customers. To assist mainly small MSBs in the development of a RBA, on September 1, 2015 FINTRAC developed an RBA workbook for MSBs.

211. Casinos vary greatly in size, complexity, and business models. All the relevant gaming activities are subject to AML/CFT requirements where (on the basis of the model in place) the province or the Crown corporation is responsible for their compliance. Representatives from casinos demonstrated a good understanding of their AML/CFT obligations and of the most frequent ML typologies in their sector. Nevertheless, their implementation of CDD measures seems to follow a tick-box approach rather than be based on an articulated risk-assessment. Moreover, casinos seem to be essentially focused on cash, and appear to underestimate to some extent the risk posed by funds received from accounts with FIs.

212. DPMS are highlighted as a high-risk in the NRA. Compliance examinations conducted between 2012 and 2014 revealed industry-wide non-compliance. FINTRAC has worked with two DPMS associations (namely the Canadian Jewelers Association, CJA, and the Jewelers Vigilance Canada, JVC, which, together, represent about one quarter of the Canadian DPMS) to strengthen compliance of this sector. This has led to an increase in these DPMS' understanding of their AML/CFT obligations, as shown in subsequent examinations. Nevertheless, the absence of licensing or registration system or other forms of controls applicable to the sector in its entirely creates major practical obstacles for FINTRAC to properly establish the precise range of subjects that it should reach out to.

213. The real estate agents met, despite being aware of the results of NRA, consider that they face a low risk because physical cash is not generally used in real estate transactions. As the normal practice is to accept bank drafts—agents consider banks have mitigated the ML/TF risk. In the province of Quebec, notaries trust accounts are used to deposit the funds involved in real estate transactions—real estate agents therefore consider that notaries are in a better position to detect possible ML activities, but Quebec notaries are not currently covered by the AML/CFT regime. Real estate agents are overly confident on the low risk posed by "local customer," as well as non-resident customer originating from countries with high levels of corruption.

214. The accountants' level of awareness of AML/CFT obligations is quite low. The competent professional association underlined that, in the absence of guidance and outreach efforts, accountants are often unclear as to when they are subject to the AML/CFT regime.

215. BC notaries provide a wide range of services related to residential and commercial real estate transfers. They are, however, not fully aware of the risk and their gatekeeper role in relation to

[78] Under the glossary of the NRA the said category has been defined as these MSBs are focused on retail transactions, and have stand-alone computer systems and street-level retail outlets across Canada. Of these, one sub-group offers currency exchanges only, typically in small values, and is often found in border towns (e.g., duty-free shops), while the other sub-group offers currency exchanges, but may also offer money orders and EFTs, typically as an agent of a national full-service MSB.

real estate transactions. Like real estate agents, they consider that all risks have been mitigated by the bank whose account the funds originated from.

216. In May 2015, FINTRAC issued guidance to assist REs in the implementation of their RBA. Most representatives of DNFBPs considered this helpful, but also expressed the need for further initiatives focused on their respective activities.

217. AML/CFT obligations are inoperative towards legal counsels, legal firms and Quebec notaries involved in the activities listed in the standard. In February 2015, the Supreme Court of Canada declared that a portion of Canada's AML/CFT legislation is unconstitutional as to attorneys, because it violates the solicitor-client privilege. Representatives from the private sector and the Canadian authorities confirmed that lawyers in Canada are frequently involved in financial transactions, often related to high-risk sectors, such as real estate, as well as in the formation of trust and companies. In the context of real estate transactions, in particular, lawyers and Quebec notaries provide not only legal advice, but also trading services,[79] and receive sums from clients for the purchase of a property or a business, deposited and held temporarily in their trust accounts. Representatives of the Federation of Law Societies, although aware of the findings of the NRA, did not demonstrate a proper understanding of ML/TF risks of the legal profession. In particular, they appeared overly confident that the mitigation measures adopted by provincial and territorial law societies (i.e., the prohibition of conducting large cash transactions[80] and the identification and record-keeping requirements for certain financial transactions performed on behalf of the clients)[81] mitigate the risks. While monitoring measures are applied by the provincial and territorial law societies, they are limited in scope and vary from one province to the other. The onsite visit interviews suggested that the fact that AML/CFT requirements do not extend to legal counsels, legal firms and Quebec notaries also undermines, to some extent, the commitment of REs performing related functions (i.e., real estate agents and accountants).

CDD and Record-Keeping

218. CDD obligations, and especially those dealing with beneficial ownership, politically exposed foreign persons (PEFPs) and, for FIs, wire transfers, are not fully in line with FATF standards. In addition, some DNFBPs are not subject to AML/CFT requirements and monitoring (see TCA for more details).

219. Since February 2014, FIs are required to obtain, take reasonable measures to confirm, and keep records of the information about an entity's beneficial ownership. In practice, FIs seem to

[79] This is notably confirmed by the exemption from the requirement to be licensed as real estate agent granted under the relevant provincial legislation (for example, in British Columbia, Real Estate Service Act, Section 3, (3) lett. f, and, for Quebec Notaries, Quebec Notary Act, Art.18).

[80] Model Rule on Cash Transactions adopted by the Council of the Federation of Law Societies of Canada on July 2004.

[81] Model Rule on Client Identification and Verification Requirements, adopted by the Council of the Federation of Law Societies of Canada on March 20, 2008 and modified on December 12, 2008.

interpret this new provision as requiring mostly a declaration of confirmation by the customer that the information provided is accurate, to be followed, in some cases, by an open source search. Only a few of the FIs interviewed stated that they would spend time to check the information received and verify the information through further documents and information, which raises concerns. The undue reliance on a customer's self-declaration (as a way to replace the duty to confirm the accuracy of the information provided) appears to be a significant deficiency in the implementation of preventive measures and OSFI has issued findings to FRFIs requiring that more robust beneficial ownerships confirmation measures be undertaken. Moreover, REs have limited methods to confirm the accuracy of beneficial ownership information (see IO.5). Several FIs are in the process of implementing the new requirement by reviewing the information gathered for their existing customers, but most of the FIs interviewed were unable to establish the current stage of this review.

220. Due to the recent entry in force of the new beneficial ownership requirements, there is limited information on how well FRFIs are complying with the new obligations. Recent supervisory findings—albeit limited in numbers—suggest that serious deficiencies remain.

221. Discussions with DNFBPs, in particular those with real estate representatives, highlighted that even basic CDD requirements are not properly understood and that the implementation of the "third-party determination rule" seems to be mainly limited to asking the customer whether he/she is acting under the instructions of other subjects, without further enquiry.

222. Measures to prevent and mitigate the risks emanating from corruption and bribery (classified as very high threats in the NRA) are insufficient, because of shortcomings in the legal framework (see TCA) and weak implementation of existing requirements. REs' capacity to properly detect these criminal activities is significantly undermined. This is in particular the case with DNFBPs considering that they are not required to take specific measures when dealing with PEPs. In order to determine whether they are in a business relationship with foreign PEPs (i.e., PEFPs) or their family members, FIs combine the information gathered through the client identification forms and the screening process (realized mainly through commercial databases). Most FIs interviewed limited their search to the customer and did not seem to establish whether they were dealing with "close associates" of PEFPs. Furthermore, the range of information required by FIs is limited to the source of funds, and does not always include the source of wealth. Most FIs appear to be over-reliant on the self-declaration of the customer to determine the source of funds, and do not perform further verification of the accuracy of the information provided. The approval of senior management can be obtained "within 14 days" from the day on which the account is activated, which will be extended to 30 days when the new provisions on domestic PEPs enter into force. Some FIs confirmed that, during that timeframe, the PEPs can operate the account—the business relationship can therefore be conducted without adequate controls having taken place. According to OSFI's supervisory findings, in some cases, the involvement of senior management occurs even beyond the prescribed timeframe.

223. There are nevertheless some encouraging signs: over the last four fiscal years, FINTRAC assessed non-FRFIs' determination of PEFPs[82] in the context of 2,508 examinations in four different sectors (credit unions and caisses populaires, trust and loan companies, MSB and securities dealers), and identified shortcomings were identified in only four percent of the cases.

224. Several FRFIs, including the D-SIBs,[83] interviewed, apply an onboarding procedure for all customers who include the same determination in relation to "domestic PEPs" and the same enhanced due diligence measures; in order to determine whether a customer is a "domestic PEP," the large banks rely mainly on the information contained in commercial databases. The notion of "domestic PEP" that they apply varies greatly from one institution to the other, and focuses on customers only, i.e., without taking the beneficial owners into account. Some non-FRFIs expressed the need for timely guidance to clarify and facilitate the implementation of the new requirement regarding domestic PEPs and their close associates.

225. DNFBPs, however, are not required to determine whether they are dealing with foreign PEPs. The interviews conducted confirmed that the political role of customers is not an element that DNFBPs take into account in practice to determine whether further mitigation measures are necessary.

226. While FRFIs have adequate record-keeping measures in place, the smaller credit unions, retail money services business and DNFBPs active mainly in the real estate sector implement weaker measures, which are mainly paper based or based on a combination of paper and manual procedures. FINTRAC identified several deficiencies in record-keeping procedures of BC notaries as well, especially with respect to the conveyancing of real estate.

227. Correspondent banking services are mostly offered by D-SIBs. The D-SIBs have a centralized global management and monitoring of correspondent banking relationships. In some cases, they go above and beyond the current requirements: for example, when reviewing correspondent bank relationships, they also take the quality of AML/CFT supervision into account. Controls on correspondent banking seem to be also reviewed through visits on site and testing procedures by the internal audit. According to OSFI supervisory findings, FRFIs properly assess these services as a higher risk activity, taking necessary mitigation measures.

228. Before introducing new technologies and products, banks typically conduct an assessment of the potential ML/TF risks (and, in doing so, go beyond the requirements of Canadian law). Some banks indicated the lack of information from the authorities regarding typologies on possible

[82] The said determination is considered in relation to the following cases: the opening of new accounts (financial entities and securities), when an EFT over Can$10,000 is sent or received (financial entities and MSBs) or a lump sum payment of Can$100,000 or more in respect to an annuity or life insurance policy.

[83] In this respect, OSFI Guidelines B-8, Deterring and detecting ML/TF, explain that FRFIs are not (currently) under any legal obligation to identify domestic PEPs *per se*, nevertheless, where a FRFI is aware that a client is a domestic PEP, the FRFI should assess what effect this may have on the overall assessed risk of the client. If the assessed risk is elevated, the FRFI should apply such enhanced due diligence measures as it considers appropriate.

exploitation of emerging products that would be helpful in their risk assessment. Among the new products it is worth noting that pre-paid cards are used in Canada but are not currently subject to AML/CFT requirements.[84] Nevertheless, OSFI has alerted FRFIs in the context of its inspections to the need to consider that reloadable prepaid cards operate similarly to deposit accounts, and therefore require equivalent mitigation measures. OSFI supervisory findings reveals that in two cases, FIs had failed to integrate their risk assessment regarding prepaid cards into their overall risk assessment methodology as well as to establish effective controls over their agents. Following OSFI's supervisory interventions, the two institutions are now implementing prepaid access controls in reloadable card programs similar to controls over deposit accounts. Regulatory amendments to include prepaid cards in the regulations are being developed. Other new products currently used—albeit to a very limited extent—include virtual currencies,[85] which fall outside the current framework but which the government has proposed to regulate for AML/CFT purposes.[86]

229. Some of the larger FIs and money transfer companies go beyond current requirements for wire transfers and the filing of EFTRs by applying stricter measures: they notably monitor such transfers on a continuous basis through sample checks of wires received on behalf of customers in order to verify whether they contain adequate originator information, and, if not, take up the matter with the originating banks.

230. FIs have a good understanding of their obligations with respect to TFS (see IO.10). MSBs belonging to large networks, although they are not required to screen on a continuous basis their customer base against the sanctions lists, in practice do so. Onsite supervisory inspections revealed, however, deficiencies in the timeliness of the name-screening processes, as well as in their scope (because they do not always extend the screening to the beneficial owners and authorized signers of corporate entities). According to industry representatives and FINTRAC, this is not the case in smaller independent MSBs, where less sophisticated procedures of record-keeping and monitoring are in place.

231. DNFBPs, in particular in the real estate sector, acknowledged that they do not fully understand the requirements related to TFS. They also recognized that their implementation of these requirements is weak, largely because their procedures are mainly paper-based.

[84] Global open loop prepaid card transaction volumes have grown by more than 20 percent over the past four years and were expected to reach 16.9 billion annually in 2014. Despite pre-paid open loop access (thus meaning any financial product that allows customers to load funds to a product that can then be used for purchases and, in some cases, access to cash or person-to-person transfers) has been considered under the NRA of high vulnerability rating, pre-paid cards are not currently subject to AML/CFT requirements.

[85] According to the Canadian Payments Association, as of April 10, 2014, there were between 1,000 and 2,000 daily transactions in Canada involving bitcoin, which represent 1/100 of 1 percent of the total volume of Canada's daily payments transactions. See Senate Canada, Digital Currency: you can't flip this coin!, June 2015, p. 23.

[86] The legislation to include dealing in virtual currencies among MSBs has been passed, and the associated enabling regulations are being developed.

Reporting Obligations and Tipping Off

232. With the exception of casinos, reporting by the DNFBPs sectors is very low, including in high-risk sectors identified in the NRA.

Table 18. Number of STRs Filed by FIs and DNFBPs

	2011–2012	2012–2013	2013–2014	2014–2015
FIs				
Banks	16,739	17,449	16,084	21,325
Credit Unions/Caisses Populaires	11,473	12,217	12,522	16,576
Trust and Loan Company	617	757	702	729
Life Insurance	379	379	453	427
MSB	35,785	42,246	46,158	47,377
Securities dealers	811	1,284	2,087	1,825
DNFBPs				
Accountants	-	1	-	-
BC Notaries	1	-	-	1
Casinos	4,506	4,810	3,472	3,994
DPMS	66	129	235	243
Real Estate	15	22	22	34
Total	70,392	79,294	81,735	92,531

233. Nevertheless, FINTRAC is of the view that the quality of STRs is generally good and improving. The 1,256 examinations conducted in this respect from 2011/12 to 2014/15, revealed that 82 percent of REs examined complied with their obligation. In particular, the REs' write-up for Part G of the reporting form (which relates to the reason for the suspicions) has evolved over the years from a basic summary to a very thorough and complex analysis of the facts. FINTRAC also noted that the percentage of STRs submitted with errors has significantly decreased, namely from 84 percent (in July 2011) to 17 percent (in July 2015). Most FIs interviewed rely on both front line staff and automated monitoring systems to detect suspicions. At the end of their internal evaluation process, if the STR is not filed, a record is kept with the rationale for the lack of reporting. STRs are generally filed within 30 days.

234. Awareness and implementation of reporting obligations vary greatly amongst the various sections. In particular: casinos are adequately aware of their reporting obligations. The larger casinos detect suspicious transactions not only through front-line staff, but also through analytical monitoring tools developed at the corporate level on the transaction performed and on the basis of video-investigation in order to identify possible unusual behaviors (such as passing chips). They also report to FINTRAC suspicious transactions that were merely attempted. The real estate sector, however, appears generally unaware of the need to report suspicious transactions that have not been executed. In brokerage firms, the detection of suspicious transactions is mainly left to the "feeling" of the individual agents, rather than the result of a structured process assisted by specific red flags. MSBs, securities dealers and DPMS have significantly increased the number of STRs filed,

mainly in response to the outreach, awareness raising and monitoring activities performed by FINTRAC. The caisses populaires have also increased their reporting as a result of the centralized system of detection of suspicious transactions developed by the Fédération des Caisses Desjardins du Quebec.

235. The larger REs interviewed had good communication channels with FINTRAC and receive adequate feedback on an annual basis on the quality of their STRs and on the number of convictions related to FINTRAC's disclosure. In particular, a Major Reporter Group was established in FINTRAC to foster dialogue. In this context, FINTRAC hosted, in May 2014, a first forum for D-SIBs to enhance compliance with STRs obligations and targeted feedback sessions, and another, in 2015, for casinos. D-SIBs and casinos met considered these forums particularly helpful. Small banks and most categories of DNFBPs do not to receive the same kind of feedback.

236. Tipping off does not appear to be a significant problem in Canada. REs have included in their internal policies, controls and training initiatives some provisions that address the prohibition of tipping off. The measures are considered effective by FINTRAC. So far, no charges have been laid as regards tipping off.

Internal Controls and Legal/Regulatory Requirements Impending Implementation

237. OSFI supervisory findings conducted in the last three years confirm that FRFIs apply sufficient internal controls to ensure compliance with AML/CFT requirements with the five core elements of the compliance regime.[87] A key OSFI finding is the scope of the two-year review, which is frequently more limited to the existence of controls rather than to their effectiveness.

238. REs with cross-border operations include their overseas branches in their AML/CFT program and extend their internal controls to their foreign subsidiaries. They also adopt the more stringent of Canadian or host jurisdiction rules in their group-wide AML/CFT framework on areas where host country requirements are stricter or more in line with FATF standards. The larger banks reported that they had sharing information mechanisms at group level and, in cases where the local jurisdiction had created obstacles to the information sharing, the local branches were closed.

239. Three of the D-SIBs have branches in Caribbean countries: the two REs interviewed took specific risk mitigating measures by adopting an enterprise-wide management to the highest level. As a result, every high-risk client in the Caribbean must be pre-approved both by senior management in the business and the compliance officer.

[87] Under PCMLTFR s.71(1), the five elements of the compliance regime are the following: appointment of a compliance officer, development and application of written compliance policies and procedures, assessment and documentation of ML/TF risks and of mitigating measures, written ongoing training program, a review of the compliance policies and procedures to test their effectiveness. The review has to be done every two years. Failure to implement any of these five elements is considered serious violation under AMPR and shall lead to an administrative monetary penalty of up to Can$100,000 for each one (ss.4 and 5).

240. The data provided by FINTRAC indicates an uneven level of compliance among non-FRFIs. Credit unions and caisses populaires have good internal controls in place, which is not the case for trust and loan companies, securities dealers, insurance sector and MSBs: several deficiencies have been identified, including incomplete or not updated policies and procedures, the limited scope of controls, a lack of comprehensive assessment of effectiveness, and no communication to senior management.

241. DNFBPs other than casino and BC notaries have either no or weak internal controls. The discussions with real estate sector representatives also revealed some concerns about the effective control of the proper implementation of AML/CFT requirements by their agents. Some DNFBPs professional associations are working with their members to assist them in increasing their level of compliance and in increasing their awareness with their obligations. In this context, the associations felt that further engagement with FINTRAC would be useful.

Overall Conclusions on Immediate Outcome 4

242. Canada has achieved a moderate level of effectiveness for IO.4.

SUPERVISION

A. Key Findings

FINTRAC and OSFI have a good understanding of ML and TF risks; and FIs and DNFBPs are generally subject to appropriate risk-sensitive AML/CFT supervision, but supervision of the real estate and DPMS sectors is not entirely commensurate to the risks in those sectors.

The PCMLTFA is not operative in respect of legal counsels, legal firms, and Quebec notaries—as a result, these professions are not supervised for AML/CFT purposes which represents a major loophole in Canada's regime.

A few providers of financial activities and other services fall outside the scope of Canada's supervisory framework (namely TCSPs other than trust companies, and those dealing with open loop pre-paid card, including non FI providers on line gambling and virtual currency, factoring companies, leasing and financing companies, check cashing business, and unregulated mortgage lenders), but legislative steps have been taken with respect to online gambling, open-loop pre-paid cards and virtual currencies..

Supervisory coverage of FRFIs is good, but the current supervisory model generates some unnecessary duplication of effort between OSFI and FINTRAC.

FINTRAC has increased its supervisory capacity to an adequate level but its sector-specific expertise is still somewhat limited. OSFI conducts effective AML/CFT supervision with limited resources.

Market entry controls are good and fitness and probity checks on directors and senior managers of FRFIs robust. There are, however, no controls for DPMS, and insufficient fit-and-proper monitoring of some REs at the provincial level.

Remedial actions are effectively used but administrative sanctions for breaches of the PCMLTFA are not applied in a proportionate and/or sufficiently dissuasive manner.

Supervisory actions have had a largely positive effect on compliance by REs. Increased guidance and feedback has enhanced awareness and understanding of risks and compliance obligations in the financial sector and to a lesser extent in the DNFBP sector.

B. Recommended Actions

Canada should:

- Ensure that all legal professions active in the areas listed in the standard are subject to AML/CFT supervision.

- Coordinate more effectively supervision of FRFIs by OSFI and FINTRAC to maximize the use of resources and expertise and review implementation of Canada's supervisory approach to FRFIs.
- Ensure that FINTRAC develops sector-specific expertise, continues to have a RBA in its examinations, and applies more intensive supervisory measures to the real estate and DPMS sectors.
- Ensure that there is a shared understanding between FINTRAC and provincial supervisors of ML/TF risks faced by individual REs and ensure adequate controls are in place after market entry at the provincial level to prevent criminals or their associates from owning or controlling FIs and DNFBPs.
- Ensure that the administrative sanctions regime is applied to FRFIs and that AMPs are applied in a proportionate and dissuasive manner including to single or small numbers of serious violations and repeat offenders. Ensure that OSFI's guidelines relating to AML/CFT compliance and fitness and probity measures are subject to the administrative sanctions regime for non-compliance.
- Provide more focused and sector-specific guidance and typologies for the financial sector and further tailored guidance for DNFBPs, particularly with respect to the reporting of suspicious transactions.

The relevant Immediate Outcome considered and assessed in this chapter is IO.3. The recommendations relevant for the assessment of effectiveness under this section are R.26–28, R.34 and 35.

C. Immediate Outcome 3 (Supervision)

Licensing, Registration and Controls Preventing Criminals and Associates from Entering the Market

243. Market entry controls are applied at federal and provincial level. After market entry, there are effective measures in place at the federal level to ensure that when changes in ownership and senior management occur, FRFIs conduct appropriate fitness and probity (F&P) checks. The federal prudential regulator, OSFI, applies robust controls when licensing a federally regulated financial institution (FRFI). Due diligence measures, including criminal background checks on individuals, are carried out at the market entry stage and OSFI has refused or delayed applications when issues arise. OSFI provided an example where it became aware of misconduct by a small domestic bank's former CEO and ultimately undertook a suitability review of the person. OSFI concluded that he was not suitable to be an officer of the bank and recommended that he not be a member of the board. The bank removed the officer and as a result, OSFI's supervisory oversight strategy of the bank was downgraded. After market entry, FRFIs are responsible for implementing controls around the appointment of senior managers and directors of FRFIs under OSFI Guidelines. OSFI supervises FRFIs

for compliance around conducting background checks but this control is not as robust as it is the responsibility of FRFIs to apply fit and proper controls after market entry stage rather than OSFI's in the approval of the appointment of senior managers in FRFIs. Provincial regulators apply market entry controls for non-FRFIs (e.g., securities dealers, credit unions, and caisses populaires). These controls include criminal checks to verify the integrity of applicants and to ensure that RE's implement fit and proper controls. The controls are usually conducted by the RE but are subject to oversight by the provincial regulators. These market entry controls differ between provinces and sectors but, overall, the market entry controls being applied by provincial regulators are robust.

244. Since its last MER, Canada has implemented a money service business (MSB) registration system under the supervision of FINTRAC. One exception to the federal system of registration is in Quebec, where MSBs register with the Autorité des marchés financiers (AMF) and FINTRAC. Applicants for registration undergo criminal record checks and fitness and probity checks by FINTRAC and AMF. Individuals convicted of certain criminal offenses are ineligible to own or control an MSB. FINTRAC monitors the control of MSBs as they are required to submit updated information on owning or controlling individuals or entities when changes occur and again when the MSB applies for renewal of its registration every two years. FINTRAC has refused to register applicants and has revoked registration when the applicant was convicted for a criminal offense. An example was given where FINTRAC revoked the registration of two MSBs after the conviction of two individuals that owned both MSBs. Another example was provided where an MSB terminated its relationship with an agent due to fitness and probity concerns about the agent as part of follow-up activity conducted after an examination by FINTRAC. When an MSB registration is denied, revoked, expired, or pending, FINTRAC follows-up appropriately, for example by conducting an offsite review or onsite visit to the MSBs' last known address to ensure that the entity is not operating illegally.

245. There are market entry controls for most DNFBPs in Canada that require them to be licensed or registered by provincial regulators or by self-regulatory bodies (SRBs). Criminal checks are applied by supervisors and SRBs to casinos, BC notaries, accountants, and real estate brokers and agents during the licensing or registration process. The only exception to this is in the DPMS sector where there is no requirement to be registered or licensed or to be subjected to other forms of controls to operate in Canada. All casinos are provincially owned and apply thorough fit and proper procedures for employees.

246. After market entry, provincial regulators conduct some ongoing monitoring of non-FRFIs and DNFBPs and withdraw licenses or registration for criminal violations. The assessment team was provided with examples of restrictions or cancellations of investment dealers' registration by the Investment Industry Regulatory Organization of Canada (IIROC) due to misconduct or a violation of the law. However, FINTRAC does not have responsibility for the licensing or registration of FIs or DNFBPs (apart from MSBs) and non-federal supervisors do not appear to implement the same level of controls to monitor of non-FRFIs and DNFBPs to ensure that they are not controlled or owned by criminals or their associates after the licensing or registration stage.

Supervisors' Understanding and Identification of ML/TF Risks

247. Supervisors in Canada participated in the NRA process and understand the inherent ML/TF risks in the country. FINTRAC and OSFI have a good understanding of ML/TF risks in the financial and DNFBP sectors.

248. FINTRAC is the primary AML/CFT supervisor for all REs in Canada and is relied upon by provincial regulators to understand ML/TF risks within their population and to carry out AML/CFT specific supervision. Provincial supervisors integrate ML/TF risk into their wider risk assessment models and leverage off FINTRAC for their assessment of ML/TF risks as FINTRAC has responsibility for AML/CFT compliance supervision in Canada.

249. OSFI is the prudential regulator for FRFIs and conducts an ML/TF specific risk assessment that applies an inherent risk rating to entities on a group-wide basis rather than an individual basis. It is also able to leverage off its prudential supervisors to better understand the vulnerabilities of individual FRFIs complementing the results of the NRA. OSFI demonstrated that it understands the FRFIs' ML/TF risks through its risk assessment model that appropriately identifies the vulnerabilities in the different sectors and REs under its supervision. It also collaborates well with FINTRAC and other supervisors on their understanding of ML/TF risk. This is very important strength of Canada's system because FRFIs account for over 80 percent of the financial sector's assets in the country. The sector is dominated by a relatively small number of FRFIs: the six D-SIBs control the banking market and hold a significant portion of the trust and loan company and securities markets in Canada. The largest life insurance companies in Canada are also federally regulated. OSFI has identified 34 FRFIs as high-risk, 32 as medium-risk, and 66 as low-risk. The D-SIBS are all rated as high-risk, given their size, transaction volumes and presence in a range of markets. OSFI updates its risk category for an FRFI or FRFI group on an ongoing basis following onsite assessments, ongoing monitoring and follow-up work. The outcomes from OSFI's risk assessment are effective.

250. FINTRAC has recently developed a sophisticated risk assessment model that assigns risk ratings to sectors and individual REs: the model was reviewed in detail by the assessment team and was compared against the data being collected and analyzed in FINTRAC's case management tool. The model is a comprehensive ML/TF analytical tool that considers various factors to predict the likelihood and consequence of non-compliance by a RE. On the basis of its analysis, it rates reporting sectors and entities and the rating is then used to inform its supervisory strategy. FINTRAC's risk assessment has rated all 31,000 REs under the PCMLTFA and identified banks, credit unions, caisses populaires, securities dealers, MSBs and casinos as high-risk. FINTRAC has incorporated the findings of the NRA into the model to take account of the inherent risk ratings identified in the real estate and DPMS sectors.

251. Other supervisors, notably AMF and IIROC, integrate ML/TF risk into wider operational risk assessment models of entities that they supervise. They rely on FINTRAC to understand the ML/TF risks among all REs and to disseminate this information to prudential or conduct supervisors, given FINTRAC's role as primary supervisor for AML/CFT compliance in Canada. This appears to be happening in cases where AML/CFT issues arise in the course of prudential or conduct supervision.

However, FINTRAC does not share with other supervisors its understanding of ML/TF risks in particular sectors on a regular basis. Provincial supervisors are therefore not aware of the ML/TF risks faced in their respective sectors, particularly around vulnerabilities relevant to ownership and management controls in the non-FRFI and DNFBP sectors. Similarly, FINTRAC and OSFI do not sufficiently share their understanding of detailed risks in FRFIs, e.g., through sharing of existing tools to carry out an integrated risk assessment of all FRFIs. As a result, they do not adequately leverage off their respective knowledge of the different business models and compliance measures in place.

Risk-Based Supervision of Compliance with AML/CFT Requirements

252. The regulatory regime involves both federal and provincial supervisors. FINTRAC is responsible for supervising all FIs and DNFBPs for compliance with their AML/CFT obligations under the PCMLTFA. Other supervisors may incorporate AML/CFT aspects within their wider supervisory responsibilities although the assessment team found that in instances where an AML/CFT issue arose, the primary regulator would refer the issue to FINTRAC. Given the primary responsibility held by FINTRAC for all REs and the federal and provincial division of powers for financial supervision other than in the areas of AML/CFT, combined with the geographical spread of the Canadian regulatory regime, the assessment team focused primarily on FINTRAC and OSFI's supervisory regime, but also met with provincial supervisors (e.g., AMF in Quebec) and other supervisors (e.g., IIROC for investment dealers).

253. FINTRAC has increased its resources and the level of sophistication of its compliance and enforcement program ("supervisory program") in recent years. In 2014/2015, there was 79 full-time staff employed in FINTRAC's supervisory program. Of this, 57 staff members were involved in direct enforcement activities including outreach and engagement (10), reports monitoring (5), examinations (37), and AMPs/NCDs (5). It has also developed, and continues to develop, its supervisory capabilities on a RBA. Its understanding of the different sectors and business models and of how AML/CFT obligations apply taking into account materiality and context is somewhat limited. This was communicated to the assessors by REs in the banking and real estate sectors during the onsite visit. FINTRAC has nevertheless increased its understanding of its different reporting sectors which is a challenge given the large number and diverse range of entities it supervises.

254. A range of supervisory tools is used by FINTRAC to discharge its supervisory responsibilities and, for the most part, those tools are applied consistently with the risks identified. A case management tool determines the level and extent of supervision to be applied to sectors and individual REs scoping specific areas for examinations, recording supervisory findings and managing follow-up activities. High-risk sectors are subject to onsite and desk examinations (details of which are contained in this report). Less intensive supervisory tools are used for lower-risk sectors. These tools include self-assessment questionnaires (Compliance Assessment Reports or CARs); observation letters (setting out deficiencies that require action); Voluntary Self Declarations of Non-Compliance (VSDONC); and policy interpretations on specific issues that require clarification. The use of observation letters was piloted with the caisses populaires sector in 2013/2014. FINTRAC had identified that caisses populaires were reporting large cash transactions of more than Can$10,000

through automated teller machines which was not possible given the low limit on transactions through such machines. Observation letters were used to correct a misinterpretation of reporting obligations and clarify the correct way to report these types of transactions. FINTRAC also uses outreach tools for lower risk sectors assistance and awareness building tools among smaller REs with limited resources, compliance experience and works with industry representatives. While supervisory measures are generally in line with the main ML/TF risks, more intensive supervisory measures should be applied in higher risk areas such as the real estate and DPMS sectors. FINTRAC has updated its risk assessment to identify those sectors as high-risk, in line with the findings of the NRA.

255. OSFI applies a close touch approach to AML/CFT supervision of FRFIs. It engages with FRFIs through its prudential supervisors on an ongoing basis and is well placed to supervise higher-risk entities from an AML/CFT perspective given its knowledge of RE's business models OSFI has a particular focus on the large banking groups (D-SIBs) and insurance companies that dominate the financial market in Canada. These are identified as not only high-risk for prudential purposes but also for ML/TF as identified by OSFI and in the NRA. There is a specialist AML compliance (AMLC) division solely responsible for AML/CFT and sanctions supervision in OSFI and allocates its resources on a risk sensitive basis to supervise FRFIs. OSFI's "AML and ATF (i.e., CFT) Methodology and Assessment Processes" assesses the adequacy of FRFIs' risk management measures through its program of controls and assesses FRFIs' compliance with legislative requirements and OSFI guidelines. The AMLC division has expertise in the sectors it supervises and is covering the principal FRFIs leveraging off prudential supervision. OSFI has a good understanding of its sector, its staff has a high degree of expertise and it is adequately supervising FRFIs for AML/CFT compliance (in conjunction with FINTRAC). The number of OSFI AML/CFT supervisors (i.e., currently 10 supervisors including senior management) is, however, too low given the size of supervisory population and the market share and importance of FRFIs in the Canadian context.

256. FINTRAC and OSFI provided comprehensive statistics, case studies, and sample files relating to examinations of FIs and DNFBPs. There were a greater number of examinations of FIs than DNFBPs; in line with Canada's understanding of ML/TF risk and there were more desk-based than onsite examinations. Between April 2010 and March 2015, 3,431 examinations (1,949 desk-based and 1,482 onsite) of FIs were conducted. During the same period, there were 1,300 examinations (895 desk-based and 405 onsite) of DNFBPs.

Table 19. AML/CFT Examinations Conducted by FINTRAC/OSFI in Canada 2009–2015

Sector	Activity Sector	Number of ERs (primary population)	FINTRAC/OSFI Examinations						
Financial Institutions (FIs)			2009/10	2010/11	2011/12	2012/13	2013/14	2014/15	Total
Financial Entities	Banks	81	11	10	15	10	19	16	81
	Trusts and Loans	75	6	6	13	7	6	7	45

	Credit Unions/Caisse Populaire	699	173	205	432	301	170	165	1,446
Life Insurance	Life Insurance	89	70	54	8	13	123	61	329
Money Service Businesses	Money Service Businesses	850	210	201	426	222	161	143	1,363
Securities Dealers	Securities Dealers	3829	83	120	136	129	167	85	720
Total FI—Desk Exam			270	260	668	389	409	223	2,219
Total FI—Onsite Exam			283	336	362	293	237	254	1,765
Total FIs			553	596	1,030	682	646	477	3,984
DNFBPs			2009/10	2010/11	2011/12	2012/13	2013/14	2014/15	Total
Accountants	Accountants	3,829	48	20	0	25	11	10	114
BC Notaries	BC Notaries	336	0	0	0	16	1	6	23
Casinos	Casinos	39	12	12	5	10	1	6	46
Dealers of Precious Metals and Stones	Dealers of Precious Metals and Stones	642	0	0	10	166	276	2	454
Real Estate	Real Estate	20,784	90	70	40	270	203	140	813
Total DNFBP—Desk Exams			83	41	27	322	391	114	978
Total DNFBP—Onsite Exams			67	61	28	165	101	50	472
Total DNFBPs			150	102	55	487	492	164	1450
Total FIs and DNFBPs—Desk Exams			353	301	695	711	800	337	3197
Total FIs and DNFBPs—Onsite Exams			350	397	390	458	338	304	2237
Total FIs and DNFBPs			703	698	1,085	1,169	1,138	641	5,434

257. Both FINTRAC and OSFI demonstrated that they apply scoping mechanisms within their examination strategies. Factors used by FINTRAC to prioritize examinations include: its follow-up strategy; concurrent assessments (with OSFI); market share; cycles; risk score; theme-based; regional selections and compliance coverage (used for lower risk where the preceding factors may not apply). OSFI primarily relies on its risk rating of FRFIs to inform its examination strategy and supervises on a cyclical basis with high-risk entities supervised on a three-year cycle, medium risk on a four-year

cycle and low risk on a five-year cycle. It does, however, also supervise on a reactive basis arising out of information received from FRFIs, prudential supervisors or FINTRAC. An average onsite examination conducted by FINTRAC lasts between 2–3 days typically involving 2–3 supervisors, whereas onsite examinations of FRFIs typically last between 1 and 3 weeks and involves 10 or more supervisors from both OSFI and FINTRAC.

Supervision of FRFIs

258. Since 2013, FRFIs have been supervised by OSFI and FINTRAC concurrently. This involved examinations of high and medium risk FRFIs by each agency concurrently but with OSFI taking a top down (i.e., group wide) approach and FINTRAC taking a bottom up (i.e., individual entities/sector) approach with the two agencies coordinating their approaches during examinations but issuing separate supervisory letters setting out their respective findings. At the time of the onsite, it was planned to move to a more coordinated approach through joint examinations. Between 2009 and 2015, OSFI and FINTRAC conducted 126 assessments of FRFIs (OSFI carried out 78, FINTRAC carried out 48, and 22 were concurrent). During that period, OSFI and FINTRAC assessed all 6 D-SIBs (18 assessments in total) that hold a significant share of the Canadian financial market. OSFI issued 373 findings, including 97 requirements relating to lack of processes to comply with AML/CFT obligations and 276 recommendations relating to broader prudential AML/CFT risk management findings. The largest number of findings reflected changes that were required to correct or enhance policies or procedures and the failure to ensure that risk assessment processed included prescribed criteria, and weaknesses in applying these criteria.

259. There is good supervisory coverage of FRFIs in Canada, which is being applied on a risk-sensitive basis. The level and intensity of the supervision of FRFIs was detailed to the assessment team by FINTRAC and OSFI, sample files were reviewed and feedback was also received from individual FRFIs during the onsite. OSFI provided examples of examinations and its follow-up activity including an AML/CFT examination of a major bank (D-SIB). A 2010 assessment of the bank found its AML/CFT program to be basic or rudimentary and there were 27 major findings ranging from instances of non-compliance with the PCMLTFA and weak risk management processes and policies. OSFI conducted an extensive follow-up program in tandem with the host regulators. When OSFI determined that the action plan to remedy deficiencies was not progressing satisfactorily it met with senior management in the bank. Enhanced monitoring by OSFI was implemented up until 2013 when the bank had adequately addressed the deficiencies to OSFI's satisfaction. Another example was provided involving a bank, which was a small subsidiary of a foreign bank and identified significant issues in its AML/CFT program, OSFI conducted quarterly monitoring of the bank which resulted in all recommendations being addressed by the bank. OSFI and FINTRAC provided examples where they have leveraged off each-others' supervisory findings including where a conglomerate life insurance company had issues with the process for submitting electronic fund transfer reports to FINTRAC that was subsequently reported to OSFI by FINTRAC that led to a prudential finding by OSFI. FINTRAC has also used OSFI's observations of compliance regime gaps to expand its standard scope of that RE to include a review of the compliance regime.

260. OSFI is taking measures to ensure that FRFIs heighten monitoring around overseas investment in Canada to mitigate any risk of illicit flows of funds entering the financial system. OSFI is also monitoring overseas branches of FRFIs as part of its group wide supervisory approach. There are three D-SIBs with branches in the Caribbean and South America. OSFI supervises FRFI on a group wide basis and FRFIs apply group wide policies and procedures and oversee controls (including ongoing monitoring of transactions) applied in overseas branches in Canada. From the discussions held and the material submitted it was found that OSFI exercises rigorous oversight of parent banks' group-wide controls in this key area.

261. Despite there being good supervisory coverage of FRFIs, the split of AML/CFT supervision generates some duplicative efforts. There are currently two agencies supervising FRFIs for AML/CFT compliance, which may be desirable given the size and importance of FRFIs, but suffers to some extent from insufficient coordination between the two agencies and duplication of supervisory resources. OSFI has a good understanding of its sectors and is implementing an effective supervisory regime with limited resources. FINTRAC has more resources but has a very wide population to supervise for AML/CFT compliance that may hinder a full appreciation of FRFIs' business models.

Supervision of Non-FRFIs and DNFBPs

262. FINTRAC is applying its supervisory program to non-FRFIs and DNFBPs on an RBA. It is conducting more examinations in higher-risk sectors and using assistance, outreach, and compliance questionnaires to a large extent in sectors that it sees as lower-risk.

263. FINTRAC has shown that it is focusing mostly on high-risk non-FRFIs, securities, MSBs, and credit unions/caisses populaires for onsite examinations. It is, however, also conducting onsite examinations in lower-risk sectors, although it is conducting more desk exams in those sectors. FINTRAC also uses other supervisory tools for lower risk REs in the financial sector. Onsite examinations have been undertaken by FINTRAC of non-FRFIs including securities dealers, credit unions, and caisses populaires. The market share of credit unions is concentrated in a relatively small number of credit unions that are being supervised by FINTRAC and credit unions in Canada do not have cross-border operations. Another priority area for FINTRAC is the supervision of MSBs given the high-risk assigned to the sector. It has conducted a high number of examinations of MSBs relative to the size of the primary population figures provided to the assessment team. There appears to be ongoing cooperation between primary regulators and FINTRAC concerning the supervision of non-FRFIs based on details of referrals from other supervisors under MOU arrangements that were provided to the team. FINTRAC is adopting an adequate RBA to supervision of the non-FRFI sector.

264. FINTRAC applies intensive supervisory measures to casinos in line with the risks identified in the sector. This involves in-depth onsite examinations that are conducted on a cyclical basis that ranges from a two to five-year cycle based on key factors such as size, risk level, and market share. The three largest casinos (that represent 80 percent of the sector's market share) are examined on a two-year cycle. For other sectors, it has been relying on less intensive activities such as assistance

and outreach to DNFBPs to build awareness of compliance obligations. FINTRAC identified the real estate sector and DPMS as medium-risk and accordingly is applying less intensive supervisory tools to those sectors. In the NRA, however, both sectors have been identified as high-risk. FINTRAC is therefore updating its risk assessment of these two sectors in line with the findings of the NRA with a view to applying more intensive measures in the future (including onsite examinations). FINTRAC is relying on the risk model (amongst other factors) of real estate agents to decide on examination selections to cover the sector. It also does not appear to identify adequately DPMS businesses in Canada that fall within the definition of the PCMLTFA.

265. FINTRAC utilizes lower intensity activities to good effect for lower-risk REs. Between 2011 and 2013, close to 10,000 compliance questionnaires (CARs) were issued to mainly sectors identified as lower or medium ML/TF risk. The questionnaire results were used to initiate close to 250 "themed-CAR" risk-informed examinations based principally on the significant non-compliance identified in the CAR. Observation letters are also used to highlight repeated non-compliance or reporting anomalies and remedial action is taken if the entity fails to respond or does not resolve the issues.

266. The legal profession is not currently subject to AML/CFT supervision due to a successful constitutional challenge that makes the PCMLTFA inoperative in respect of legal counsels, legal firms, and Quebec notaries. There is therefore no incentive for the profession to apply AML/CFT measures and participate in the detection of potential ML/TF activities. The exclusion of the legal profession from AML/CFT supervision is a significant concern considering the high-risk rating of the sector and its involvement in other high-risk areas such as the real estate transactions as well as company and trust formation. This exclusion also has a negative impact on the effectiveness of the supervisory regime as a whole because it creates an imbalance amongst the various sectors, especially for REs that perform similar functions to lawyers.

Remedial Actions and Effective, Proportionate and Dissuasive Sanctions

267. Supervisors in Canada take a range of remedial actions. There is also an administrative monetary penalties (AMPs) regime in place that is the responsibility of FINTRAC to apply under the PCMLTFA. OSFI and FINTRAC require REs to remediate any deficiencies identified during the assessment process. OSFI has implemented a graduated approach to applying corrective measures or sanctions for FRFIs. Both OSFI and FINTRAC issue supervisory letters to entities subject to AML/CFT assessment that contain supervisory findings and REs are required to take appropriate remedial action. OSFI has provided examples of follow-up action it has taken when FRFI fails to take remedial action.

268. OSFI and FINTRAC have thorough ongoing monitoring and follow-up processes to ensure remediation and have provided examples of steps taken to ensure that deficiencies have been addressed in the FRFI sector, MSBs and a large FI. Measures taken by supervisors include follow-up meetings, further examinations, action plans, and sanctions. OSFI may "stage" FRFIs, which is an enhanced monitoring tool involving four stages where severe AML/CFT deficiencies remain unaddressed. Staging is an effective tool to improve compliance as demonstrated by the Canadian

authorities in case studies. There were examples provided where a small bank had not applied AML/CFT obligations correctly and where a staged RE underwent follow-up examinations demonstrated the process increased compliance. FINTRAC also provided examples of monitoring activities of non-FRFIs and DNFBPs where follow-up meetings and reexaminations of MSBs and large FIs resulted in significant improvements in compliance. Remedial actions have also been applied when REs failed to respond to mandatory CARs in the real estate sector. Follow-up activities on all non-responders found that of 55 non-responders, 37 were inactive REs, 1 was a late responder, 10 had inaccurate addresses, and 7 were true non-responders (i.e., increasing RE's risk profile). Where low levels of reporting have been identified, FINTRAC has conducted examinations and put in place remedial actions to increase reporting. This appears to have had an effect on reporting in the institutions concerned, but does not address the wider issue of general low levels of reporting. Supervisors have demonstrated that effective steps have been taken to a large extent to ensure that remediation measures are in place to address AML/CFT deficiencies.

269. FINTRAC can apply sanctions on all REs (including FRFIs) under the AMP regime. AMPs have been imposed and non-compliance disclosures (NCD) have been made to LEAs by supervisors for serious AML/CFT breaches and failure to address significant deficiencies. A notice of violation (NOV) is issued to the RE outlining the violation and penalty prior to an AMP being imposed. The most common violations cited in a NOV were for compliance regime deficiencies and reporting violations. AMPs are not always made public but can be published in egregious cases. AMPs have been imposed in the credit unions and caisses populaires, securities, MSBs, casinos, and real estate sectors but at the time of the onsite an AMP had not been applied to a FRFI. The imposition of AMPs in the MSB and casino sector was reported to have had a significant dissuasive effect in those sectors and FINTRAC confirmed that compliance had improved in those sectors as a result. However, the level of AMPs being applied is low relative to the reporting population and the size of the Canadian market. AMPs had not been applied to FRFIs at the time of the onsite is an issue that needs to be addressed. The non-sanctioning of FRFIs, the low number of AMPs applied to other FIs and the low level of fines imposed to date is unlikely to have a dissuasive effect on FRFIs/larger FIs given their market share and the resources available to them. FINTRAC provided the assessors with current statistics at the time of the onsite (see table below) and with figures for NOVs, which included, among others, the FRFI sector, but for which proceedings were not concluded. OSFI has published guidelines for FRFIs on AML/CFT compliance, and while these guidelines cannot result in a financial penalty under OSFI's regulatory enforcement regime they are subject to measures such as staging.

Table 20. Administrative Monetary Penalties for AML/CFT Breaches Between April 1, 2010 and March 31, 2015

Sector	NOV Issued	Reporting Entity Size				Total Value of NOVs Issued	Publicly Named
		Micro	Small	Medium	Large		
Casino	4	0	0	0	4	2,435,500	0
Financial Entities	15	0	6	9	0	897,705	3

MSB	28	22	5	1	0	768,375	16
Real Estate	7	6	1	0	0	197,310	2
Securities	5	0	3	2	0	587,510	4
Total	**59**	**28**	**15**	**12**	**4**	**Can$4,886,400**	**25**

270. FINTRAC can submit an NCD to LEAs for failure to comply with the PCMLTFA, but this is only done in the most serious cases. Between 2010/2011 and 2014/2015, FINTRAC submitted seven NCDs (all from the MSB sector). These resulted in five investigations being commenced with two cases leading to criminal charges and one conviction (two individuals and one RE).

271. There are proportionate remedial actions being taken by supervisors, in particular extensive follow-up activities by supervisors (e.g., staging by OSFI) that demonstrated their dissuasive effect on the RE involved in the process as it exposes the RE being "staged" to costly remedial activities over a long period of time and ancillary costs such as higher deposit insurance premiums. While remedial actions, as opposed to AMPs, appear effective with respect to the individual RE they apply to, their wider dissuasive impact on other entities is limited, notably because they are not made public. More importantly, the lack of AMPs being applied to FRFIs and the relatively low level of fines imposed negatively impact the effectiveness of the enforcement regime as it affects its dissuasiveness. The non-application of the AMP regime to OSFI guidelines also affects the effectiveness of the Canadian supervisory regime.

Impact of Supervisory Actions on Compliance

272. FINTRAC and OSFI provided examples where their actions have had an effect on compliance through the use of action plans, follow-up activities and findings from subsequent examinations. Feedback from the private sector indicates that supervisors' actions have led to increased compliance in the financial sector. There were examples given of increased compliance in the FRFI, MSB and insurance sectors arising out of examinations and follow-up activities conducted by supervisors. It was reported by the private sector that the "close touch" nature of OSFI's supervision has enhanced compliance by FRFIs with their AML/CFT obligations. There has been an increase in compliance by REs as FINTRAC's compliance activities increased in recent years, e.g., MSB and casinos, and with the publication of additional information about PCMLTFA obligations.

273. FINTRAC and OSFI have provided written examples of examination findings and follow-up outcomes that demonstrate their effect on compliance by specific FIs and DNFBPs. There has been an increase in compliance among FRFIs and non-FRFIs (casinos) that are subject to cyclical examinations. The more intensive focus on higher risk areas in examination selection strategies has increased compliance in sectors such as FRFIs, MSBs, securities dealers, and credit unions.

274. OSFI and FINTRAC supervisory measures to ensure compliance and their remedial actions are having a clear effect on the level of compliance of the individual RE that they apply to. OSFI has a robust follow-up system to monitor the remediation of deficiencies identified. OSFI requires FRFIs provide documentary evidence supporting progress on a continuous basis and requires validation

prior to closure of every finding. Quarterly monitoring meetings are conducted with every D-SIB, and meetings with other FRFIs are frequently conducted at the request of OSFI or the FI when there are significant concerns or outstanding issues. Significant remedial steps have been taken by FRFIs based on findings by supervisors and OSFI has demonstrated that it has comprehensive supervisory measures to ensure compliance including the use of more intensive supervision (staging). FINTRAC's follow-up activities have been shown to have a positive effect on compliance by non-FRFIs and DNFBPs. It conducted 515 subsequent examinations across non-FRFIs and DNFBPs over a three-year period and by comparing previous performance indicators with the follow-up indicators revealed that the average deficiency rate had reduced by 13 percent due to increased compliance. AMPs, when applied, have also had a positive effect on the compliance of REs as demonstrated in follow-up examinations.

275. FINTRAC uses a supervisory tool that assigns "deficiency rates" to REs that are examined. It rates the levels of non-compliance on each specific area of the examination that leads to an overall deficiency rating being assigned to the RE. The overall rating is high, medium, or low and the RE's rating is used to tailor appropriate remedial measures to be put in place. Once remediation has occurred, a follow-up rating is applied and this is compared with the previous rating to identify whether compliance improvements have been made by the RE. The use of deficiency rates at RE and sector level is a useful tool to measure the effect the examination and follow-up process has on compliance by REs. Overall, supervisory measures taken in Canada are having an effect on compliance with improvements demonstrated—albeit to varying degrees—both in the financial and DNFBP sectors. Information provided indicates that compliance has improved in the financial sector, but less so in DNFBPs particularly in the real estate and DPMS sectors.

Promoting a Clear Understanding of AML/CTF Obligations and ML/TF Risks

276. There is a good relationship and open dialogue between OSFI and FRFIs. The private sector reports that OSFI has a good understanding of the compliance challenges faced by FRFIs and provides constructive feedback. OSFI has published compliance guidelines and raises awareness through participation in outreach activities. FINTRAC has published a substantial amount of guidance on its website and increased its level of feedback and guidance to both the financial and, albeit to a lesser extent, the DNFBP sectors. FINTRAC deals with general enquiries through a dedicated call line and has published query specific policy interpretations, both of which are reported by the private sector to be good guidance tools. FINTRAC has dealt with a substantial amount of queries and it has a "Major Reporters" team that provides guidance directly to the largest reporters (mostly financial sector and casinos). It has also taken good steps to raise awareness amongst the MSB sector around the requirement to register and to explain AML/CFT obligations. However, more focused and sector-specific guidance and typologies is required for the financial sector as well as further tailored guidance for DNFBPs to enhance their understanding of the ML/TF risks that they face and of their AML/CFT obligations, particularly with respect to the reporting of suspicious transactions.

277. Supervisors have increased AML/CFT awareness through the use of presentations, seminars, public-private sector forums, establishment of OSFI supervisory colleges, and meetings

with the industry. FINTRAC has engaged with non-FRFIs and DNFBPs conducting 300 presentations between 2009 and 2015. It has also hosted events to raise awareness on compliance obligations including a Major Reporters Forum in the financial sector in 2014 and a Casino Forum in 2015.

278. Overall, in light of supervisors' efforts and ML/TF risks in Canada, FINTRAC provides good quality general guidance to REs, but not enough sector-specific compliance guidance and typologies especially in the real estate and DPMS sectors.

Overall Conclusions on Immediate Outcome 3

279. Canada has achieved a substantial level of effectiveness with IO.3.

LEGAL PERSONS AND ARRANGEMENTS

A. Key Findings

Canadian legal entities and arrangements are at a high risk of misuse for ML/TF and mitigating measures are insufficient both in terms of scope and effectiveness.

Some basic information on legal persons is publicly available. However, nominee shareholder arrangements and, in limited circumstances bearer shares, pose challenges in ensuring accurate, basic shareholder information.

Most TCSPs, including those operated by lawyers, are outside the scope of the AML/CFT obligations and DNFBPs are not required to collect beneficial ownership information. These pose significant loopholes in the regime (both in terms of prevention and access by the authorities to information).

FIs do not verify beneficial ownership information in a consistent manner.

The authorities rely mostly on LEAs' extensive powers to access information collected by REs. However, there are still many legal entities in Canada for which beneficial ownership information is not collected and is therefore not accessible to the authorities.

Access to beneficial ownership is not timely in all cases and beneficial ownership information is not sufficiently used.

For the majority of trusts in Canada, beneficial ownership information is not collected.

LEAs do not pay adequate attention to the potential misuse of legal entities or trusts, in particular in cases of complex structures.

B. Recommended Actions

Canada should:

- As a matter of priority, increase timeliness of access by for competent authorities to accurate and up-to-date beneficial ownership information—consider additional measures to supplement the current framework.
- Take the necessary steps to make the AML/CFT requirements operative with regards to all legal professions providing company or trust-related services.
- Ensure that FIs and DNFBPs identify and take reasonable measures to verify the identity of beneficial owners based on official and reliable documents.

- Take appropriate measures to prevent the misuse of nominee shareholding and director arrangements and bearer shares.
- Ensure that basic information indicated in provincial and federal company registers is accurate and up-to-date.
- Apply proportionate and dissuasive sanctions for failure by companies to keep records; to file information with the relevant registry; or to update registered information within the required 15-day period.
- Determine and enhance the awareness of the ML and TF risks from an operational perspective and the means through which legal persons and trusts are abused in Canada, taking into account ML schemes investigated in Canada as well as international typologies involving legal entities and legal arrangements.

The relevant Immediate Outcome considered and assessed in this chapter is IO.5. The recommendations relevant for the assessment of effectiveness under this section are R.24 and 25.

C. Immediate Outcome 5 (Legal Persons and Arrangements)

Public Availability of Information on the Creation and Types of Legal Persons and Arrangements

280. Innovation, Science and Economic Development Canada (ISED, formerly Industry Canada) provides a comprehensive overview and comparison on its internet homepage of the various types, forms, and basic features of federal corporations under CBCA, and gives detailed guidance on the incorporation process.[88] Similar information and services are provided through the homepages of all provincial governments except that of New Brunswick. The relevant web links are easy to find through ISEDC's homepage and provide public access to the relevant provincial laws that describe the various legal entities available; the name and contact information for the relevant authority competent for registration; and the procedures to be followed to establish a legal entity. In addition, the Canada Business Network, a collaborative arrangement among federal departments and agencies, provincial and territorial governments, and not-for-profit entities aimed at encouraging entrepreneurship and innovation also provides comprehensive information on the various types of legal entities as well as various forms of partnerships available at the federal and provincial/territorial levels.[89] For legal arrangements, the CRA provides on its homepage comprehensive information on the various trusts structures available under Canadian law.[90]

[88] See www.ic.gc.ca/eic/site/cd-dgc.nsf/eng/cs04843.html#articles.

[89] See www.canadabusiness.ca/eng/page/2853/#toc- corporations.

[90] See www.cra-arc.gc.ca/tx/trsts/typs-eng.html.

Identification, Assessment and Understanding of ML/TF Risks and Vulnerabilities of Legal Entities

281. Both legal entities and legal arrangements in Canada are at a high risk of being abused for ML/TF purposes. The NRA indicates that organized crime and third-party ML schemes pose a very high ML threat in Canada. Some of FINTRAC's statistics reflected in the NRA suggest that well over 70 percent of all ML cases and slightly more than 50 percent of TF cases involved legal entities. Canadian legal entities play a role in the context of channeling foreign POC into or through Canada, as well as in the laundering of domestically generated proceeds.[91] Typologies identified include: foreign PEPs creating legal entities in Canada to facilitate the purchase, of real estate and other assets with the proceeds of corruption; laundering criminal proceeds through shell companies in Canada and wiring the funds to offshore jurisdictions; and utilization of Canadian front companies to layer and legitimize unexplained sources of income and to commingle them with or mask them as profits from legitimate businesses.[92]

282. LEAs generally concurred with the NRA's findings, and have observed a high number of companies being established without carrying out any business activities, and the use of corporate entities and trusts in Canada to facilitate foreign investment. LEAs also stated that they encounter difficulties in identifying beneficial owners of Canadian companies owned by entities established abroad, particularly in the Caribbean, Middle East, and Asia. While the legal powers available to LEAs are comprehensive and sufficient, the instances in which LEAs were able to identify the beneficial owners of Canadian legal entities and legal arrangements appear to have been very limited and investigations do not sufficiently focus on international and complex ML cases involving corporate elements. Some LEAs are therefore less familiar with ML typologies involving corporate structures. Also, in a number of cases that have been investigated and where Canadian companies were owned by foreign entities or foreign trusts, it was not possible for LEAs to identify the beneficial owners.

Mitigating Measures to Prevent the Misuse of Legal Persons and Arrangements

283. Canada has a range of measures available to collect information on the control and ownership structures of legal entities as outlined below, and comprehensive investigation powers to locate and obtain such information if and as needed (see also R.24). (i) In cases where a legal entity enters into a business relationship with a Canada FI, that FI must collect and keep beneficial ownership information. (ii) The federal register or the provincial register where the legal entity is incorporated must collect information; and the CRA collects information on legal entities as part of the tax return. (iii) The legal entities themselves are required to keep records of their activities, shareholders and directors. For public companies listed on the stock exchange disclosure requirements exist for shareholders with direct or indirect control over more than 10 percent of the

[91] FINTRAC Research Brief: Review of Money Laundering Court Case between 2000 and 2014 determines that one of the most frequently used vehicles for ML (in a sample of 40 Canadian Court Cases reviewed) were companies acting as shells for or allowing for a commingling of illicit proceeds with regular business transactions.

[92] Ibid., as well as Project Loupe and Project Chun.

company's voting rights. Only measure (iii)—maintenance of records by the companies—apply to all legal entities created in Canada.

284. Legal entities in a business relationship with a Canadian FI must provide basic and beneficial ownership information to the FI which has an obligation under the PCMLTFA to maintain this information and confirm its accuracy as needed (see R.10). Many of the FIs that the assessors met confirmed that beneficial ownership would generally be obtained through self-disclosure by the customer, and, in some instances, be followed by an open data search to confirm the accuracy of the information provided. Most FIs stated that they would not require the customer to provide official documents to establish the identity of the beneficial owners, nor carry out any independent verification measures other than the open data search. Of the 2.5 million registered legal entities in Canada and customers of a Canada FI, only a fraction had accuracy checks performed with respect to beneficial ownership. In addition, the mitigation of risks is limited by the fact that TCSPs, including those operated by lawyers, are outside the scope of the AML/CFT obligations and DNFBPs are not required to collect beneficial ownership information.

285. Federal and provincial registers record basic information on Canada companies and their directors, as well as on partnerships with businesses in Canada, but do not require the collection of beneficial ownership information. Alberta and Quebec have slightly more comprehensive registration mechanisms, which also cover shareholder information. All information maintained in the federal and provincial registers is publicly available. Updating requirements exist and violations thereof can be sanctioned criminally, but no sanction has been imposed in practice. The reliability of the information recorded raises concerns because there is no obligation on registrars to confirm the accuracy of the basic company information provided at the time of incorporation. Once the incorporation has been completed, companies are obliged to update their records held by the government registrar when there is a material change (e.g., a change in directors) and on an annual basis, and may do so electronically. The same situation applies to partnerships that register for a business permit. The updating process of registered information involves the company reviewing the information indicated in the register and confirming that the information is still correct. There is no need to submit any supporting documents. Despite the absence of verification process at the company registration stage, LEAs stated that basic company information would generally be reliable and comprehensive both on the provincial and federal levels, but they also raised concerns with respect to the accuracy and completeness of shareholder information in the registers of Quebec and Alberta. The CRA, as part of its tax revenue collection obligation, also obtains information on legal entities. However, such information does not include beneficial ownership information.

286. All legal entities, whether incorporated or registered at the federal or provincial level, are subject to record-keeping obligations. All statutes require the keeping of share registers, basic company information, accounting records, director meeting minutes, shareholder meeting minutes and the company bylaws and related amendments. While the relevant obligations are relatively comprehensive, their implementation raises serious concerns. ISEDC and provincial company registries indicated that they would consider company laws to be "self-enforcing" by shareholders, interested parties and the courts, and that they would have no mandate to enforce the

implementation of the relevant provisions. While the Director of Corporations Canada has statutory powers to inspect company records, this power has been used only in the context of a shareholder's complaint and not to verify whether a company complies with its record-keeping obligations or to assist the RCMP in obtaining relevant information. So far, no company has been sanctioned criminally for failure to keep accurate and comprehensive company records. The LEAs expressed concern over the accuracy and completeness of companies' records, and stated that it would often be difficult to establish the true shareholder of a company as shareholder registers would often be either outdated or imprecise as they would not indicate whether the registered shareholder is the actual beneficial owner of the share or a proxy for another person.

287. Disclosure obligations for publicly listed companies are comprehensive and include beneficial ownership information.

288. Both bearer shares and nominee shareholders and directors are permitted in Canada. According to the authorities, bearer shares are rarely issued, but nominee shareholder arrangements are a frequent occurrence, and typically involve the issuance of shares in the name of a lawyer, who holds the shares on behalf of the beneficial owner. While companies are generally obliged to keep share registers, there is no obligation on nominees to disclose their status and information on the identity of their nominator, nor to indicate when changes occur in the beneficial ownership of the share.

Timely Access to Adequate, Accurate and Current Basic and Beneficial Ownership

289. For information that is not publicly available, Canada has a wide range of law enforcement powers available to obtain beneficial ownership information as discussed in R.24. While the legal powers available to LEAs are comprehensive and sufficient, the instances in which LEAs were able to identify the beneficial owners of Canadian legal entities or legal arrangements appear to have been very limited and investigations do not sufficiently focus on international and complex ML cases involving corporate elements. In a number of cases that have been investigated and where Canadian companies were owned by foreign entities or foreign trusts, it was not possible for LEAs to identify the beneficial owners. This was due mainly to foreign jurisdictions not responding to requests by the Canadian authorities for beneficial ownership information.

290. As indicated in IO.6, other important practical limitations hamper the effectiveness of investigations relating to legal entities and legal arrangements. Despite the adequacy of their powers, it is often difficult for LEAs to obtain beneficial ownership information. As a result, their access to that information is not timely. The relevant Director under each corporate statute has the power to request company records but in practice this power has never been used to assist the RCMP in obtaining beneficial ownership information on a specific legal entity. Equally, at the time of the onsite visit the CRA had not made use of its newly acquired power to refer information to the RCMP in case of a suspicion of a listed serious offense.

Timely Access to Adequate, Accurate and Current Basic and Beneficial Ownership Information on Legal Arrangements

291. The level of transparency of legal arrangements is even lower than in the case of legal entities. There are two mechanisms in place to collect information on trusts: (i) the CRA, as part of the tax collection process, requires the provision of information on the trust assets and the trustee; and (ii) FIs are required to obtain information in relation to customers that are or represent a trust. These two measures suffer from significant shortcomings, both in terms of their scope and effective implementation, for the same reasons as in the context of legal persons, and only a small fraction of Canadian trusts file annual tax returns. There is also a fiduciary duty under common law principles of trustees vis-a-vis those who have an interest in the trust. While this makes it necessary for the trustee to know who the beneficiaries are, it does not necessarily mean that trustees keep records or obtain information on the beneficial ownership of the trust in practice.

292. The information collected by FIs about legal arrangements raise the same concerns of reliability as outlined for legal entities because FIs rely mostly on the customer to declare the relevant information, they do not require official documentation to establish the identity of the beneficial owners, and do not conduct an independent verification of the information provided. Furthermore, there is no obligation on trustees to declare their status to the FI. As a result, in many cases, the FI may not know that the customer is acting as a trustee. It is unclear how many of the millions of trusts estimated to exist under Canadian law are linked with a Canadian FI.

Effectiveness, Proportionality and Dissuasiveness of Sanctions

293. Proportionate and dissuasive criminal sanctions are available under the PCMLTFA, the CBCA and provincial laws for failure by any person to comply with the record-keeping obligations or registration or updating requirements under the law (see write up for R.24 for more details), but none have been imposed between 2009 and 2014.

294. So far, there seems to have been few instances in which administrative measures were applied for a failure by FIs to identify the beneficial owner or confirm the accuracy of the information received. Similarly, no legal entity in Canada has been struck off the company registry based on in its involvement in illicit conduct. In sum, sanctions have not been applied in an effective and proportionate manner.

Overall Conclusions on Immediate Outcome 5

295. Canada has achieved a low level of effectiveness for IO.5.

INTERNATIONAL COOPERATION

A. Key Findings

International cooperation is important given Canada's context, and Canada has the main tools necessary to cooperate effectively, including a central authority supported by provincial prosecution services and federal counsel in regional offices.

The authorities undertake a range of activities on behalf of other countries and feedback from delegations on the timeliness and quality of the assistance provided is largely positive. Assistance with timely access to accurate beneficial ownership information is, however, challenging, and some concerns were raised by some Canadian LEAs about delays in the processing of some requests.

The extradition framework is adequately implemented.

Canada also solicits other countries' assistance to fight TF and, to a somewhat lesser extent, ML.

Informal cooperation appears effective amongst all relevant authorities, more fluid and more frequently used than formal cooperation, but the impossibility for FINTRAC to obtain additional information from REs, and the low quantity of STRs filed by DNFBPs limit the range of assistance it can provide.

B. Recommended Actions

Canada should:

- Ensure that, where informal cooperation is not sufficient, LEAs make greater use of MLA to trace and seize/restraint POC and other assets laundered abroad.
- Ensure that good practices, such as consultation with prosecution services are applied across police services with a view to improve the use of MLA to identify and pursue ML, associated predicate offenses and TF cases with transnational elements.
- Assess and mitigate the causes for the delays in the processing of incoming and outgoing MLA requests.
- Consider amending the MLACMA to include the interception of private communications (either by telephone, email, messaging, or other new technologies) as a measure that can be taken by the authorities in response of a foreign country's MLA request without the need to open a Canadian investigation.

The relevant Immediate Outcome considered and assessed in this chapter is IO.2. The recommendations relevant for the assessment of effectiveness under this section are R.36–40.

C. Immediate Outcome 2 (International Cooperation)

Providing and Seeking Constructive and Timely MLA and Extradition

296. Since its previous assessment, Canada has greatly improved its statistics on MLA, and is now able to show several different aspects of MLA related to ML and TF. Canada receives a large number of MLA requests each year. From 2008 to 2015, it received a total of 4,087 MLA requests across all offenses, including 383 for ML investigations and 34 related to TF investigations.

297. The IAG[93] prioritizes the requests (in terms of urgency, court date or other deadline, seriousness of the offense, whether the offense is ongoing, danger of loss of evidence, etc.); it contacts the foreign authorities to obtain further information if the request is incomplete or unclear; and forwards it to the Canadian police for execution (if no court order is needed), or to the IAG's provincial counterparts, or to a counsel within federal DOJ Litigation Branch, if a court order is required.

298. Canada generally provides the requested assistance, both in the context of ML and TF cases:

Table 21. Outcome of Incoming MLA Requests for ML

FISCAL YEAR	EXECUTED	WITHDRAWN	ABANDONED	REFUSED
2008–2009	24	0	4	2
2009–2010	23	1	1	0
2010–2011	21	1	5	1
2011–2012	42	5	4	0
2012–2013	39	1	8	3
2013–2014	56	5	8	0
2014–2015	48	4	6	1
TOTAL	253	17	36	7

Table 22. Outcome of Incoming MLA Requests for TF

FISCAL YEAR	EXECUTED	WITHDRAWN	ABANDONED	REFUSED
2008–2009	10	0	0	0
2009–2010	2	1	2	0
2010–2011	6	0	0	0

[93] The IAG is part of the Litigation Branch of the federal DOJ, and which assists the Minister of Justice as central authority for Canada.

2011–2012	3	1	1	0
2012–2013	5	0	0	0
2013–2014	0	1	0	0
2014–2015	8	0	0	0
TOTAL	34	3	3	0

299. The assistance provided is of good quality, as was confirmed by the feedback received from 46 countries. There have been numerous good cases of assistance, especially with the U.S., including covert operations, joint investigations and extraditions. This is an important positive output of the Canadian framework in light of the risk context (e.g., the extensive border with the U.S., the size of the U.S. economy, and the opportunities it offers to criminal activity).

300. Canada undertakes a range of activities on behalf of other countries. It is, however, limited in its ability to provide in a timely manner accurate beneficial ownership information of legal persons and arrangements established in Canada, for the reasons detailed in IO.5 and IO.7. The fact that Canada cannot intercept, upon request, private communications (either telephone or messaging) in the absence of a Canadian investigation can also hamper foreign investigations, especially those pertaining to OCGs from or with links to Canada or international ML. While this measure is not specifically required by the standard, it is particularly relevant in the Canadian context given the high risk emanating from OCGs, including those with ties to other countries. The scope of this practical shortcoming is, however, limited by the fact that, in most instances, a domestic investigation is likely to be initiated, thus enabling the Canadian authorities to share evidence collected from wiretaps.

301. To facilitate MLA, Canada entered into 17 administrative arrangements with non-treaty partners over the past two years. It also executed over 300 non-treaty requests, mostly to interview witnesses and to provide publicly available documents.

302. Measures were also taken to expedite MLA. The IAG may now send the information requested by a foreign country directly, without the need for a second judicial order. The evidence shared includes, for example, transmission data for an electronic or telephonic message, which help identify the party communicating, tracking data that identify the location of a person or an object, information about a bank account and the account holder. In addition, LEAs that have obtained evidence lawfully for the purposes of their own investigation, may share this information with foreign counterparts without the need for a judicial order authorizing this sharing. For example, evidence obtained through wiretapping by Canadian police may be shared with foreign counterparts in this manner, as confirmed by case law.[94]

303. According to the feedback from delegations, the average time for Canada to respond to their requests varies between 4 and 10 months. The majority of delegations stated that assistance was timely, or did not comment on timeliness, with only one country commenting that the process

[94] See Supreme Court's decision in *Wakeling v. United States of America* 2014, SCC 72.

was slow. Some Canadian LEAs also expressed concerns with the length of time taken to process some of the incoming and outgoing requests. The IAG explains that some of the factors that contribute to lengthening the process include: (i) missing information in the request and the requesting state's slow response to requests for clarification or additional information; (ii) litigation (i.e., when a party affected by the request contests the validity of the court order required, particularly in instances the litigation continues into appellate courts; (iii) because the fact that Canada is awaiting the fulfillment of a condition by the foreign authorities (e.g., in cases where Canada has restrained assets, a final judgment of forfeiture issued by the relevant foreign court may be pending); and (iv) the complexity of the file (e.g., cases involving multiple bank accounts, many witnesses, several Canadian provinces and successive supplemental requests). According to the Auditor General Report 2014, the DOJ processes formal requests for extradition and obtains evidence from abroad appropriately, but does not monitor the reasons for delays in the process.[95] The report found that only 15 percent of the overall time needed to process MLA requests are within Justice Canada's control, and 30 percent of the overall time to process extradition requests are within its control. Justice Canada can only take actions to mitigate the delays when it develops insight about the reasons for the delays. In response to the comments by the Auditor General of Canada and after consultations with its international partners and closer research of its files in more recent years, there has been a significant reduction in the delays associated with executing MLA requests made to Canada.

304. Canada extradites its nationals. Pursuant to the Supreme Court of Canada's decision in *U.S. v. Cotroni*, where the extradition of a Canadian citizen is sought based on facts that might form the basis for a prosecution in Canada, certain consultations and an assessment of evidence and circumstances must take place before a decision can be made as to whether to prosecute or extradite. In 99 percent of such cases, the circumstances favor extradition. Between 2008 and 2015, Canada received 92 extradition requests based on a charge for ML. From the 92 requests, 77 came from the U.S. As a result of these requests, a total of 48 persons were extradited, while 13 were subject to other measures such as deportation, discharge, voluntary return, or were not located or the means of the return not listed. In the seven cases where the request was refused, the grounds were related either to insufficient evidence to show knowledge of ML, concerns with human rights record or prison conditions in the requesting state, or the defendant was not located. Between 2008 and 2015, five persons were extradited for TF.

305. More than half (52 percent) of the extradition requests take from 18 months to five years to be completed; from which 28 percent take from three to five years to be completed. An approximate of 4 percent take more than five years to be completed. Most of the delegations mentioned having successful extradition requests with Canada, although some mentioned having experienced delayed responses from the Canadian authorities regarding those requests.

[95] Report of the Auditor General of Canada—Fall 2014, p. 11, available at http://www.oag-bvg.gc.ca/internet/docs/parl_oag_201411_02_e.pdf. The assessors reviewed 50 extradition and MLA files from between 2011 and 2013, which included incoming and outgoing requests, and both ongoing and closed files.

Seeking Timely Legal Assistance to Pursue Domestic ML, Associated Predicate and TF Cases with Transnational Elements

306. From 2008 to 2015, Canada sent more than 700 MLA requests, including 124 (i.e., around 17 percent) on the grounds of ML charges. Some requests were made, e.g., in the context of real estate or to obtain bank records, as well as to freeze and confiscate funds or assets abroad.[96] Most of these requests were made on the basis of investigations conducted in the province of Quebec (which is in line with the findings in IO.7 and IO.8). Between 2008 and 2015, Canada also made 24 requests in the context of TF investigations, 11 of which during fiscal year 2014/2015 in light of increased concern about "foreign fighters."

307. The number of request for assistance on ML cases has increased over the years, but still appears relatively low in light of Canada's risk profile. The authorities explained that they frequently have recourse to informal means of cooperation (see core issue 2.3 below) in lieu of MLA because it is quicker. However, while informal means do simplify and expedite the process of assistance, they cannot substitute formal MLA in all cases (e.g., when there is a need for the tracing or the freezing of assets abroad). The relatively small number of outgoing requests may also be explained by the fact that Canada is not pursuing complex and transnational ML schemes to the extent that it should (see IO.7). Although the outflows of POC generated in Canada appear to be moderate in comparison to the inflows of POC generated abroad, data suggests that Canadian citizens and corporations use tax havens and offshore financial centers to evade taxes, in particular those located in the Caribbean, Europe, and Asia—cooperation with the relevant countries in these regions would therefore prove helpful to Canada. Some domestic provincial LEAs mentioned concerns about the delay in the sending of requests to foreign countries. In response to that point, the IAG assures that the same case management prioritization measures are in place for outgoing requests as for incoming requests.

Seeking and Providing Other Forms of International Cooperation for AML/CTF Purposes

308. Canadian agencies regularly seek and provide other forms of international cooperation to exchange financial intelligence and other information with foreign counterparts for AML/CFT purposes. In particular, the cases studies provided as well as the discussions held onsite indicate a regular use by LEAs of foreign experts, missions abroad to secure evidence and assets, and joint investigations. Canada does not separate the information according to the function (i.e., seeker or provider of assistance), and the information provided therefore combines the objects of core issues 2.3 and 2.4.

309. FINTRAC is both a FIU and a regulator/supervisor:

- As Canada's FIU: FINTRAC is a member of the Egmont Group and shares information only on the basis of MOUs with counterparts. FINTRAC is open to sign a MOU with any FIU, and

[96] From 2008 to 2005, Canada sent 113 requests with respect to tracing (bank or real estate records) and 33 requests with respect to freezing/restraint (funds or assets).

the process can be concluded very quickly, but sometimes this does not happen due to the absence of interest of the foreign FIU. At the time of the onsite there were 92 MOUs with foreign FIUs. In the absence of an MOU, they cannot share information. According to the feedback provided by other delegations, the information provided by FINTRAC is of good quality. Nevertheless, some limitations have a negative impact on the type of information that FINTRAC can share: more specifically, the fact that (i) FINTRAC is not habilitated to request and obtain further information from any REs; (ii) there are no STRs from lawyers. Canada receives far more requests for assistance than it sends to support Canadian investigations and prosecutions. Although there were fewer queries sent to its foreign counterparts a few years ago, FINTRAC has recently increased the number of requests sent. The queries received and sent to the U.S. (which, as mentioned above, is a major Canadian partner in international cooperation) are generally comparable. In addition to requests sent, the significant increase of FINTRAC's numbers of proactive disclosures sent to its counterparts (2012–2013:52; 2013–2014:93; 2014–2015:190) highlights the Canadian FIU's willingness to share the relevant information it holds with its foreign partners.

- As a supervisor, FINTRAC regularly shares information with foreign supervisors and consults with international partners. In addition to general information, it also exchanges, on an on-going basis, since 2009, compliance information on operational processes with AUSTRAC. After several bilateral meetings, FINTRAC and AUSTRAC are working together in compliance actions on an MSB that operates both in Canada and in Australia. FINTRAC's public MSB registry was also provided to Australia and other jurisdictions, because the comparison of MSB lists is useful during the criminal record check of MSBs, who may operate in more than one country. FINTRAC has also an MOU with FINCEN.

310. The RCMP regularly exchanges information with its foreign counterparts. Cooperation is developed through police channels (Interpol, Europol, Five Eyes Law Enforcement Group), through the Camden Asset Recovery Informal Network (CARIN) and through several MOUs, including one with The People's Republic of China. The existence of this MOU with China is important in light of the risks of inward flow of illicit money generated in China; however, no assistance with this country was reported in the province of British Columbia, despite the fact that it appears to be at greater risk of seeing its real estate sector misused to launder POC generated in China. The RCMP uses a well-established and effective network of liaisons officers (42 officers and 10 intelligence analysts in 26 countries) to seek and provide assistance and other types of information, in ML and TF investigations. It shares intelligence information, carries out investigations on behalf of foreign counterparts, and participates in joint investigations, as demonstrated in several cases studies provided by the authorities. From 2008 to 2013, it sent 98 requests for assistance on PPOC and ML/TF-related occurrences to the U.S., 94 to Europe and 60 to Asia. The RCMP and other police forces are also the ones who execute incoming requests of assistance, when there is no need for a judicial order, and the information or documentation is publicly available or can be obtained on a voluntary basis.

311. OSFI concluded 30 MOUs with various international prudential supervisors. No statistical information was provided in this respect but the authorities mentioned that OSFI regularly exchanges information regarding FRFIs with its foreign counterparts. In 2012, OSFI hosted an AML/CFT Supervisory College on five conglomerate banks with 19 foreign regulators in attendance. The College provided an opportunity for the foreign regulators to provide information on AML/CFT supervision in the host jurisdictions, and also for the banks themselves to provide an overview of their AML/CFT programs. The OSFI Relationship Management Team also hosts Supervisory Colleges of a general prudential nature, where foreign regulators attend. When OSFI conducts assessments at foreign operations of FRFIs, it seeks cooperation of the host regulator, who usually participates on the onsite with OSFI. The Colleges are an important and effective way for the sharing of information with OSFI's foreign counterparts.

312. The CBSA cooperates on a regular basis with U.S. Immigration and Custom Enforcement (ICE) and U.S. Custom Border Protection for the Sharing of Currency Seizure Information, including in AML/CFT matters. This cooperation is very important due to the extensive border shared by Canada and the U.S. Cases provided by the authorities demonstrated the CBSA's participation in joint operations. CBSA also receives information from the U.S. Department of Homeland Security, which helps the detection of suspected POC and leads to the seizure of the currency. Its participation in the Homeland's Security BEST Program resulted in the CBSA initiating 103 criminal investigations related to the smuggling of narcotics, smuggling of currency and firearms and illegal immigration. The CBSA also receives international cooperation from foreign governments or law enforcement and maintains strong collaboration with the 5-Eyes Community. It shares FINTRAC results with partner agencies in the U.S. on files that indicate ML activities that cross the Canada/U.S. border (Mexican Mennonites, outlaw motorcycle gangs, Persian organized crime). Nevertheless, the authorities also mentioned that financial information and information on import and export files declared in Canada are difficult to obtain by their counterparts, due to Canada's strong privacy framework.

313. The CRA has 92 Tax treaties and 22 Tax Information Exchange Agreements (TIEA) with international partners. However, CRA and CBSA do not cooperate under the Customs Mutual Assistance Agreement with the U.S. As is common for Canadian authorities, they would always require and MLAT to share the information regarding trading operations (where there is an important risk of trade-based ML, especially considering that more than 60 percent of Canada's GDP consists of international trade). Between 2009 and 2015, the CRA sent 72 requests and received 11 requests for exchange of information to foreign counterparts, in the context of criminal investigations.

314. The CSIS regularly receives from and shares financial information with FINTRAC in support of both organizations' mandates. In relation to high-risk travelers, it uses financial intelligence to determine how ready an individual may be to travel by determining whether they have purchased equipment, or if they have saved up money that could be used to support themselves while they are abroad. Due to confidentiality issues and matters of national security, CSIS did not provide the assessors any statistical data.

315. Feedback from the countries on Canada's assistance through other forms of cooperation is generally good. Most of the delegations indicated that the information received from FINTRAC in response to their requests was useful, of good content and of high quality. The limitation to request further information from any REs and bank information was, however, also reported. FINTRAC's average time to respond to request from its counterparts is 35 days (which is in line with the Egmont Group standards). The feedback from the U.S. FIU is very positive. FINTRAC and FINCEN have had a strong working relationship for years, both as FIUs and as AML/CFT supervisory/regulatory agencies, which is very important in light notably of the extensive border between the two countries, the illicit flows of criminal money, as well as the linkages between OCGs active in both countries. The U.S., which is Canada's main partner in cooperation, also reported and outstanding cooperation exchange with CRA. They indicated that the CRA responds to American requests for records in a very timely manner and has provided assistance in the location and coordination of witness interviews.

International Exchange of Basic and Beneficial Ownership Information of Legal Persons and Arrangements

316. While the authorities recognize the risk of misuse of Canadian legal persons and arrangements, they do not appear to have identified, assessed and understood with sufficient granularity the extent to which Canadian legal persons and legal arrangements are misused for ML or TF in the international context. In addition, there are serious concerns about the timeliness access to relevant information by competent authorities as well as with respect to the quality of the information collected by REs. As a result, cooperation in relation to foreign requests regarding BO of legal persons and arrangements cannot be fully effective.

317. Canada, and FINTRAC in particular, regularly receives requests for corporate records and information on beneficial ownership of both corporations and trusts (which points to the relevance of Canadian legal entities and trusts in international ML operations). FINTRAC provides the requested information as long as it already has it (i.e., it has received a STR or other report including VIRs regarding the relevant corporation or trust), it can access it (e.g., information from the corporate registries of Alberta and Quebec, or from the MSB registry, when the ownership is 25 percent or more, or from any other public source). The IAG also receives requests for basic and beneficial ownership information which it forwards to LEAs for execution. Between 2008 and 2015, it received 222 for corporate or business records, including 78 related to ML and 1 to TF investigations. Most of these requests have been executed.

Overall Conclusions on Immediate Outcome 2

318. Canada has achieved a substantial level of effectiveness for IO.2.

Annex I. Technical Compliance

This annex provides detailed analysis of the level of compliance with the Financial Action Task Force (FATF) 40 Recommendations of Canada in their numerical order. It does not include descriptive text on the country situation or risks, and is limited to the analysis of technical criteria for each Recommendation (R.). It should be read in conjunction with the Detailed Assessment Report (DAR).

Where both the FATF requirements and national laws or regulations remain the same, this report refers to analysis conducted as part of the previous Mutual Evaluation in 2008. The report for that assessment or evaluation is available from the FATF website.[1]

Recommendation 1—Assessing Risks and Applying a Risk-Based Approach

The requirements of R.1 were added to the FATF standard in 2012 and were, therefore, not assessed during the previous mutual evaluation of Canada.

Obligations and Decisions for Countries

Risk Assessment

Criterion 1.1—The Government of Canada has developed a risk assessment framework to support the identification, assessment and mitigation of ML/TF risks and includes a process to update and enhance this assessment over time. ML and TF threats were documented separately. Canada completed its first National Risk Assessment (NRA), the "Assessment of Inherent Money Laundering and Terrorist Financing Risks in Canada," in December 2014. In April 2015, the senior officials of participating federal departments and agencies endorsed the internal and draft public versions of the report. In July 2015, the Minister of Finance, on behalf of the government, released the public version of the NRA.[2] Canada's ML/TF Inherent RA is supported by a documented NRA Methodology with defined concepts on ML/TF risks and rating criteria. The report, which reflects the situation in Canada up to December 31, 2014, provides an overview of the ML/TF threats, vulnerabilities, and risks in Canada before the application of mitigation measures.

The NRA consists of an assessment of the inherent (i.e., before the application of any mitigation measures) ML/TF threats and inherent ML/TF vulnerabilities of key economic sectors and financial products, while considering the contextual vulnerabilities of Canada, such as geography, economy, financial system, and demographics.

Pursuant to the Interpretative Note to R.1, if countries determine through their risk assessments that there are types of institutions, activities, businesses, or professions that are at risk of abuse from ML and TF, and which do not fall under the definition of financial institution or DNFBP, they should consider applying AML/CFT requirements to such sectors. In that regard, the 2008 MER discussed

[1] See www.fatf-gafi.org/countries/a-c/canada/documents/mutualevaluationofcanada.html.

[2] See www.fin.gc.ca/pub/mltf-rpcfat/index-eng.asp.

whether Canada had considered extending AML requirements to white-label ATMs (see paragraphs 1357 to 1364). In a 2007 FINTRAC report highlighted the vulnerability of white-label ATMs to ML, and various press articles highlight the risk of misuse of white-label ATMs. The authorities are considering mechanisms to address this risk.

Criterion 1.2—The Department of Finance Canada (Finance Canada) is the designated authority for coordinating the work associated with the ongoing assessment of ML/TF risks. In Canada, government responsibilities in regard to AML/CFT are divided between the federal government and the ten provinces (the three territorial governments exercise powers delegated by the federal parliament). In that regard, the execution of AML/CFT actions involves collaboration and coordination across all levels of government.

The terms of reference for (i) the Interdepartmental Working Group on Assessing ML and TF Risks in Canada and (ii) the permanent National Risk Assessment Committee (NRAC; the senior-level AML/CFT Committee) establish Finance Canada as the designated authority for the initiative. The Minister of Finance is the Minister responsible for the PCMLTFA. Therefore, as decided by the Cabinet, the responsibility for coordinating the AML/CFT regime and the NRA falls also to Finance Canada.

Criterion 1.3—Canada's risk assessment framework contemplates a process to update and enhance this assessment over time. In accordance with the document "Proposed Governance Framework for Canada's ML/TF Risk Assessment Framework" (endorsed on November 13, 2014), the NRA update is now coordinated through the NRAC, the successor body to the Working Group that developed the NRA. The Terms of Reference of NRAC were approved at the senior-level AML/CFT Committee in April 2015. NRAC is composed of representatives of the federal departments and agencies that comprise Canada's AML/CFT (and may invite other public and private sector partners to participate), which facilitates sharing findings across the organizations represented to help them understand the evolving risks and ML/TF environment, as well as discuss and propose mitigations. Finance Canada is the permanent co-chair of the NRAC; the other co-chair position rotates every two years among other federal departments or agencies. NRAC is required to prepare a formal update every two years on the results of the risk assessment and an informal update on an annual basis. The reports are addressed to the senior level AML/CFT Committee. As Canada completed its NRA in December 2014, it is relatively up to date. Furthermore, the Committee will meet every six months or more frequently, if needed, to review emerging threats and new developments and will report to the senior-level Committee on an annual basis with updates.

Criterion 1.4—Information on the results of the NRA is provided to competent authorities, self-regulatory bodies, FIs and DNFBPs through different working groups, committees and outreach activities. The NRA was released publicly on July 31, 2015 (and is available on the websites of Finance, FINTRAC, and OSFI). The NRA methodology and results were also shared and discussed beforehand by Finance

Risk Mitigation

Criterion 1.5—The risk mitigation is implemented through various thematic national strategies, to wit: National Identity Crime Strategy (2011), Canada's Counter-terrorism Strategy (2013); National Border Risk Assessment 2013–2015; 2014–2016 Border Risk Management Plan; Enhanced Risk Assessment Model and Sector profiles; OSFI's AMLC Division AML and CFT Methodologies and Assessment Processes; OSFI-Risk Ranking Criteria; and the CRA's techniques to identify registered charities and organizations seeking registration that are at risk of potential abuse by terrorist entities and/or associated individuals.

Criterion 1.6—Financial activities are subject to AML/CFT preventive measures as required in the FATF Recommendations, except when these activities are conducted by the sectors that are not subject to AML/CFT obligations under the PCMLTFA. These sectors include check-cashing businesses, factoring companies, and leasing companies, finance companies, and unregulated mortgage lenders, among others. The NRA assessed the ML/TF vulnerabilities of factoring, finance and financial leasing companies as medium risk, while pointing out that these entities were very small players as a proportion of Canada's financial sector. However, the ML/TF risks for these sectors has not been proven to be low and the non-application of AML/CFT measures is not based on a risk assessment.

Except for the legal profession, all DNFBP sectors are required to apply AML/CFT preventive measures. Lawyers are covered as obliged AML/CFT entities, pursuant to PCMLTR, Section (s.) 33.3; however, the AML/CFT provisions are inoperative in relation to lawyers and Quebec notaries (who provide legal advice and are, therefore, considered legal counsel, PCMLTFA s.2) as a result of a 2015 Supreme Court of Canada ruling.

Supervision and Monitoring of Risk

Criterion 1.7—REs are required to implement enhanced or additional measures in high-risk situations pursuant to PCMLTFA, ss.9.6(2) and 9.6(3) and PCMLTFR, §71(c) and 71.1(a) and (b) (see discussion on R.10 for additional information on enhanced CDD measures). The REs are expected to integrate the NRA results in their own risks assessments.

PCMLTFA, s.9.6(2) provides that REs develop and apply policies and procedures to address ML and TF risks. PCMLTFA, s.9.6(3) and PCMLTFR, s.71.1(a) and (b) require REs to apply "prescribed special measures" to update client identification and beneficial ownership information, and to monitor business relationships when higher risks are identified through the entity's risk assessment.

Nevertheless, the provisions discussed in the paragraphs above do not apply to the sectors that are not subject to reporting obligations under the PCMLTFA. These include sectors such as the legal counsels, legal firms and Quebec notaries, factoring companies, financing and leasing companies, among others. Of these sectors, the legal counsels, legal firms and Quebec notaries are exposed to ample ML opportunities and are exposed to higher risks. Therefore, as the legal profession is not

required to take enhanced measures regarding higher ML risks (or any ML risks, for that matter) the risks associated with this sector are not being effectively mitigated.

Exemptions

Criterion 1.8—PCMLTFR ss.9, 62 and 63 provide for exemptions from the customer identification and record-keeping requirements in certain specific circumstances assessed as low risk by the authorities (for details about the exemption regime, see discussion on R.10 below). OSFI and FINTRAC continuously assess the risks associated with their supervised sectors and the current assessment of low risks appear to be consistent with the findings of the NRA.

Criterion 1.9—PCMLTFA, s.40(e) requires FINTRAC to ensure compliance with PCMLTFA provisions. PCMLTFA, s.9.6 (1)–(3) requires REs Act to implement measures to assess ML and TF risks, and monitor transactions in respect of the activities that pose high ML/TF risks. OSFI and FINTRAC apply a risk-based approach to the supervision of their supervised sectors. As discussed previously, the legal profession is not subject to AML/CFT obligations and is, therefore, not monitored by FINTRAC. However, some high-risk DNFBPs are not subject to AML/CFT obligations and are, thus, not supervised in relation to their obligations under R.1.

Obligations and Decisions for Financial Institutions and DNFBPS

Risk Assessment

Criterion 1.10—PCMLTFA, s.9.6(2) and PCMLTFR, §71(c) requires REs to conduct risk assessments and consider all the relevant risk factors before determining what is the level of overall risk and the appropriate level and type of mitigation to be applied. PCMLTFR, s.71(e) provides that the REs shall keep their risk assessments up to date. All supervised entities and those subject to examination by FINTRAC are obligated under their sector legislation or PCMLTFA, s.62 to provide any material that FINTRAC or sector regulators may require. FINTRAC Guideline 4 (Implementation of a Compliance Regime, February 2014) provides a checklist of products or services that should be considered high-risk. OSFI Guideline B-8 (Deterring and Detecting Money Laundering and Terrorist Financing) provides instruction on the FRFIs risk assessment policies and procedures. As mentioned above, none of the AML/CFT requirements are applicable to lawyers, legal firms, and Quebec notaries.

Risk Mitigation

Criterion 1.11—

a) Under PCMLTFA s 9.6(1) and PCMLTFR, s.71, REs are required to develop written AML/CFT compliance policies and procedures, which are approved by a senior officer of the RE in accordance with PCMLFTR s.71(1)(b).

b) These policies and procedures, the risk assessment and training program are required to be reviewed at least every two years (PCMLFTR, ss.71(1)(e) and 71(2)). The REs must also assess and document ML and TF risks (PCMLTFA, s.9.6(2) and PCMLFTR, s.71(1)(c)).

c) There are several different provisions that require REs to implement enhanced or additional measures in high-risk situations: Under PCMLTFA, ss.9.6(2) and 9.6(3), REs are required to assess ML and TF risks and enhanced due diligence, record keeping, and monitoring of financial transactions that pose a high risk of ML or TF. The PCMLTFR requires REs to apply enhanced measures when high risks are identified in their activities as a result of ongoing monitoring. The sectors covered by the PCMLTFR are banks and other deposit-taking institutions (s.54.4); life insurance (s.56.4); securities (s.57.3); MSBs (s.59.02); accountants (s.59.12); real estate (s.59.22); British Columbia Notaries (s.59.32); real estate developers (s.59.52), casinos (s.60.2); and Departments and agents of the Queen in rights of Canada or a province for the sale or redemption of money orders for the general public (s.61.2). The provisions addressing the legal profession are not applicable to legal counsels, legal firms, and Quebec notaries for the reasons stated earlier. FINTRAC, Guideline 4, and OSFI Guideline B-8 provide additional guidance.

Criterion 1.12—The Canadian AML/CFT legislation does not provide for simplified measures.

Weighting and Conclusion

The main inherent ML and TF risks were identified and assessed for the implementation of appropriate mitigation. **Canada is largely compliant (LC) with R.1**

Recommendation 2—National Cooperation and Coordination

Canada was rated LC in the 2008 MER with former FATF R.31; the cooperation between the FIU and LEAs was not considered to be fully effective.

Criterion 2.1—Several national strategies and policies are in place to inform AML/CFT policies and operations. The main AML policies and strategies are the National Identity Crime Strategy (RCMP 2011); National Border Risk Assessment 2013–2015 (CBSA); 2014–16 Border Risk Management Plan (CBSA); Enhanced Risk Assessment Model and Sector profiles (FINTRAC); AMLC Division AML and CFT Methodology and Assessment Processes (OSFI); Risk Ranking Criteria (OSFI); Risk-Based Approach to identify registered charities and organizations seeking registration that are at risk of potential abuse by terrorist entities and/or associated individuals (CRA) and CRA-RAD Audit Selection process. The RCMP is currently developing their National Strategy to Combat Money Laundering. These AML strategies and policies are linked to the 2011 Canadian Law Enforcement Strategy on Organized Crime. In addition, the Government's other main AML/CFT concerns are reflected in Finance Canada's Report on Plans and Priorities,[3] which outlines the AML/CFT regime's spending plans, priorities and expected results. Canada's CFT strategy forms part of the broader

[3] Page 29, Report on Plans and Priorities 2015–16, Department of Finance Canada (2015). See http://www.fin.gc.ca/pub/rpp/2015-2016/index-eng.asp.

Counter-terrorism Strategy.[4] Similarly, the country's PF strategy forms part of the broader strategy to counter the proliferation of chemical, biological, radiological, and nuclear weapons.[5]

The TRWG is an interdepartmental body that serves as a forum to enhance dialogue, coordination, analysis, and collaboration, among PS Portfolio members and government departments with an intelligence mandate, on issues related to threat resourcing, including ML, TF and proliferation activities, organized crime and other means through which threat actors resource their activities. It also highlights the security and intelligence components of files associated with Canada's AML/ATF Regime.

Criterion 2.2—Finance Canada is the domestic and International policy lead for the whole AML/CFT regime, and is responsible for its overall coordination, including AML/CFT policy development and guiding and informing strategic operationalization of the NRA framework.

Criterion 2.3—The Canadian regime is also supported by various interdepartmental formal and informal working-level bilateral and multilateral working groups and committees, depending on the nature of the issues to be addressed including: NRAC; NCC; IPOC; IFAC; TRWG, and the ICC.

To combat ML, Canada also coordinates domestic policy on the federal criminal forfeiture regime under the IPOC. IPOC's interdepartmental Director General-level Senior Governance Committee led by Public Safety Canada includes: CBSA, CRA, PPSC, PS, PWGSC, and the RCMP. The Committee is mandated to provide policy direction, promote interdepartmental policy coordination, promote accountability, and to support the Initiative.

The NCC is the primary forum that reviews progress of the National Agenda to Combat Organized Crime. NCC's 5 Regional Coordinating Committees communicate operational and enforcement needs and concerns to the NCC, acting as a bridge between enforcement agencies and officials and public policy makers. Canada coordinates domestic AML policy on the federal criminal forfeiture regime under the IPOC Advisory Committee and the IPOC Senior Governance Committee.

The IFAC is an interdepartmental consultative body that has the responsibility for the sharing, analysis, and monitoring of information related to ML/TF threats posed to Canada by foreign jurisdictions or entities. The ICC assists the Minister of Public Safety and Emergency Preparedness by providing the requisite analysis and considerations to inform the recommendations to the Governor in Council regarding listing of entities.

OSFI and FINTRAC coordinate their activities through a common approach for supervision of FRFIs, starting in 2013, by conducting simultaneous AML/CFT examinations. FINTRAC informs its compliance enforcement strategies with findings provided by other federal and provincial regulators

[4] *Building Resilience Against Terrorism: Canada's Counter-terrorism Strategy*. Public Safety Canada (2013). See http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rslnc-gnst-trrrsm/index-en.aspx.

[5] *The Chemical, Biological, Radiological and Nuclear Strategy of the Government of Canada*. Public Safety and Emergency Preparedness Canada (2005). See https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rslnc-strtg-rchvd/index-en.aspx.

in order to monitor and enforce AML/CFT compliance by REs. FINTRAC has established 17 Memoranda of Understanding (MOU) with federal and provincial regulators for the purpose of sharing information related to compliance with Part 1 of the PCMLTFA. The RCMP leads the Integrated National Security Enforcement Teams (INSETs) in major centers throughout the country). INSETs are made up of representatives of the RCMP, federal partners and agencies such as CBSA, CSIS, and provincial and municipal police services.

Criterion 2.4—Counter-proliferation (CP) efforts, including proliferation financing, are coordinated via a formalized CP Framework created in 2013. PS chairs the Counter-Proliferation Policy Committee, at which CP partners identify, assess, and address policy and programming gaps that may undermine Canada's CP capacity. Global Affairs Canada chairs the Counter-Proliferation Operations Committee, through which CP partners work together to address specific proliferation threats with a Canadian nexus. FINTRAC is a member of the Operations Committee, and as per PCMLTFA s.55.1(1)(a), is able to disclose designated financial information to the Canadian Security Intelligence Service (CSIS) when it has reasons to suspect that it would be relevant to investigations of threats to the security of Canada, which includes proliferation activities. FINTRAC can also disclose information on threats related to proliferation to the appropriate police force and the CBSA if separate statutory thresholds are met.

Weighting and Conclusion

Canada has a number of standing committees, task forces, and other mechanisms in place to coordinate domestically on AML/CTF policies and operational activities. **Canada is compliant (C) with R.2.**

Recommendation 3—Money Laundering Offense

Canada was rated LC with former R.1 and 2 based on a number of shortcomings. The range of predicate offenses was slightly too narrow and for one part of the ML offense, the mens rea requirement was not in line with the FATF standard. Since 2008, the range of predicate offenses for ML was expanded to include tax evasion, tax fraud, and copyright offenses.

Criterion 3.1—ML activities are criminalized through Criminal Code (CC), ss.354 (possession of proceeds), 355.2 (trafficking in proceeds), and 462.31 (laundering proceeds). *Conversion or Transfer*: CC, s.462.31 criminalizes the use, transfer, sending or delivery, transportation, transmission, altering, disposal of or otherwise dealing with property with the intent to conceal or convert the proceeds and knowing or believing that all or part of that property or proceeds was obtained or derived directly or indirectly as a result of a predicate offense. S.462.31 falls somewhat short of the FATF standard due mainly because the perpetrator must intend to conceal or convert the property itself, rather than the illicit origin thereof. Additionally, no alternative purpose element of "helping any person who is involved in the commission of a predicate offense to evade the legal consequences of his or her action" is provided for. S.355.2 criminalizes many of the same acts as s.462.31 but without setting out any specific intent requirement. However, the Supreme Court in *Canada in R. v. Daoust, 2004, 1 SCR 217, 2004 SCC 6 (CanLII)* held that "the intention of parliament was to forbid the

conversion pure and simple, of property the perpetrator knows or believes is proceeds of crime, whether or not he tries to conceal it or profit from it." *Acquisition, possession or use*: Ss.354 and 355.2. criminalize the sole or joint possession of or control over (s.354) and the selling, giving, transferring, transporting, exporting or importing, sending, delivering or dealing with in any way (s.355.2) of property or things that the person knows were obtained or derived directly or indirectly from an indictable offense. Neither provision explicitly refers to the "acquisition or use," but such acts would be covered by "control over proceeds" in s.354 and the various material elements under s.355.2. *Concealment or disguise*: Under CC, s.354 it is an offense to conceal or disguise property that the perpetrator has possession of or control over, in which case liability is invoked for "possession and trafficking of proceeds." Additionally, the concealment or disguise is covered under s.355.2 and liability is for "trafficking in proceeds."

Criterion 3.2—Ss.354 and 355.2 cover acts relating to proceeds of an "indictable offense;" and s 462.31 to proceeds of a "designated offense." "Designated offense" is defined as "any offense that may be prosecuted as an indictable offense other than those prescribed by regulation". Canada's ML provisions apply to all serious offenses under Canadian law and cover a range of offenses in each FATF designated categories of predicate offenses, including tax evasion.

Criterion 3.3—All serious offenses under Canadian law, defined as offenses with a statutory sanction of imprisonment for more than six months, constitute a predicate offense for ML. As indicated in the 2008 MER, federal laws criminalize a range of serious offenses under each FATF designated categories of predicate offenses.

Criterion 3.4—Ss.354, 355.2, and 462.31 apply to any property or proceeds of property obtained or derived, directly or indirectly, from the commission of an indictable offense. No value threshold applies. "Property" is defined under s.2 of the CC to include real and personal property of every kind and deeds and instruments relating to or evidencing the title or right to property, or giving a right to recover or receive money or goods, including converted or exchanged property. The definition covers material and immaterial, tangible and intangible, and corporeal and incorporeal property as well as interest in such property.

Criterion 3.5—The legal provisions do not require a conviction for a predicate offense to establish the illicit source of property. Case law further confirmed this principle. [6]

Criterion 3.6—The text of ss.354, 355.2, and 462.31 apply the relevant offenses to indictable offenses committed in Canada and to any act or omission committed abroad that would have constituted an indictable offense had it occurred in Canada.

[6] United States of America and the Honourable Allan Rock, Minister of Justice for Canada v. Dynar, 1997, 2 SCR 462, 1997, CanLII 359 (SCC); R.c.Chun, 2015 QCCQ 2029 (CanLII); and R.c. Lavoie, 1999 CanLII 6126 (QCCQ).

Criterion 3.7—Nothing in the relevant provisions prevent their application to the person who committed the predicate offense. Canadian case law supports the notion that the ML provisions can also be applied to the person who committed the predicate offense.[7]

Criterion 3.8—As a general rule, Canada allows for the intentional element of criminal offenses to be inferred from objective factual circumstances and based on credible, admissible and relevant circumstantial evidence. This principle has been confirmed through case law in multiple instances, as indicated in the 2008 MER.[8]

Criterion 3.9—Offenses pursuant to s.354 are punishable with imprisonment for up to ten years (if the value of the property exceeds Can$5,000) or for up to two years (if the value of the property is less than Can$5,000). S.355.5 applies the same value thresholds but set out slightly stricter sanctions of imprisonment for up to 14 years or up to five years, respectively. S.462.31 provides for a statutory sanction of imprisonment for up to ten years, regardless of the amounts involved. The statutory sanctions may be increased or reduced pursuant to CC, s.718.2 based on aggravating or mitigating circumstances. CC, s.718.1 requires that the sanction in all cases be proportionate to the gravity of the offense and the degree of responsibility of the offender. The statutory sanctions are considered to be both dissuasive and proportionate.

Criterion 3.10—Legal entities may be subject to criminal liability and be held criminally responsible for ML. Pursuant to CC, s.735 (1) a legal entity, partnership, trade union, municipality or association convicted of an indictable offense is liable to a fine with the relevant amount being determined by the court. In determining the relevant sanction, s.718.21 stipulates that factors such as the advantage realized, the degree of planning involved in carrying out the offense, whether the organization has attempted to conceal its assets or convert them to avoid restitution; and any regulatory penalty imposed shall be taken into account. CC, s.718.1 requires that a sentence must in all cases be proportionate to the gravity of the offense and the degree of responsibility of the offender. Given the wide discretion the court has in determining the sanction, the statutory sanctions are considered to be dissuasive and proportionate. Parallel civil or administrative sanctions may be applied in addition to the criminal process.

Criterion 3.11—Ancillary offenses are criminalized in the general provisions of the CC (s.24—attempt; s.21 (1)—aiding and abetting; s.21 (2)—conspiracy to commit; s.22—counseling, procuring, soliciting, or inciting to commit; s.23—accessory after the fact).

Weighting and Conclusion

Canada is compliant (C) with R.3.

[7] R. v. Tortine, 1998, 2 SCR 972, 1993 CanLII 57 (SCC); and R. v. Trac at R. v. Trac, 2013 ONCA 246 (CanLII).

[8] Manitoba Court of Appeal in R. v. Jenner (2005), 195 CCC (3d) 364 at para 20; and Ontario Court of Appeal in R. v. Aiello (1978), 38 CCC (2d) 485 affirmed 46 CCC (2d) 128n SCC at page 488.

Recommendation 4—Confiscation and Provisional Measures

Canada was rated LC with former R.3.

Criterion 4.1—CC, s.462.37 (1) provides for the permanent forfeiture of proceeds of crime based on a conviction for a designated offense. CC, s.490.1 (for all crimes) and Controlled Drugs and Substances Act (CDSA), ss.16 and 17 set out similar forfeiture provisions in relation to property used or intended to be used for the commission of an indictable offense. In all cases, the court will consider forfeiture based on the application by the Attorney General. In the context of convictions for participation in a criminal organization or offenses under the CDSA, extended forfeiture orders may be granted for material benefits received within 10 years before commencement of the proceedings and income from sources that cannot be reasonably accounted for. In a standalone ML case, CC, s.462.37(1) allows for the confiscation of the proceeds of the laundering activity, as well as the property laundered, although for the latter, a stricter standard of proof would apply. CC, ss.462.37 (1) and 490.1 allow for forfeiture of property from a third party. In cases where the accused has died or absconded, forfeiture *in rem* is available under ss.462.38 and 490.2.

Equivalent value confiscation is not permitted. CC, s.462.37(3) provides for the issuance of a fine in lieu of forfeiture in cases where the court determined that a forfeiture order under CC, s.462.37 cannot be made in respect of any property. While the issuance of a fine may result in the same outcome as an equivalent value confiscation, from a legal point of view the concept of a fine cannot substitute equivalent value confiscation.

Criterion 4.2—The CC and CDSA set out a wide range of measures including search and seize warrants pursuant to CC, ss.487, 462.32 and 462.35 and CDSA, s.11; production orders pursuant to CC, s.487.018 regarding the existence of bank accounts; production orders pursuant to CC, ss.487.014 and 487.015; warrants for transmission of data including computer and telecommunication program recordings under CC, s.492.2; general information warrants under CC, s.487.01 and tax information orders under CC, s.462.48. The power under CC, s.487.01 to "use any device, investigation technique or procedure or do anything described in the warrant" is sufficiently broad to also cover account monitoring. In addition, PCMLTFA, s.23 allows for the seizure and forfeiture of cash or bearer-negotiable instruments for violations of the cross-border declaration obligation. Seizing and restraint warrants to secure property or instrumentalities for forfeiture are available under CC, ss.462.33 and 490.8 and CDSA, s.14. Seizing and restraint orders may be issued based on reasonable grounds to believe that a forfeiture order will be made in regards to the relevant property. In both cases, the judge may opt to apply provisional measures ex parte and without prior notice. CC, ss.490.3 and 462.4 permit the judge to void any conveyances of transfers unless the transfer was for valuable consideration to a bona fide third party. Prior to the issuance of a seizing or restraint order, the holder of such property may become subject to criminal liability under CC, s.354(1) provided he acted knowingly. A specific forfeiture provision for property owned or controlled by a terrorist group or property that has been or will be used to carry out a terrorist activity is set out in CC, s.83.14.

Criterion 4.3—Rights of bona fide third parties are protected through CC, ss.462.42, 462.34 (b), 490.4 (3) and 490.5 (4), which allow for exclusion of certain property from a restraining, seizing, or forfeiture order.

Criterion 4.4—The Seized Property Management Act regulates the management of seized or restrained property and the disposal and sharing of forfeited property. Under the Act, the Minister of Public Works and Government Service is competent to take into custody all such property and may take any measures he deems appropriate for the effective management thereof. Forfeited property is to be disposed of and the proceeds to be paid into the Seized Property Proceeds Account. Fines paid in lieu of forfeited property and amounts received from foreign governments under asset-sharing agreements are to be credited to the Proceeds Account as well. Excessive amounts in the Account are to be credited to accounts of Canada as prescribed by the Governor in Council.

Weighting and Conclusion

The confiscation framework has some shortcomings. **Canada is largely compliant (LC) with R.4.**

Recommendation 5—Terrorist Financing Offense

Canada was rated LC with former SR. II.

Criterion 5.1—TF is criminalized through CC, ss.83.02 to 83.04: S. 83.02 criminalizes the direct or indirect, willful and unlawful collection or provision of property with the intent that the property is to be used or knowing that the property will be used to carry out a terrorist activity. CC, s.83.04 criminalizes the use of property for the purpose of facilitating or carrying out a terrorist activity, and the possession of property intending that it be used or knowing that it will be used to facilitate or carry out a terrorist activity. CC, s.83.01 defines "terrorist activity" to cover all acts which (1) constitute an offense as defined in one of the conventions and protocols listed in the Annex to the TF Convention, all of which are criminalized in Canada; and (2) any other act or omission carried out with terrorist intent.

Criterion 5.2—CC, s.83.03(a) criminalizes the direct or indirect collection or provision of property with the intent that such property is to be used or knowing that such property will be used to benefit any person who is facilitating or carrying out a terrorist activity. The offense applies also where the property is used by the financed person for a legitimate purpose. CC s.83.03(b) covers the direct or indirect collection or provision of property, knowing that such property, in whole or in part, will benefit a terrorist group. "Terrorist group" includes a person, group, trust, partnership, or fund or unincorporated associations or organizations that has as one of its purposes or activities the facilitating or carrying out of any terrorist activity. The mental element required under subsection (b) is slightly stricter than under subsection (a) as the offense only applies where the perpetrator knows that property will be used for the benefit of a terrorist group, but not where he merely intends for this to be the case. For both CC, ss. 83.03 (a) and (b), the courts have interpreted the term "facilitates" broadly to cover "any behavior/activity taken to make it easier for another to commit a

crime."[9] The term thus includes the "organizing or directing of others" to commit a terrorist activity, or the "contributing to the commission of a terrorist activity by a group of persons acting with a common purpose."

Criterion 5.3—"Property" is defined under CC, s.2 to include real and personal property of every kind and deeds and instruments relating to or evidencing the title or right to property or giving a right to recover or receive money or goods, including converted or exchanged property. CC, ss.83.01 to 83.03 are not limited in scope to financing activities involving illicit property. The source of the property used for the financing activity is irrelevant.

Criterion 5.4—CC, s.83.02 implies that the financing offense can also be applied in cases where a person collects or provides property merely with the intention to finance a specific terrorist activity. Thus, it is neither required that the financed activity has been attempted or committed, nor that the money collected or provided is linked to a specific terrorist activity. CC, s.83.03(b) extends to the collection or provision of funds for the benefit of a terrorist group, regardless of the purpose for which the funds are eventually used, but does not cover financing merely with the intent to benefit an individual terrorist or terrorist organization. For financing of individual terrorists, CC, s.83.03(a) applies where the financed person is facilitating or carrying out a terrorist activity at the time the financing activity takes place and CC, s.83.03(b) covers situations where the property collected or provided is known to be used by or benefit a terrorist.

Criterion 5.5—Canada allows for the intentional element of criminal offenses to be inferred from objective factual circumstances and based on credible, admissible, and relevant circumstantial evidence. This principle has been confirmed through case law in multiple instances, as indicated in the 2008 MER.[10]

Criterion 5.6—The statutory sanctions for a natural person is imprisonment for up to ten years with the possibility of an increased or reduced sentence pursuant to CC, ss.718.2 and 718.21 based on aggravating or mitigating circumstances. The statutory sanctions are considered to be both dissuasive and proportionate.

Criterion 5.7—Legal entities may be held criminally responsible for terrorism financing. Pursuant to CC, s.735 (1) of the CC, a legal entity, partnership, trade union, municipality, or association may fine in an amount that is in the direction of the court. CC, s.718.21 stipulates that factors such as the advantage realized, the degree of planning involved in carrying out the offense, whether the organization has attempted to conceal its assets or convert them to avoid restitution; and any regulatory penalty imposed shall be taken into account by the court. CC, s.718.1. CC further requires that the sentence be proportionate to the gravity of the offense and the degree of responsibility of

[9] R. v. Nuttall, 2015 BCSC 943 CanLII.

[10] Manitoba Court of Appeal in R. v. Jenner (2005), 195 CCC (3d) 364 at para. 20; and Ontario Court of Appeal in R. v. Aiello (1978), 38 CCC (2d) 485 affirmed 46 CCC (2d) 128n SCC at page 488.

the offender. Given the wide discretion by court in determining the sanction, the statutory sanctions are dissuasive and proportionate. Parallel civil or administrative sanctions may be applied.

Criterion 5.8—Ancillary offenses are criminalized in the general provisions of the CC (s.24—Attempt; s.21 (1)—aiding and abetting; s.21 (2)—conspiracy to commit; s.22—counselling, procuring, soliciting or inciting to commit; s.23—accessory after the fact). s.83.03 criminalizes inviting another person to provide or make available property for TF and ss.83.21 and 83.22 to knowingly instruct, directly or indirectly, any person to carry out an activity for the benefit of, at the direction of or in association with a terrorist group for the purpose of enhancing the ability of that group to facilitate or carry out a terrorist activity.

Criterion 5.9—Canada takes an all crimes approach to defining predicate offenses for ML. TF is, thus, a predicate offense for ML.

Criterion 5.10—CC, ss.83.02 and 83.03 apply regardless of whether the underlying terrorist activity is committed inside or outside Canada, or whether the terrorist group or financed person is located inside or outside Canada.

Weighting and Conclusion

TF is set out as a separate criminal offense that covers all aspects of the offense set out in the Terrorism Financing Convention, with minor shortcomings. **Canada is largely compliant (LC) with R.5.**

Recommendation 6—Targeted Financial Sanctions Related to Terrorism and Terrorist Financing

Canada was rated LC with former SR. III. For certain FIs and other persons or entities that may hold targeted funds the assessors found that the names of designated persons and entities were not effectively communicated, the guidance issued was not sufficient and the implementation of the relevant legal provisions was not effectively monitored. The framework for the implementation of the TF-related targeted financial sanctions remains substantially unchanged. A new Security of Canada Information Sharing Act was adopted in 2015 to facilitate the sharing of information between Canadian government agencies with regards to any activity that undermines the security of Canada, including terrorism.

Identifying and Designating

Under United Nations Act, s.2, the Governor in Council may issue regulations to give effect to decisions and implement measures decided by the UNSC pursuant to Article 41, Chapter VII of the UN Charter. Two Regulations were issued on this basis—the *United Nations Al-Qaida and Taliban Regulations (UNAQTR) and the Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism* (RIUNRST). In 2001, Canada enacted an additional domestic terrorist listing procedure under CC, ss.83.05 to 83.12 in addition to the RIUNRST. Over time, the listing mechanism under the CC has become the primary domestic listing regime and consequently no listings have

been added to the RIUNRST since 2006. The Security of Canada Information Sharing Act facilitates implementation of the mechanisms by allowing for the exchange of information between government agencies with regards to terrorism, either spontaneously or upon request.

Criterion 6.1—Sub-criterion 6.1a—Department of Foreign Affairs, Trade and Development Act, s.10(2)(b) assigns responsibility to the Minister of Foreign Affairs for all communications between Canada and international organizations, including for proposing designations under UNSCR 1267/1989 or 1988 to the relevant UN Sanctions Committees.

Sub-criterion 6.1b—Based on the above mentioned s.10(2)(b), the Minister of Foreign Affairs identifies, reviews, and proposes individuals or entities for designation, in consultation with an interdepartmental committee of security and intelligence officials. The interdepartmental committee on average meets once a month to discuss all listing regimes.

Sub-criterion 6.1c—The authorities stated that the identification process outlined above is based on a standard of "reasonable grounds to believe" and that a criminal conviction was not necessary for proposing the designation of an entity or individual to the UN. In the absence of any written procedures on this point, the assessors were not in a position to verify the authorities' view.

Sub-criterion 6.1d—Canada supports co-designation and co-sponsorship and its experience in proposing designations was so far limited to cosponsoring proposals for designations. To propose designations, Canada would use the UN standard forms and follow the procedures outlined under UNSCR's 2160 and 2161 (2014) and the relevant Sanctions Committee Guidelines.

Sub-criterion 6.1e—The authorities stated that Canada would provide as much relevant information to support a proposal for designation as possible, including identifying information and a statement of case.

Criterion 6.2—Sub-criterion 6.2a—Canada implements UNSCR 1373 through two distinct mechanisms: (i) for terrorist groups, CC, s.83.05 grants the Governor in Council the authority to list, on the basis of a recommendation by the Ministry of Public Safety Canada, a person, group, trust, partnership or fund or unincorporated association or organization. Requests for designation from another country can also be considered under the CC process; (ii) the RIUNRST designates the Governor in Council as responsible for making designations on the basis of a recommendation by the Minister of Foreign Affairs (Article 2 RIUNRST). The Minister may recommend a designation under the RIUNRST also based on a request from another country. In practice the mechanisms under the CC is the main one and no listings have been added to the RIUNRST since 2006.

Sub-criterion 6.2b—The CC and RIUNRST include mechanisms for identifying targets for designation and to decide upon designations based on clearly stipulated criteria in line with the designation criteria under UNSCR 1373.

Sub-criterion 6.2c—Foreign requests for designations are processed the same way as domestic designations. As a first step, authorities ensure that a request for listing is supported by verified facts

that meet the legal threshold. Verification includes both factual and legal scrutiny. After verification is completed, the proposed listing is presented to the Cabinet and the relevant Minister recommends to the Governor in Council that the foreign request be granted. Authorities stated that the process takes on average six months but can be expedited, if necessary.

Sub-criterion 6.2d—The Governor in Council takes the decision to designate based on "reasonable grounds to believe" that a person meets the designation criteria in CC or the RIUNRST, independently from any criminal proceedings.

Sub-criterion 6.2e—The authorities stated that when making 1373 request to other countries, as much identifying information as possible would be provided to the requesting country to allow for a determination that the reasonable basis test is met Canada stated that it is in regular contact with its allies to discuss potential listings and notifies G7 partners prior to any domestic listing.

Criterion 6.3—The Canadian Security Intelligence Service Act s. 12 grants the CSIS the power to collect and analyze information on activities that may threaten Canada's security and to report and advise the government of any such activities. The Security of Canada Information Sharing Act, s.5 further allows government agencies to share such information. In the context of a criminal suspicion or the designation procedure under CC, s.83.05 the authorities may also collect information under criminal procedures. The outlined measures may in all cases be applied *ex parte* to avoid tipping off.

Freezing

Criterion 6.4—The UNAQTR, CC and RIUNRST set out a wide range of prohibitions to deal with property of or provide financial services to designated persons. The prohibitions apply as soon as any person is designated by the competent UN Sanctions Committee (for UNSCR 1267/1989 or 1988) or is added to the Regulations Establishing a List of Entities pursuant to the CC or is included in Schedule 2 to the RIUNRST (for UNSCR 1373). The prohibitions apply without delays, as soon as a person has been designated by the UN (for UNSCR 1267 and 1988) or was added to the domestic list. The term "person" covers both natural and legal persons.

Criterion 6.5—No authority has been designated for monitoring compliance by FIs and DNFBPs with the provisions of the UNAQTR, CC, and RIUNRST. Sanctions for violations of the Regulations are available but have never been applied in practice.

Sub-criterion 6.5a—The UNAQTR, CC and RIUNRST prohibit that any person or entity in Canada or any Canadian outside Canada knowingly deals with; provides financial or other services to; or enters into or facilitates any financial transaction involving funds or property of a designated person. The prohibition applies as soon as a person is listed and covers all aspects of the freezing obligation, thus also without prior notice.

Sub-criterion 6.5b—The UNAQTR, RIUNRST, and CC target funds or property owned or controlled, directly or indirectly, by any designated person or by any person acting on behalf or at the direction of a designated person. In the case of the UNAQTR but not the CC, does the prohibition extend also

to funds derived or generated from such property. The concepts of "ownership and control" also cover property owned and controlled jointly. The obligations under all three procedures apply to property of every kind, including any funds, financial assets or economic resources.

Sub-criterion 6.5c—The UNAQTR, the CC, and RIUNRST prohibit Canadians and any persons in Canada from making property or financial or other services available, directly or indirectly, for the benefit of a designated person (Articles 4 RIUNRST; CC, ss.83.08 and UNAQTR s.4 and 4.1. CC, s.83.03 further criminalizes the provision of property or services to a listed entity, but the prohibition does not extend the provision of services to entities owned or controlled by a designated person or persons acting on behalf or at the discretion of a designated person.

Sub-criterion 6.5d—Canada makes public all designations under all three listing regimes on government websites and through notification services. FRFIs have the option of signing up to receive information notices regarding list changes from OSFI and/or directly from the 1267 Al-Qaida Sanctions Committee and the 1988 Taliban Sanctions Committee. OSFI receives a note verbale from the 1267 Al-Qaida Sanctions Committee and the 1988 Taliban Sanctions Committee in advance of a formal press release (i.e., before the Committees lists the entities publically). OSFI sends out email alerts to those entities that subscribe to its email notifications of any changes to the lists the same day or subsequent day from receiving the note verbale. However, if there are extensive changes to the lists, this process can be delayed by two weeks. The UN 1267 Al-Qaida Committee and 1988 Taliban Sanctions Committee also notify all email subscribers, which can include FIs or any persons, of new listings and de-listings the same day or the next UN business day. REs are informed without delay of any entities listed under the CC and RIUNRST. When an entity becomes listed pursuant to the CC, a notice is published in the *Canada Gazette*, which constitutes official public notice of the listing. These changes are also included in OSFI's email notifications. Public Safety also issues a news release for all new listings and de-listings, and both Public Safety and OSFI include information on its websites.

Sub-criterion 6.5e—Banks, cooperative credit societies, savings and credit unions, and insurance companies are required to determine, on a continuous basis, whether they are in possession of targeted funds or property and must regularly report this and any associated information to the competent supervisory authority (OSFI or FINTRAC depending on whether it is a FRFI or not). A more general obligation applies to any person in Canada and any Canadian outside Canada to report to the RCMP or the CSIS transactions or property believed to involve targeted funds.

Sub-criterion 6.5f—The CC and the RIUNRST both prohibit persons from "knowingly" dealing with listed entities. Third parties acting in good faith are thus protected in that they would not be covered under these obligations. The CC further clarifies that any person who "acts reasonably in taking, or omitting to take, measures to comply" with the relevant obligations shall not be liable in any civil action if they took all reasonable steps to satisfy themselves that the relevant property was owned or controlled by or on behalf of a terrorist group. The procedures under the UNAQTR, the RIUNRST, and the CC for delisting and access to frozen funds also apply to protect bona fide third parties.

De-Listing, Unfreezing and Providing Access to Frozen Funds or other Assets

Criterion 6.6—The UNAQTR, CC and RIUNRST set out mechanisms for the delisting of persons or entities that do not meet the designation criteria (respectively in UNAQTR, ss.5.3. and 5.4.; CC, ss.83.05(5) and 2.1., and RIUNRST, s.2.2). Both Regulations and the CC are published in the official Gazette and the relevant procedures are, thus, "publicly known." CC, s.85.05(9) requires the Minister of Public Safety and Emergency Preparedness to review the list of entities every two years to determine whether there are still reasonable grounds for the entities to remain listed. The Minister can recommend to the Governor in Council at any time that an entity be delisted, either as part of the review process or upon application by the listed entity. Information on delisting processes is also set out at: www.international.gc.ca/sanctions/countries-pays/terrorists-terroristes.aspx?lang=eng.

Sub-criterion 6.6a—Under the UNAQTR, the Minister, based on written receipt of a motion to delist under s 5.3, decides whether to forward a petition for delisting to the UN. The Minister's submission must be in accordance with guidance issued by the relevant UN Sanctions Committee. The possibility of a judicial review of the Minister's decision is provided for under s.5.4. Procedures to unfreeze funds of de-listed entities are not available but the obligations under the UNAQTR automatically cease to apply once a person is removed from the UN's list.

Sub-criterion 6.6b—The delisting procedures under the CC and RIUNRST are similar to those under the UNAQTR insofar as a listed entity may apply in writing to the relevant Minister to request to be removed from the list. Upon receipt of a written application for delisting from the relevant Minister, it has 60 days to determine whether there are reasonable grounds to recommend a delisting to the Governor in Council. The applicant can seek a judicial review of this decision.

Sub-criterion 6.6c—Judicial review of the listing decision is available upon receipt of a motion to delist.

Sub-criterion 6.6d and 6.6e—UNAQTR, s.5.3 provides Canadians and any residents of Canada the option to apply to the Minister to be delisted from the 1988 or 1267 sanctions lists in accordance with the Guidelines of the 1988 and 1267 Sanctions Committees.

Sub-criterion 6.6f—Pursuant to UNAQTR, s.10 and RIUNRST, s.10 a person claiming not to be a listed entity may apply to the Minister of Foreign Affairs for a certificate stating that the person is not a listed entity. The Minister then has a specific period of time to issue the certificate if it is established that the individual is not a listed entity. CC, s.83.07 allows an entity claiming not to be a listed entity to apply to the Minister of Public Safety and Emergency Preparedness for a certificate stating that it is not a listed entity.

Sub-criterion 6.6g—Any changes to designations under the UNAQTR, CC or RIUNRST result in the publication of an updated Schedule to the relevant Regulation. For changes to the 1267/1988 lists, FIs and DNFBPs can subscribe to an automatic notification system. OSFI also notifies those entities that have subscribed to its email list of any changes to any of the three listing regimes.

Criterion 6.7—The Minister of Foreign Affairs or the Minister of Public Safety and Emergency Preparedness (for the CC) may grant a person access to frozen funds to cover basic or extraordinary expenses pursuant to UNAQTR, s.10.1, CC, s.83.09 or RIUNRST, s.5.7. Under the UNAQTR, the Minister must notify (for basic expenses) or obtain authorization from (for extraordinary expenses) the relevant UN Sanctions Committee before he/she may grant a motion for access to frozen funds. Once granted, the Minister issues a certification exempting the relevant property or funds from the scope of the Regulations. Under UNAQTR the procedures applied by the Minister have to be in line with the requirements under UNSCR 1452 (2002).

Weighting and Conclusion

There are some shortcomings in regard to the requirements of UN Resolutions 1267, 1988, and 1373. **Canada is largely compliant (LC) with R.6**.

Recommendation 7—Targeted Financial Sanctions Related to Proliferation

R.7 includes new requirements that were not part of the previous assessment.

Criterion 7.1—Two regulations implementing targeted financial sanctions (TFS) relating to Iran and North Korea were issued under Canada's United Nations Act—the *Regulations Implementing the United Nations Resolutions on Iran* (RIUNRI) and the *Regulations Implementing United Nations Resolutions on the Democratic People's Republic of Korea* (RIUNRDPRK). Both require any person in Canada and any Canadian outside Canada to implement TFS in relation to individuals or companies that have been designated by the UN under paragraph 8(d) of UNSCR 1718 (ss.7, 8, and 9 RIUNRDPRK for North Korea) or paragraphs 10 or 12 of UNSCR 1737 (ss.5, 6, 9 and 9.1 RIUNRI for Iran). Under both regulations, it is clear that the relevant prohibition applies only from the date the relevant UNSCR came into force and not retroactively. Neither regulation specifies that sanctions must be applied "without delay," but the relevant obligations and prohibitions apply as soon as a person or entity is included in the UN's list of designated persons, and the communication procedures described under criterion 7.2(d) are sufficient that new listings are brought to the attention of the public. The Security of Canada Information Sharing Act facilitates the implementation of the two regulations by allowing for the exchange of information between government agencies with regards to proliferation of nuclear, chemical, radiological, or biological weapons, either spontaneously or upon request.

Criterion 7.2—Under UN Act, s.2 the Governor in Council issues regulations to give effect to decisions and implement measures decided by the UN Security Council (UNSC) pursuant to Article 41, Chapter VII of the UN Charter. Section 9 of the RIUNRDPRK and RIUNRI impose freezing obligations by prohibiting any person in Canada and any Canadian outside Canada from dealing with; or entering into or facilitating any financial transaction relating to; or providing financial or other related services in relation to property owned or controlled directly or indirectly by a designated person or by a person acting on behalf or at the direction of a designated person.

Sub-criterion 7.2.a—The legal prohibitions are triggered without delay as soon as a person is designated by the UN.

Sub-criterion 7.2b—The above-mentioned prohibitions apply to property owned or controlled by a designated person, including those owned or controlled jointly, or by a person acting on behalf or at the direction of a designated person.

Sub-criterion 7.2c—Under both regulations, it is an offense to make property or any financial or other related services available, directly or indirectly, for the benefit of a designated person. Article 3 of the UN Act prescribes sanctions of a fine of up to Can$100,000 or imprisonment for not more than two years or both (upon summary conviction); or to imprisonment for a term of not more than 10 years (upon conviction on indictment).

Sub-criterion 7.2d—The communication procedures described in criterion 6.5d are also applicable in the context of the RIUNRI and RIUNRDPRK. Canada publishes new designations in the public Canada Gazette, as well as on government websites and through notification services. The Ministry of Foreign Affairs has issued guidance for both sanction regimes.[11]

Sub-criterion 7.2e—All FRFIs and casualty insurance companies, savings and credit unions, and other provincially regulated FIs are required to determine, on a continuous basis, whether they are in possession of targeted funds or property and must freeze such property and regularly report this and any associated information to the competent supervisory authority (ss.11 RIUNRI and RIUNRDPRK). More general obligations apply to any person in Canada and any Canadian outside Canada to report to the RCMP or the CSIS transactions or property believed to involve targeted funds.

Sub-criterion 7.2f—The RIUNRI and RIUNRDPRK prohibitions apply only in cases where a person acts "knowingly." Bona fide third parties acting in good faith are, therefore, protected.

Criterion 7.3—Apart from the notification system outlined, under criterion 7.2.e, Canada does not have a mechanism in place for monitoring compliance by FIs and DNFBPs with the provisions of the RIUNRI and RIUNRDPRK. Sanctions for violations of the Regulations are available, but have never been applied in practice.

Criterion 7.4—Global Affairs Canada provides guidance on its homepage on the procedures and content of the RIUNRI and RIUNRDPRK.[12] While the homepage provides information that needs to be submitted as part of an application to the Minister for delisting, it does not give information on the procedures applied by the Minister to submit delisting requests to the UN on behalf of a designated person or entity.

[11] See www.international.gc.ca/sanctions/countries-pays/iran.aspx?lang=eng; and www.international.gc.ca/sanctions/countries-pays/korea-coree.aspx?lang=eng.

[12] See footnote 16.

Sub-criterion 7.4a—Neither the Regulations nor the Global Affairs' homepage provide information on the availability of the UN Focal Point as a direct or indirect way to effect a delisting.

Sub-criterion 7.4b—Claims of false positives can be filed with and granted by the Minister under RIUNRDPRK, s.14 and RIUNRI, s.16.

Sub-criterion 7.4c—RIUNRDPRK, s.15 and RIUNRI, s.17 further provide for the possibility for the Minister to grant access to frozen funds subject to the conditions and procedures set out in UNSCR 1718 and 1737.

Sub-criterion 7.4d—FIs and DNFBPs can subscribe to the UNs automatic notification system found on its website. OSFI also notifies those entities that have subscribed to its email list of any changes to any of the three listing regimes. Detailed guidance on the provisions of the RIUNRI and RIUNRDPRK is provided on the Global Affairs' homepage.

Criterion 7.5—Neither Regulation allows for additions to frozen accounts, but the Minister may permit such additions on the basis of a one-off exemption. Payments from frozen accounts are permitted under the circumstances set out in relevant UNSCRs based on RIUNRI, s.19 and RIUNDPRK, s.15.

Weighting and Conclusion

There are minor shortcomings in regard to the implementation of the RIUNRI and RIUNRDPRK. **Canada is largely compliant (LC) with R.7.**

Recommendation 8—Non-Profit Organizations

Canada was rated LC with former SR. VIII, with only one deficiency having been identified regarding coordination amongst competent domestic authorities.

Criterion 8.1—Sub-criterion 8.1a—The adequacy of laws and regulations relating to NPOs is reviewed on an ongoing basis and has recently resulted in amendments of various laws and regulations.

Sub-criterion 8.1b—Canada has carried out a risk assessment of its NPO sector and determined that registered charities pose the greatest risk of TF in Canada and, thus, shall fall within the functional definition of "non-profit organization" as defined under the FATF standard. Canada's risk mitigation efforts are primarily focused on registered charities.

The NRA, which focuses on inherent risk, indicates that both for domestically and internationally operating charities, it may be difficult in practice to determine the origin or ultimate use of funds. In addition to the NRA, the CRA in 2015 conducted a comprehensive review of the entire NPO sector. Other relevant studies and reviews include the Canadian Non-Profit and Voluntary Sector in Comparative Perspective in March 2005; the Canada Survey on Giving, Volunteering and Participating in 2010; and the CRA's Non-Profit Organization Risk Identification Project, all of which

provide insight into the way NPOs are organized and operate in Canada. All registered charities, regardless of the value of their assets, as well as non-charitable NPOs with assets in excess of Can$200,000 or annual investment income exceeding Can$10,000, must file an annual Information Return with the CRA, which includes information about their activities, assets and liabilities, and the amount of money received during the fiscal period in question. Incorporated NPOs are subject to additional filing obligations pursuant to the relevant statutes. NPOs must indicate whether they carry out activities outside of Canada (and specify where) and disclose the physical location of their books and records. Through information provided in these returns, the CRA has the capacity to obtain timely information on the activities, size, and relevant features of the NPO sector and to identify those NPOs that are particularly at risk of abuse by virtue of their activities or characteristics.

Sub-criterion 8.1c—The efforts described under the previous sub-criteria are ongoing and continuously integrate new information on the sector's potential vulnerabilities.

Criterion 8.2—Awareness-raising events are focused on registered charities as those are the organizations that fall within the FATF definition of NPOs. The CRA is undertaking efforts to increase awareness amongst registered charities of terrorism financing risks and vulnerabilities, including on international best practices for mitigating terrorism financing risks in the charities sector, sound governance, accountability procedures, transparency reporting, as well as consultative processes and presentations by senior management. The CRA also maintains a grants program to motivate and reward the development and application of innovative compliance programs amongst charities. Many of these activities include a TF component.

Criterion 8.3—Canada imposes comprehensive registration and regulatory requirements on charities under the Income Tax Act (ITA). Other NPOs may operate without being subject to any registration requirements, but are subject to record-keeping obligations on their stated purpose, administration, and management pursuant to the federal or provincial legislation under which they were established. In addition, all registered charities, regardless of the value of their assets, and all NPOs with assets in excess of Can$200,000, or annual investment income exceeding Can$10,000 must file an annual information return with the CRA. Based on the information provided by the authorities, it is estimated that as of December 2014, a total of 180,000 NPOs existed in Canada of which 86,000 or about 50 percent, were registered under the ITA. Under the ITA, a failure by a registered charity to comply with the registration requirements, including links to terrorism, may result in denial or revocation of registration. Under the Charities Registration (Security Information) Act the CRA may utilize all information available to determine the existence of terrorism links for new applications or existing registrations, including security or criminal intelligence and otherwise confidential information. Once registered, charities are required to file annual information returns and financial statements, including information on the directors and trustees, the location of activities, the charity's affiliation and the organization's name. Much of the information is made publicly accessible on the CRA's homepage. Donations, spending, and record keeping are regulated under the ITA. The CRA is granted wide powers under Part XV of the ITA to administer and enforce the provisions of the law. The CRA is responsible for ensuring compliance by registered charities with the

requirements under the ITA and to sanction non-compliance. In addition, law enforcement and intelligence authorities monitor NPOs and investigate those suspected of having links to terrorism.

Criterion 8.4—Based on the information provided by the authorities, it is estimated that as of December 2014 a total of 180,000 NPOs existed in Canada of which 86,000 or about 50 percent, were registered under the ITA. According to the CRA's NPO Sector Review of 2015, the 86,000 registered charities represent 68 percent of all revenues of the NPO sector and nearly 96 percent of all donations. CRA-registered charities also account for a substantial share of the sector's foreign activities as about 75 percent of internationally operating NPOs are registered as charities.

Sub-criteria 8.4a and b—Charities registered under the ITA have comprehensive annual filing obligations, including on their directors and trustees, and financial statements including balance sheets and income statements. All this information is publicly available at the CRA's webpage.

Sub-criterion 8.4c—All registered charities, regardless of their assets, and all other types of NPOs with revenue in excess of Can$200,000, and/or annual investment income exceeding Can$10,000, must file an annual information return with the CRA, including financial information. In addition, registered charities with revenue in excess of Can$100,000 and/or property used for charitable activities over Can$25,000 and/or that have sought permission to accumulate funds, must provide financial information. CRA-Charities must ensure that charities' funds are fully accounted for by reviewing and conducting analysis of information submitted in the annual information return. Where there are irregularities or concerns CRA-Charities may conduct an audit to review charity's finances and activities in detail.

Sub-criterion 8.4d—Registration with the CRA is optional, not mandatory.

Sub-criterion 8.4e—ITA-registered charities are required to know intermediaries that provide services on its behalf, and to ensure that charity funds are used only for charitable activities. As such, there is an obligation to know enough about beneficiaries to meet this obligation. NPOs can be held liable for acts by associated NPOs if the court finds that there is an agency relationship between the two, which provides an additional incentive for NPOs to know associate NPOs. Records of registered charities must be sufficient for the CRA to verify that the charity's resources have been used in accordance with its activities.

Sub-criterion 8.4f—Comprehensive record-keeping obligations apply both for ITA registered charities and other types of NPOs based on the provisions of provincial or federal legislation.

Criterion 8.5—As part of their annual information return, charities must provide a breakdown of financial information related to revenue and expenditures. This includes information on the total expenditures for charitable activities, management and administration, and gift to qualified donees. Charities must also report ongoing and new charitable programs. Where audits reveal financial irregularities, the CRA may apply a range of sanctions set out in the ITA. The CRA is granted a wide range of powers to monitor registered charities for compliance with the filing obligations under the

ITA and to apply sanctions, including financial penalties and suspensions, or revocation of registration.

Criterion 8.6—Sub-criterion 8.6.a—For registered charities, the registration system under the ITA is supported by the Charities Registration (Security Information) Act which allows the Minister of Public Safety and Emergency Preparedness to take into account criminal and security intelligence reports on registered charities or those applying for registration. The CSIS and also the RCMP and CBSA contribute information to these criminal and security intelligence report. The CRA has entered into MOUs with the CSIS and RCMP to facilitate the process. Any suspicion that a specific charity is linked to terrorism may result in registration being denied or revoked.

Sub-criterion 8.6.b—For ITA registered charities, the CRA may share certain information about registered charities with the public, including foreign counterparts, online through the CRA's website, or upon request. Information that is publicly accessible includes governing documents, the name of directors or trustees, annual information returns, and financial statements.

Sub-criterion 8.6.c—For non-publicly available information, the ITA allows but does not oblige the CRA to disclose to FINTRAC, as well as the RCMP and CSIS, information about charities suspected of being involved in FT. Equally, the Security of Canada Information Sharing Act (SCISA) permits the CRA to share any taxpayer information relevant to a terrorism offense (under part II of the CC) or threats to the security of Canada (under the CSIS Act) with competent authorities, including any information that the CRA may have on the broader sector of NPOs. FINTRAC is required under the PCMLTFA to disclose information to the CRA with regards to registered charities. Additional information-sharing powers are available under the Security of Canada Information Sharing Act whenever there is a threat to Canada's national security. For NPOs other than registered charities, regular investigative and information-gathering powers under the criminal procedure code are available to obtain records and information they are required to maintain under provincial or federal NPO legislation.

Criterion 8.7—The CRA may share certain information about registered charities with foreign counterparts, including governing documents, the names of directors or trustees, annual information returns, and financial statements. Additional information may be shared by the CRA with foreign tax authorities. If required, information on registered charities or NPOs may also be shared by FINTRAC and the RCMP as described under R.40 or based on formal MLA. In sum, Canada is found to have appropriate points of contact and procedures in place to respond to international request for information sharing regarding particular NPOs.

Weighting and Conclusion

Canada is compliant (C) with R.8.

Recommendation 9—Financial Institution Secrecy Laws

In its 2008 MER, Canada was rated C with R.4, and neither the relevant laws nor the applicable FATF R. have subsequently changed. The MER assessors' only concern was that data protection law implementation was subject to excessively strict interpretations that might prevent LEAs accessing information in the course of investigations.

Criterion 9.1—Various constitutional and legal provisions impose confidentiality obligations over personal information and individuals' privacy. In particular, s.8 of the Canadian Charter of Rights and Freedoms (which forms part of Canada's Constitution) provides that everyone has the right to be secure against unreasonable search and seizure. According to the Supreme Court of Canada, the purpose of s.8 is to protect a reasonable expectation of privacy. Accordingly, those who act on behalf of a government, including LEAs and supervisors, must carry out their duties in a fair and reasonable way. Canada also has two privacy laws: the Privacy Act covers the personal information-handling practices of federal government departments and agencies; and the PIPEDA is the main federal private-sector privacy law.

PIPEDA, s.5 notably contains specific obligations concerning organizations' collection, dissemination, and use of customers' personal information. Every province and territory has its own public-sector legislation and the relevant provincial act applies to provincial government agencies (in lieu of the Privacy Act). Some provinces also have private-sector privacy legislation. Alberta, British Columbia, and Québec notably have legislation that have been declared "substantially similar" to the PIPEDA and apply to private-sector businesses that collect, use, and disclose personal information while carrying out business within these provinces. Finally, several federal and provincial sector-specific laws also include provisions dealing with the protection of personal information: The federal Bank Act, in particular, contains provisions regulating the use and disclosure of personal financial information by FRFIs (ss.606 and 636 (1)); and most provinces also have laws governing credit unions that require the confidentiality of information related to members' transactions.

Various provisions also govern the authorities' access to information: of the PIPEDA, s.7(3)(d), in particular, provides that an organization may, without the individual's knowledge or consent or judicial authorization, disclose personal information that it has reasonable grounds to believe could be useful in the investigation of a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed and the information is used for the purpose of investigating that contravention. The "substantially similar" laws in Alberta, British Columbia, and Quebec contain broadly equivalent provisions. The PCMLTFA also contains a number of provisions that enable FINTRAC to access information (ss.62-63) and the Bank Act (ss.643-644) and equivalent provisions governing other FRFIs gives OSFI powers to access all records of FRFIs.

As regards sharing of information between competent authorities, implementation of the Privacy Act, which obliges federal government departments and agencies to respect privacy rights, does not seem to have caused AML/CFT problems. The PCMLTFA (ss.55, 55.1, 56 and 65(1) and (2)) empowers FINTRAC to disclose information to a range of law enforcement and other competent authorities within Canada in specified circumstances. Similarly, the PCMLTFA, s.65.1(1)(a) allows FINTRAC to

make agreements with foreign counterparts to exchange compliance information. The Bank Act, s 636(2) also enables OSFI to disclose information to other governmental agencies.

Weighting and Conclusion

Canada is compliant (C) with R.9.

Recommendation 10—Customer Due Diligence

In the 2008 MER, Canada was rated NC with R.5. There were numerous deficiencies, and also the CDD requirement did not cover all FIs as defined by the FATF. Subsequently, both the PCMLTFA and PCMLTFR were amended to include measures covering the circumstances in which CDD must take place. Further PCMLTFR amendments, effective from February 2014, addressed most of the remaining deficiencies.

The 2008 MER noted that the requirement to conduct CDD excluded financial leasing, factoring, and finance companies. The Sixth FUR (2014) concluded that the set of sectors not covered by the AML/CFT regime and not yet properly risk assessed was not a major deficiency. Since then, Canada's NIRA assessed the ML/TF vulnerabilities of factoring, finance, and financial leasing companies as medium risk, while pointing out that these entities were very small players. Sectors not covered by the AML/CFT regime are continually evaluated to identify trends indicating a higher ML/TF risk rating. Their current exclusion from the scope of the AML/CTF regime is an ongoing minor deficiency.

Criterion 10.1—In its 2008 MER, Canada explained that, while there was no explicit prohibition on opening anonymous accounts, the basic CDD requirements on all new account holders effectively prohibited anonymous accounts. This also applied to accounts in obviously fictitious names. The legal position remains unchanged: The PCMLTFA, s.6.1, requires REs to verify identity in prescribed circumstances and s.64 of the PCMLTFR sets out the measures to be taken for ascertaining identity. However, the 2008 assessors were concerned about the absence of detailed rules or guidance for FIs' use of numbered accounts, including compliance officers having access to related CDD information. Subsequently, OSFI Guideline B-8 addressed this latter point, covering the provision of account numbering or coding services that effectively shield the identity of the client for legitimate business reasons. Thus, FRFIs should ensure that they had appropriately ascertained the identity of the client and that the firm's Chief AML Officer could access this information. Consequently, this deficiency has been partially addressed through an adequate control mechanism, for FRFIs only, albeit not by enforceable means. This is a relatively minor matter.

When CDD is Required

Criterion 10.2—PCMLTFR ss.54, 54.1, 55, 56, 57, 59(1), 59(2) and 59(3) of the require FIs to ascertain the identity of their clients when establishing business relations. Similarly, all REs must ascertain the identity of every client with whom they conduct an occasional large cash transaction of Can$10,000 or more. Two or more such transactions that total over Can$10,000, conducted within a period of

24 hours, are deemed a single transaction. CDD is required for both cross-border and domestic wire transfers exceeding Can$1,000.

Pursuant to PCMLTFR s.53.1(1) FIs must) take reasonable measures to verify the identity of every natural person or entity who conducts, or attempts to conduct, a transaction that should be reported to FINTRAC (i.e., where there is suspicion of ML or TF). This obligation applies (s.62(5)) even when it would not otherwise have been necessary to verify identity. Also, FIs must reconfirm (s.63 (1.1) of the PCMLTFR) the client's identity where doubts have arisen about the information collected. However, this measure applies only to natural persons, not to legal persons or arrangements.

The limited application of this last measure remains a deficiency under 10.2(e).

Required CDD Measures for all Customers

Criterion 10.3—PCMLTFA, s.6.1 of the requires REs to verify the identity of a person or entity in prescribed circumstances and in accordance with the Regulations. PCMLTFR ss.64 to 66 detail the measures that REs must take to ascertain the identity of a prescribed individual, corporation and "entity other than a corporation.[13]" For individuals, acceptable identification documents include a birth certificate, driver's license, passport, or other similar document. For corporations, the corporation's existence is confirmed, and the names and addresses of its directors ascertained, by reference to its certificate of corporate status. However, other methods are acceptable, e.g., a record that it is required to file annually under applicable provincial securities legislation or any other record that validates its existence as a corporation. The existence of an entity other than a corporation must be confirmed by reference to a partnership agreement, articles of association, or other similar record that ascertains its existence. These legal provisions meet the FATF standard.

Criterion 10.4—The "Third Party Determination" provisions of the PCMLTFR require FIs to determine whether their customers are acting on behalf of another person or entity. Where an account is to be used by or on behalf of a third party, the FI must collect CDD information on that third party and establish the nature of the relationship between third party and account holder.

Criterion 10.5—PCMLTFR s.11.1(1) requires FIs, at the time the entity's existence is confirmed, to obtain the following information:

- For corporations, the name of all directors of the corporation and the name and address of all persons who own or control, directly or indirectly, 25 percent or more of the shares of the corporation;

- For trusts, the names and addresses of all trustees and all known beneficiaries and settlors of the trust;

[13] This is not defined in the Regulations, but would include any kind of unincorporated business or legal arrangement.

- For entities other than corporations or trusts (typically, a partnership fund or unincorporated association or organization), the name and address of all persons who own, directly or indirectly, 25 percent or more of the shares of the entity; and

- In all cases, information establishing the ownership, control, and structure of the entity.

Under the PCMLTFR, s.11.1(2), REs further need to "take reasonable measures to confirm the accuracy of the information obtained" on beneficial ownership. This requirement implies the need to use reliable sources to obtain the requisite information and the FATF standard[14] allows identification data to be obtained "from a public register, from the customer, or from other reliable sources." Also, OSFI Guideline B-8 usefully indicates that "reasonable measures" to identify ultimate beneficial owners could include not only requesting relevant information from the entity concerned, but also consulting a credible public or other database or a combination of both. This Guideline also makes clear that the measures applied should be "commensurate with the level of assessed risk."

No specific legal provisions cover beneficial ownership of personal accounts. However, the PCMLTFR, in effect, establish beneficial ownership of personal accounts: in particular, s.9 requires REs to determine whether personal accounts are being used on behalf of a third party and, for personal accounts in joint names, all authorized signatories are subject to CDD measures.

Criterion 10.6—PCMLTFR, s.52.1, requires every person or entity that forms a business relationship under the Regulations to keep a record of the purpose and intended nature of that business relationship. OSFI Guideline B-8 amplifies this requirement, requiring a FRFI to be satisfied that the information collected demonstrates that it knows the client.

Criterion 10.7—PCMLTFR ss.54.3 (financial entities), 56.3 (life insurance sector), 57.2 (securities dealers), 59.01 (MSBs), and 61.1 (departments or agencies of the government or provinces that sell or redeem money orders) require all covered REs to conduct ongoing monitoring of their business relationships. Section 1(2) defines this to mean monitoring on a periodic basis, according to assessed risk, by a person or entity of their business relationships with clients for the purpose of (i) detecting transactions that must be reported to FINTRAC; (ii) keeping client identification information up to date; (iii) reassessing levels of risk associated with clients' transactions and activities; and (iv) determining whether transactions or activities are consistent with the information.

Where higher risks are identified, PCMLTFR, ss.71.1(a)-(c)) require "prescribed special measures" to be taken, which include enhanced measures to keep client identification and beneficial ownership information up to date and also to monitor business relationships in order to detect suspicious transactions. The Regulations do not explicitly cover scrutiny of the source of funds.

[14] FATF Methodology (February 2013), p.147.

Specific CDD Measures Required for Legal Persons and Legal Arrangements

Criterion 10.8—The PCMLTFR requirements for FIs to understand the nature of the customer's business and its ownership and control structure cover legal persons or legal arrangements.

Criterion 10.9—See c.10.3 above, which covers identification and verification of legal persons and arrangements. The PCMLTFR (ss.14(b), 14.1(b), 15(1)(c), 20, 23(1)(b), 30(b) and 49(b)) require the collection of information on power to bind the legal person or arrangement in relation to an account or transaction. However, the Regulations do not cover gathering the names of relevant persons having a senior management position in the legal person or arrangement. Where an RE is unable to obtain information about the ownership, control, and structure of a trust or other legal arrangement, the PCMLTFR (s.11.1(4)(a)) require reasonable measures to be taken to ascertain the identity of the most senior managing officer of the entity concerned.

The Regulations (s.65(1)) require confirmation of a corporation's existence, and its name and address, by reference to its certificate of corporate status or other acceptable official record. The existence of an entity other than a corporation must be confirmed by referring to a partnership agreement, articles of association, or other similar record. There is no specific requirement, in this case, to obtain the address of the registered office or principal place of business, if different. Consequently, for non-corporate legal persons and for legal arrangements such as trusts, the standard is only partially met. Partnership agreements, etc., are unlikely to confirm details of address and principal place of business. Similarly, while trust documents usually contain sufficient information to satisfy the account-holding FI as to name, legal form, and proof of existence; such documents usually do not provide additional information about the registered address or principal business of the trust.

In addition, trust companies are required, when acting as trustee of a trust (ss.55 (a)–(c)) to (i) of the PCMLTFR) to ascertain the identity of every person who is the settlor of an inter vivos trust: (ii) confirm the existence of, and ascertain the name and address of, every corporation that is the settlor of an institutional trust; and (iii) confirm the existence of every entity, other than a corporation, that is the settlor of an institutional trust. Under the Regulations (s.55 (d)), where an entity is authorized to act as a co-trustee of any trust, the trust company must (i) confirm the existence of the entity and ascertain its name and address; and (ii) ascertain the identity of all persons—up to three—who are authorized to give instructions with respect to the entity's activities as co-trustee. Finally, under the Regulations (s.55 (e)), trust companies must ascertain the identity of each person who is authorized to act as co-trustee of any trust. However, as natural persons who are trustees are not REs under the PCMLTFA, they are not subject to CDD obligations.

PCMLTFR ss.11 (a)–(b) require trust companies, for inter vivos trusts, to (i) keep a record that sets out the name and address of each of the beneficiaries that are known at the time that the trust company becomes a trustee for the trust; (ii) if the beneficiary is a natural person, record their date of birth and the nature of their principal business or their occupation; and (iii) if the beneficiary is an entity, the nature of their principal business.

Criterion 10.10—The legal requirements for obtaining information on beneficial owners of customers that are legal persons are set out under c.10.5 above.

REs must confirm the existence of a corporation or non-corporate legal entity at the opening of an account or when conducting certain transactions. At the same time, they must obtain information about the entity's beneficial ownership and confirm its accuracy. Beneficial ownership refers to the identity of the individuals who ultimately control the corporation or entity, which extends beyond another corporation or another entity. The PCMLTFR requirements for corporations and other entities refer to "persons." PCMLTFA, s.2 defines "person" to mean an individual, which therefore requires the natural person to be identified. If the RE has doubts about whether the person with the controlling ownership interest is the beneficial owner, then it is deemed to have been unable to obtain the information referred to under PCMLTFR, s.11.1(1) or to have been unable to confirm that information in accordance with PCMLTFR, s.11.1(2). In this case, the RE is required, under PCMLTFR s.11.1(4), to: take reasonable measures to ascertain the identity of the most senior managing officer of the entity; treat that entity as high risk for the purpose of PCMLTFA, s.9.6(3) and apply the prescribed special measures set out in PMCLTFR, s.71.1. Where no individual ultimately owns or controls 25 percent or more of an entity, directly or indirectly, REs must nevertheless record the measures they took, and the information they obtained, in order to reach that conclusion. Also, REs must comply with PCMLTFR, s.11.1(1)(d), which requires that information "establishing the ownership, control and structure of the entity" be obtained.

Criterion 10.11—The legal requirements for collecting information on the identity of beneficial owners of customers that are legal arrangements are set out under c.10.5 and 10.9 above. It is unclear, in the case of trusts, what identification requirements apply to protectors. Beneficiaries of trusts are covered by the ongoing monitoring provisions of s. 1(2) of the Regulations, which require that client identification information and information be kept up to date.

CDD for Beneficiaries of Life Insurance Policies

Criterion 10.12—All provincial *Insurance Acts* require life insurance companies to conduct CDD on (and keep a record of) the beneficiaries of life insurance policies, so this requirement applies to insurance companies nationally. There is no specific requirement to verify the identity of the beneficiary at the time of payout.

Criterion 10.13—As life insurance companies are covered under the PCMLTFA, they must risk assess all their clients and business relationships, products and services, and any other relevant risk factors (which include the beneficiary of a life insurance policy). In cases of high risk, life insurance companies must apply enhanced measures (prescribed special measures—s.71.1 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations*).

Timing of Verification

Criterion 10.14—PCMLTFR, ss.64(2), 65(2) and 66(2)) specify the timeframe for verifying the identity of individuals, corporate and non-corporate entities. With certain exceptions, the legal obligation is

to verify identity either at the time of the transaction or before any transaction other than an initial deposit is carried out. There are two main exceptions: (i) in relation to trust company activities, identity may be verified within 15 days of the trust company becoming the trustee; (ii) in relation to life insurance transactions and government or provincial departments or agencies handling money orders, identity may be verified within 30 days of the client information record being created. These exceptions are not justified according to what is reasonably practicable or necessary to facilitate the normal conduct of business, nor is there any condition about managing the ML/TF risks of delaying identity verification.

Criterion 10.15—PCMLTFR, s.1(2) defines "business relationship" to commence on account opening or when a client conducts specified transactions that would require their identity to be ascertained. Consequently, it is not possible for a customer to utilize a business relationship prior to verification.

Existing Customers

Criterion 10.16—See c.10.7. These ongoing monitoring obligations apply to all clients, whether or not they were clients at the date of new CDD obligations coming into force. Consequently, the ongoing monitoring process covers clients whose identity had not previously been ascertained. REs are required to take a risk-based approach to keeping information on client identification, beneficial ownership and purpose, and nature of intended business relationship up to date.

Risk-Based Approach

Criterion 10.17—PCMLTFR, s.71.1 details the "prescribed special measures" to be taken in cases of high risk. This includes, for example, cases where beneficial ownership information cannot be obtained or confirmed. These special measures comprise taking enhanced measures to (i) ascertain the identity of a person or confirm the existence of an entity; (ii) keep client identification information up to date (including beneficial ownership information); (iii) monitor business relationships for the purpose of detecting suspicious transactions; and (iv) determining whether transactions or activities are consistent with the information. In addition, Appendix 1 to FINTRAC Guideline 4 provides a checklist of products or services that should be considered high-risk.

Criterion 10.18—No reduced or simplified CDD measures are in place. Instead, the PCMLTFR gives exemptions from the client identification and record-keeping requirements in specific circumstances assessed as low risk by the authorities. These exemptions are mainly contained in s. 9 (accounts used by, or on behalf of, a third party) and s.62 (mainly concerning life insurance business). Furthermore, PCMLTFR, ss.19 and 56 create a form of exemption by requiring that life insurers only conduct CDD in relation to the purchase of an immediate or deferred annuity or a life insurance policy for which the client may pay Can$10,000 or more over the duration of the annuity or policy. However, these exemptions do not apply where there is a suspicion of ML or TF.

Failure to Satisfactorily Complete CDD

Criterion 10.19—The PCMLTFA, s.9.2, provides that no RE shall open an account for a client if it cannot establish the identity of the client in accordance with the prescribed measures. Consequently, an FI that failed to conduct CDD, when obliged to do so, would be in breach of the Act and could be fined. There is no explicit prohibition on REs commencing a business relationship or performing a transaction when they are unable to comply with CDD measures if the identity of an individual cannot be ascertained or the existence of an entity confirmed when they open an account, the FI cannot open the account. This also means that no transaction, other than an initial deposit, can be carried out. Also, if the RE suspects that the transaction is related to a ML or TF offense, it must file an STR with FINTRAC. Under PCMLTFA, s.7, if the RE has reasonable grounds to suspect that the client conducts or attempts to conduct a transaction that is related to the commission or the attempted commission of an ML or TF offense, even if the client cannot be identified or his/her identity cannot be properly verified, the RE must file a STR. This requirement is amplified in FINTRAC guidance.

CDD and Tipping Off

Criterion 10.20—PCMLTFR, s.53.1 (2) specifies that the identity verification obligation does not apply where the RE believes that complying with that obligation would inform the customer that the transaction is being reported as suspicious. PCMLTFA s.7 requires an STR to be filed in these circumstances.

Weighting and Conclusion

A number of relatively minor deficiencies have been identified. **Canada is largely compliant (LC) with R.10.**

Recommendation 11—Record-Keeping

In the 2008 MER, Canada was rated LC with R.10. Two deficiencies were noted. First, the record-keeping requirement did not cover all FIs as defined by the FATF (notably financial leasing, factoring, and finance companies). Second, FIs must ensure that all records required to be kept under the PCMLTFA could be provided within 30 days, which did not meet the requirement to make CDD records available on a timely basis. The FATF standard has not since changed, the requirement being to make records available "swiftly."

Criteria 11.1 and 11.2—The PCMLTFRs.69 detail the obligation to keep records for a period of at least five years following completion of the transaction or termination of the business relationship.

The PCMLTFR outlines, for each type of covered entity, detailed record-keeping rules for CDD, account files and business correspondence. The Regulations do not specifically require retention of any internal analysis of client business that might lead to an STR. However, covered entities would need to keep this information to substantiate that they were not in contravention of PIPEDA and that the disclosure without consent would have been warranted. The Privacy Commissioner could

request this type of information under PIPEDA, s.18 as part of a compliance audit. In addition, OSFI requires FRFIs to keep such information.

Criterion 11.3—There is no clear legal obligation that transaction records be sufficient to permit reconstruction of individual transactions. However, the Regulations do specify in detail the contents of each piece of information that must be held in various records.

Criterion 11.4—The PCMLTFR s.70 requires REs to provide records upon request of FINTRAC within 30 days. This does not meet the "swiftly" standard.

Weighting and Conclusion

The deficiencies noted in the 2008 MER remain. **Canada is largely compliant (LC) with R.11.**

Recommendation 12—Politically Exposed Persons

In the 2008 MER, Canada was rated NC with R.6. There were no relevant legislative or other enforceable requirements in place.

Significant changes have been introduced since then. Requirements for FIs in relation to Politically Exposed Foreign Persons (PEFPs) were introduced in June 2008 through amendments to the PCMLTFA and PCMLTFR, specifying the enhanced customer identification and due-diligence requirements for such clients.

Subsequently, as part of a package of amendments to the PCMLTFA introduced in 2014, the coverage of the Act was extended to include Politically Exposed Domestic Persons (PEDP) and heads of international organizations. The bill was enacted on June 19, 2014; however, implementing regulations are required before the PEP provisions will come into force. These regulations, announced on July 4, 2015, will come into force one year after registration of the regulations. They will require REs to determine, under prescribed circumstances, whether a client is a PEFP, a PEDP, a head of an international organization, or a close associate or prescribed family member of any such person.

Criterion 12.1—The PCMLTFR ss.54.2, 56.1, 57.1, 59(5) require REs to take reasonable measures to determine a person's status as a PEFP. FINTRAC Guidance 6G explains the PEP determination and OSFI Guideline B-8 is also relevant.

FINTRAC Guidance (s.8.1) makes clear that reasonable measures must be taken in relation to both new and existing accounts, as well as certain electronic funds transfers (EFT). Also, those measures include asking the client or consulting a credible commercially and/or publicly available database. OSFI Guideline B-8 also details what would constitute reasonable measures to make a PEFP determination.

PCMLTFA s.9.3.2 requires REs, when dealing with a PEFP, to obtain the approval of senior management in the prescribed circumstances and take prescribed measures. For existing accounts,

PCMLTFR, s.67.1(b) requires FIs and securities dealers to obtain the approval of senior management to keep a PEFP account open. FINTRAC Guidance 6G explains when to obtain the approval of senior management.

The Regulations (s.67.2) also require REs to take reasonable measures to establish the PEFP's source of funds. FINTRAC Guidance 6G explains that reasonable measures include asking the client and OSFI Guideline B-8 gives a number of examples of acceptable sources of funds. Source of wealth is not mentioned in the Regulations; however, Guideline B-8 states that FRFIs should satisfy themselves that the amount of clients' accumulated funds or wealth appears consistent with the information provided.

The Regulations (s.67.1(1)(c)) require FIs and securities dealers to conduct enhanced ongoing transaction monitoring of PEFP and their family members' accounts. However, no similar legal requirement applies to other REs in relation to PEFPs, although FINTRAC Guidance 6G does specify enhanced ongoing monitoring of PEFP account activities. OSFI Guideline B-8 states that enhanced ongoing transaction monitoring may involve manual or automated processes, or a combination, depending on resources and needs and gives some examples of what this could comprise.

Criterion 12.2—OSFI Guideline B-8 explains that FRFIs are not (currently) under any legal obligation to identify domestic PEPs *per se*, whether by screening or flagging large transactions or in any other way. Further, even if FRFIs know they are dealing with a domestic PEP, until new regulations come into effect, they have no legal obligation to apply enhanced measures to PEDPs as they do to PEFP accounts.

Nevertheless, this OSFI guidance states that, where a FRFI is aware that a client is a domestic PEP, it should assess any effect on the overall assessed risk of the client. If that risk is elevated, the FRFI should apply appropriate enhanced due-diligence measures.

Criterion 12.3—Currently, PCMLTFA, s.9.3 includes family members of PEFPs and PCMLTFR, (s.1.1) states that the prescribed family members of a PEFP are included in the definition of a PEFP. Until the necessary implementing regulations take effect, close associates of any kind of PEP are not covered in law or regulations.

Criterion 12.4—No provisions in law or regulations relate to beneficiaries of life insurance policies who may be PEPs.

Weighting and Conclusion

Canada is non-compliant (NC) with R.12.

Recommendation 13—Correspondent Banking

In the 2008 MER, Canada was rated PC with R.7. Deficiencies were noted in relation to: assessment of a respondent institution's AML/CFT controls; assessment of the quality of supervision of respondent institutions; and inadequate CDD for payable-through accounts.

Criterion 13.1—The PCMLTFR (s.15.1 (2)) cover correspondent banking relationships, requiring FIs to collect a variety of information and documents on the respondent institution. That information includes: the primary business line of the respondent institution; the anticipated correspondent banking account activity of the foreign FI, including the products or services to be used; and the measures taken to ascertain whether there are any civil or criminal penalties that have been imposed on the respondent institution in respect of AML/CFT requirements and the results of those measures. The Regulations contain no specific requirements about determining either the reputation of the respondent institution or the quality of supervision to which it is subject. The PCMLTFR (s.15.1(3)) require the taking of reasonable measures to ascertain whether the respondent institution has in place AML/CFT policies and procedures, including procedures for approval for the opening of new accounts. There is, however, no requirement to assess the quality of a respondent institution's AML/CFT controls. PCMLTFA s.9.4 (1) requires senior management approval to be obtained for establishing new correspondent relationships. The Regulations (s.15.1(2)(f)) specify the collection of a copy of the correspondent banking agreement or arrangement, or product agreements, defining the respective responsibilities of each entity.

Criterion 13.2—The PCMLTFR (s. 55.2) stipulate that where the customer of the respondent institution has direct access to the services provided under the correspondent banking relationship (the 'payable-through account' scenario), the FI shall take reasonable measures to ascertain whether (i) the respondent institution has met the customer identification requirements of the Regulations; and (ii) the respondent institution has agreed to provide relevant customer identification data upon request.

Criterion 13.3—PCMLTFA, s.9.4 (2) prohibits correspondent banking relationships with a shell bank. In addition, the PCMLTFR (s.15.1 (2) (h) require FIs to obtain a statement from the respondent institution that it does not have, directly or indirectly, correspondent banking relationships with shell banks.

Weighting and Conclusion

Deficiencies remain under c.13.1. **Canada is largely compliant (LC) with R.13.**

Recommendation 14—Money or Value Transfer Services

In its 2008 MER, Canada was rated NC with SR VI. The main deficiencies were: lack of a registration regime for money services businesses (MSBs); no requirement for MSBs to maintain a list of their agents; and the sanction regime available to FINTRAC and applicable to MSBs was deemed not effective, proportionate, and dissuasive. Subsequently, Canada has made significant progress, and the FATF standard has been strengthened to require countries to take action to identify unlicensed or unregistered MSBs and apply proportionate and dissuasive sanctions to them.

Criterion 14.1—PCMLTFA, s.11.1 stipulates that any entity or person covered by s.5(h) of the Act, (persons and entities engaged in the business of foreign exchange dealing, of remitting funds or transmitting funds by any means or through any person, entity or electronic funds transfer network,

or of issuing or redeeming money orders, traveler's checks or other similar negotiable instruments) and those referred to in s.5(l) of the Act (those that sell money orders to the public), must be registered with FINTRAC.

Criterion 14.2—Under its mandate (PCMLTFA, s.40(e)) to ensure compliance with part 1 of the Act, FINTRAC has a process for identifying MSBs that carry out activities without registration. This includes searching advertisements and other open sources as well as through on-site visits. Additionally, MVTS whose registration status is revoked, are still tracked to ensure that they are not conducting business illegally.

The PCMLTF Administrative Monetary Penalties (AMP) Regulations describe the classification of different offenses under the PCMLTFA and the Regulations. Failure to register is classified as a serious violation. These Regulations classify violations as minor, serious, and very serious, each with a varying range of monetary penalties, up to Can$500,000. In addition to criminal sanctions and monetary penalties for non-compliance, FINTRAC uses other means to encourage compliance. Monetary penalties are only considered after giving an entity or person a chance to correct deficiencies. If a very serious violation has been committed, a fine is greater than Can$250,000, or if there is repeat significant non-compliance, FINTRAC considers publicly naming that entity or person, using its powers under s.73.22 of the PCMLTFA.

Criterion 14.3—PCMLTFA s.40 (e) gives FINTRAC the mandate to ensure compliance with the Act. FINTRAC uses its powers under the PCMLTFA (ss. 62, 63 and 63.1) to examine records and inquire into the business and affairs of REs to monitor MVTS providers for AML/CFT compliance.

Criterion 14.4—PCMLTFA, ss.11.12(1) and (2) require that a list of agents, mandataries or branches engaged in MSB services on behalf of the applicant be submitted upon registration of the MSB with FINTRAC. S.11.13 of the Act stipulates that a registered MVTS must notify FINTRAC of any change to the information provided in the application or of any newly obtained information within 30 days of the MVTS becoming aware of the change or obtaining the new information. This includes information about the MVTS's agents.

This criterion is also met through the legal obligation described under c.14.1 above.

Criterion 14.5—The PCMLTFR (s.71(1)(d)) require MVTS, who have agents or other persons authorized to act on their behalf, to develop and maintain a written ongoing compliance training program for those agents or persons. S.71(1)(e) also requires MVTS to institute and document a review of their agents' policies and procedures, risk assessment, and the training program for the purpose of testing effectiveness. Such reviews must be carried out every two years.

Weighting and Conclusion

Canada is compliant (C) with R.14.

Recommendation 15—New Technologies

In the 2008 MER, Canada was rated NC with former R.8 due to the lack of legislative or other enforceable obligations addressing the risks of new technological developments. Since then, some 40 legislative amendments to the PCMLTFA were tabled in Parliament (e.g., measures to subject new types of entities to the PCMLTFA, including online casinos, foreign MSBs and businesses that deal in virtual currencies such as Bitcoin). Canada is currently developing regulatory amendments to cover pre-paid payment products (e.g., prepaid cards) in the AML/CTF regime. The NRA examined the ML/TF vulnerabilities of 27 economic sectors and financial products, including new and emerging technologies, both in terms of products (e.g., virtual currency and pre-paid access), and sectors (e.g., telephone and online services in the banking and securities sectors).

Criterion 15.1—REs must conduct a risk assessment that includes client and business relationships, products and delivery channels, and geographic location of activities of the RE and the client(s), and any other relevant factors (PCMLTFR. s.71(1)(c)). While the requirements capture the need to assess ML/TF risks related to products and delivery mechanisms, there is no explicit legal or regulatory obligation to similarly risk assess the development of new products and business practices, nor is there any such obligation relating to the use of new or developing technologies for new and pre-existing products. However, Canada issued regulatory amendments for public comment in July 2015 clarifying that REs must consider, in their risk assessment, any new developments in, or the impact of new technologies on, the RE's clients, business relationships, products or delivery channels or the geographic location of their activities. A risk assessment review must be conducted every two years by an internal or external auditor, or by the entity (s.71(1)(e) of the Regulations). This ensures that risk assessments are regularly evaluated to capture risks, which may include new technologies. FINTRAC Guideline 4 specifies that new technology developments (e.g., electronic cash, stored value, payroll cards, electronic banking, etc.) must be included in a company's risk assessment.

Criterion 15.2—While there is a regulatory expectation in FINTRAC's risk-based approach guidance[15] which states that REs should reassess their risk if there are changes due to new technologies or other developments, there are no explicit requirements in law or regulation that FIs undertake risk assessments prior to the launch or use of such products, practices, and technologies.

Weighting and Conclusion

Canada is non-compliant (NC) with R.15.

Recommendation 16—Wire Transfers

In the 2008 MER, Canada was rated NC with SR VII, which had simply not been implemented. Canada made some progress since then. The requirements have also been very substantially

[15] See www.fintrac-canafe.gc.ca/publications/rba/rba-eng.pdf.

expanded in R.16 (i.e., inclusion of beneficiary information in wire transfers and additional obligations on intermediary and beneficiary FIs and MSBs).

Ordering Financial Institutions

Criterion 16.1—PCMLTFA, s.9.5 requires FIs to include with the transfer, when sending an international EFT, the name, address, and account number or other reference number, if any, of the client who requested it. The Act has no equivalent provision about including beneficiary name, account number or unique transaction reference number in this 'ordering FI' scenario. However, Schedule 2, Part K, of the PCMLTFR, which covers outgoing SWIFT payment instructions report information, does stipulate that, for single transactions of Can$10,000 or more, the beneficiary client's name, address and account number (if applicable) should be included. There are no enforceable provisions requiring FIs to include beneficiary information in EFTs below Can$10,000 (either as a single transaction, or multiple transactions within a 24-hour period).

Criterion 16.2—PCMLTFA s.9.5 is not limited to single transfers—it, therefore, also applies in cases where numerous individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries.

Criterion 16.3—There is no 'de minimis' threshold for the requirements of c.16.1.

Criterion 16.4—Originator information would be verified through CDD obligations (see R.10). In addition, s.53.1 of the Regulations states that the identity of every person that conducts a suspicious transaction must be ascertained, unless it was previously ascertained, or unless the FI believes that doing so would inform the individual an STR was being submitted.

Criterion 16.5—The Act's s.9.5 requirements cover both domestic and international EFTs.

Criterion 16.6—Canada does not permit simplified originator information to be provided.

Criterion 16.7—The PCMLTFR (ss.14 (m) and 30 (e)) require FIs and MSBs to keep a record of the name, address and account number, or transaction reference of the ordering client for all EFTs of Can$1,000 or more. In addition, a record must be kept of the name and account number of the recipient of the EFT, as well as the amount and currency of the transaction.

Criterion 16.8—There is no explicit prohibition on executing wire transfers where CC, ss.16.1 to 16.7 above cannot be met. However, if an RE is unable to comply with the relevant legal requirements, it cannot proceed with a wire transfer without breaking the law and being subject to AMPs.

Intermediary Financial Institutions

Criteria 16.9–16.12—The PCMLTFA and regulations use the terms "send/transfer" and "receive" to apply obligations to intermediaries, which are, therefore, subject to the same requirements that apply to ordering and beneficiary institutions. Thus, the implications of possible data loss and of straight-through processing are not captured, as they should be to meet the standard.

Beneficiary Financial Institutions

Criterion 16.13—PCMLTFA, s.9.5(b) requires FIs to take reasonable measures to ensure that any transfer received by a client includes information on the name, address, and account number or other reference number, if any, of the client who requested the transfer. These requirements apply equally to all EFTs, regardless of where they are situated in the payment chain. Where an FI is transmitting a transfer received from another FI, it is, therefore, required to ensure that complete originator information is included. There are no legal requirements relating to beneficiary information.

OSFI Guideline B-8 states that FRFIs that act as intermediary banks should develop and implement reasonable policies and procedures for monitoring payment message data subsequent to processing. Such measures should facilitate the detection of instances where required message fields are completed but the information is unclear, or where there is meaningless data in message fields. The Guideline cites a few examples of reasonable measures that could be taken.

Criteria 16.14 and 16.15—There are no specific obligations on beneficiary FIs involved in cross-border EFTs.

Money or Value Transfer Service Operators

Criterion 16.16—All obligations identified in CC, ss.16.1–16.9 above apply to MSBs and their agents.

Criterion 16.17—There are no specific legal requirements for MTVS providers either to review ordering and beneficiary information to decide whether to file an STR or to ensure that an STR is filed in any country affected and transaction information made available to the FIU.

Implementation of Targeted Financial Sanctions

Criterion 16.18—See the assessment of R.6 and R.7. The processing of EFTs, in terms of FIs taking freezing action and complying with prohibitions from conducting transactions with designated persons and entities, is adequately covered in law.

Weighting and Conclusion

The legal obligations applicable to ordering FIs and MSBs are broadly satisfactory, but there remain some weaknesses. **Canada is partially compliant (PS) with R.16.**

Recommendation 17—Reliance on Third Parties

In the 2008 MER, Canada was rated NC with R.9. In the only two scenarios where reliance on a third party or introduced business was legally allowed without an agreement or arrangement, the measures in place were insufficient to meet the FATF standard. In addition to the two reliance on third parties/introduced business scenarios contemplated by the Regulations, the financial sector

used introduced business mechanisms as a business practice. However, no specific requirements, as set out in R.9, applied to these scenarios. Only minor changes have subsequently been introduced.

Criterion 17.1—The PCMLTFR (ss.64(1)(b)(A)(I) and (II)) allow FIs, other than MSBs, and also foreign entities that conduct similar activities, to rely on affiliated third parties, or those in the same association, for the purpose of ascertaining the identity of a person.

More specific legal provisions apply to both the life insurance industry and securities dealers. A life insurance company, broker, or agent is not required to ascertain the identity of a person where that person's identity has previously been ascertained by another life insurance company, broker, or agent in connection with the same transaction or series of transactions that includes the original transaction. Similarly, a securities dealer, when opening an account for the sale of mutual funds, is not required to ascertain identity where another securities dealer has already done so in respect of the sale of mutual funds for which the account has been opened. The PCMLTFR (s.56(2) and s.62(1)(b)) refer.

Apart from the specific situations set out above, all requirements under the PCMLTFR continue to apply to the FI that has the relationship with the customer.

The PCMLTFR (s.64.1) state that, when REs use an agent or a mandatary to meet their client identification obligations, they must enter into a written agreement or arrangement with the agent or mandatary. In addition, the RE must obtain from the agent or mandatary the customer information that was obtained under the agreement or arrangement. The agent or mandatary can be any individual or entity, provided these two conditions regarding written agreement and obtaining customer information are met. Where the client is not physically present at the opening of an account, establishment of a trust or conducting of a transaction, the agent or mandatary has the same two options, outlined in ss.64(1) and 64(1.1), that an RE does when dealing with a client who is not physically present.

In the first option, the agent or mandatary must obtain the individual's name, address, and date of birth. Then, they must confirm that one of the following has ascertained the identity of the individual by referring to an original identification document:

- a financial entity, life insurance company, or securities dealer affiliated with them;
- an entity affiliated with them and whose activities outside Canada are similar to those of a financial entity, life insurance company, or securities dealer; or
- another financial entity that is a member of their financial services cooperative association or credit union central association of which they also are a member.

To use this option, the agent or mandatary must verify that the individual's name, address and date of birth correspond with the information kept in the records of that other entity. The second option requires the use of a combination of two of the identification methods set out in Part A of Schedule 7 of the PCMLTFR.

Where agents or mandataries with written agreements are concerned, the relying entity must obtain customer information supplied under the agreement. However, life insurance companies/brokers/agents or securities dealers are not required to obtain from the relied-upon institution the necessary CDD information.

Similarly, life insurance companies/brokers/agents or securities dealers are not required to satisfy themselves that copies of CDD information will be made available to them by the third party on request without delay.

There is no explicit obligation, either for relying entities with agents and mandataries or for life insurance companies/brokers/agents or securities dealers, to satisfy themselves that the FI relied on is regulated and supervised or monitored for compliance with CDD and record-keeping obligations in line with R.10 and R.11.

Criterion 17.2—The PCMLTFA and PCMLTFR do not require life insurance companies/brokers/agents or securities dealers to assess which countries are high risk for third party reliance. The authorities state that reliance may only be placed on life insurance companies/brokers/agents or on securities dealers that are subject to the PCLMTFA, and FINTRAC's oversight. If so, the scenario outlined in Criterion 17.2 would not arise.

While ss.56(2) and 62(1) (b) of the PCMLTFR do not actually preclude the possibility of reliance being placed on third parties outside Canada, with no account taken of the level of country risk, an RE can only rely on third parties outside Canada if they are affiliated with them. Canada issued regulatory amendments for public comment in July 2015 that included an amendment with respect to Group-Wide Compliance Programs that would require REs to take into consideration as part of their compliance programs the risks resulting from the activities of their affiliates.

Criterion 17.3—The PCMLTFR (ss.64(1)(b)(A)(I) and (II)) allow FIs, other than MSBs, and also foreign entities that conduct similar activities to rely on affiliated third parties, or those in the same association, for the purpose of ascertaining the identity of a person. PCMLTFA, ss9.7 and 9.8 require foreign branches and subsidiaries, subject to there being no conflict with local laws, to develop and apply policies to keep records, verify identity, have a compliance program, and exchange information for the purpose of detecting or deterring an ML or TF offense or of assessing the risk of such an offense. Thus, group-wide ML/TF standards should apply, providing appropriate safeguards.

Where there is a conflict with, or prohibition by, local laws, the RE must keep a record of that fact, with reasons, and notify both FINTRAC and its principal federal or provincial regulator within a reasonable time (PCMLTFA, s.9.7(4)).

Weighting and Conclusion

A number of deficiencies remain, even though that reliance on third parties appears to be of limited practical application. **Canada is partially compliant (PC) with R.17.**

Recommendation 18—Internal Controls and Foreign Branches and Subsidiaries

In the 2008 MER, Canada was rated LC with R.15 due to minor deficiencies and NC with R.22 due to the lack of legal obligation to ensure that foreign branches and subsidiaries applied AML/CFT measures consistent with home country standards, and obligation to pay particular attention to branches and subsidiaries in countries, which did not, or insufficiently, applied the FATF Recommendations. The current FATF standards are broadly unchanged, although R.18 specifies in more detail what should be done to manage ML/TF risk where host country requirements are less strict than those of the home country. Significant changes came into force in Canada in June 2015.

Criterion 18.1—PCMLTFA s.9.6 requires FIs to establish and implement a compliance program to ensure compliance with the Act. The program must include the development and application of policies and procedures for the FI to assess, in the course of their activities, the risk of an ML or TF offense. The PCMLTFR (ss.71(1)(a) and (b)) specify that: a person must be appointed to be responsible for implementation of the program; and the program must include developing and applying written compliance policies and procedures that are kept up-to-date and approved by a senior officer.

OSFI Guideline B-8 stipulates that FRFIs must have a Chief Anti-Money Laundering officer (CAMLO) responsible for implementation of the enterprise AML/ATF program, who should be one person positioned centrally at an appropriate senior corporate level of the FRFI. Separately, OSFI Guideline E-13 requires that FRFIs must have a Chief Compliance officer with a clearly defined and documented mandate, unfettered access and, for functional purposes, a direct reporting line to the Board.

Neither the PCMLTFA nor PCMLTFR contain any specific obligations regarding FIs' screening procedures when hiring employees. Similarly, there are no measures in place in sector legislation at the federal or provincial level. OSFI Guideline E-17 details OSFI's expectations in respect of screening new directors and senior officers of FRFIs at the time of hiring. However, this applies only to a defined set of "Responsible Persons," not to all employees.

The PCMLTFR (s.71(1)(d)) require REs that have employees, agents or other persons authorized to act on their behalf to develop and maintain a written ongoing training program for those individuals. In addition, OSFI Guideline B-8 advises FRFIs to ensure that written AML/ATF training programs are developed and maintained. Appropriate training should be considered for the Board, Senior Management, employees, agents and any other persons who may be responsible for control activity, outcomes or oversight, or who are authorized to act on the Company's behalf, pursuant to the PCMLTFR.

The PCMLTFR (s.71(1)(e)) oblige all REs to institute and document a review of their policies and procedures, the risk assessment and the training program for the purpose of testing effectiveness. That review must be carried out every two years by an internal or external auditor of the RE, or by the RE itself, if it has no auditor. OSFI Guideline B-8 amplifies the requirement in a number of ways and also sets out an expected standard of self-assessment of controls applicable to FRFIs.

Criterion 18.2—Measures which came into effect in June 2015 expanded section 9.7 of the PCMLTFA to cover foreign branches as well as subsidiaries. The effect was to require FIs, securities dealers, and life insurance companies to implement policies and procedures for CDD, record-keeping and compliance programs that are consistent with Canadian requirements and apply across a financial group.

A new s.9.8(1) of the Act introduced requirements for REs to have policies and procedures in place for how they will share information with affiliates for the purpose of detecting or deterring an ML or TF offense or of assessing the risk of such an offense. This provision is sufficiently widely drawn to cover the kind of customer, account, and transaction information stipulated in the FATF standard. There are no prohibitions in either the PCMLTFA or PIPEDA on sharing of information, including STRs, within financial groups, domestically or cross-border.

The new law did not cover safeguards on the confidentiality and use of information exchanged. However, the necessary safeguards already exist under PIPEDA (s.5 and Schedule 1), which apply equally to client information received from a branch or subsidiary under the PCMLTFA.

Criterion 18.3—Under newly amended s.9.7(4) of the PCMLTFA, when local laws would prohibit a foreign branch or foreign subsidiary from implementing policies that are consistent with Canadian AML/ATF requirements, the RE must advise FINTRAC and their principal regulator. (In the case of FRFIs, this is OSFI; for provincially regulated FIs, the relevant provincial supervisor).

Weighting and Conclusion

There is a remaining deficiency regarding the internal controls aspect of R.18. **Canada is largely compliant (LC) with R.18.**

Recommendation 19—Higher-Risk Countries

In the 2008 MER, Canada was rated PC with R.21, because there were no general enforceable requirements for FIs to give special attention to transactions or business relationships connected with persons from higher-risk countries, no measures advising of other countries with AML/CFT weaknesses, and no requirement to examine the background and purpose of transactions and to document findings. The FATF standard remains broadly the same, but there have been major changes in Canada since 2008.

Criterion 19.1 and 19.2—Part 1.1 of the PCMLTFA, which entered into force in June 2014, introduced two new authorities for the Minister of Finance: (i) the authority to issue directives requiring REs to apply necessary measures to safeguard the integrity of Canada's financial system in respect of transactions with designated foreign jurisdictions and entities. The measures contemplated included CDD, monitoring and reporting of any financial transaction to FINTRAC; (ii) the authority to recommend that the Governor-in-Council issue regulations limiting or prohibiting REs from entering into financial transactions with designated foreign jurisdictions and entities. These authorities enable Canada to take targeted, legally enforceable, graduated, and proportionate financial

countermeasures against jurisdictions or foreign entities with insufficient or ineffective AML/ATF controls. These measures can be taken in response to a call by an international organization, such as the FATF, or unilaterally. The Minister has not issued any countermeasures under Part 1.1; however, OSFI and FINTRAC have regularly drawn the attention of FRFIs and REs to the FATF calls on members, and have issued regular guidance in Notices and Advisories following each FATF meeting. OSFI has issued prudential supervisory measures against FRFIs it believes have not implemented FATF expectations (PCMLTA (s.11.42) and PCMLTFR (s.71.1)).

Criterion 19.3—Risk assessments on jurisdictions with AML/ATF weaknesses are conducted through the IFAC Under s.11.42(3) of the Act, the Minister's decision to issue a Directive may require the Director of FINTRAC to inform all REs. Additional guidance is provided through FINTRAC advisories and OSFI notices, available online, encouraging enhanced CDD with respect to clients and beneficiaries involved in transactions with high-risk jurisdictions.

Weighting and Conclusion

Canada is compliant (C) with R.19.

Recommendation 20—Reporting of Suspicious Transactions

In the 2008 MER, Canada was rated LC with R.13 and SR. IV because some FIs (e.g., financial leasing, factoring and finance companies) were not covered by the obligation to report and there was no requirement to report attempted transactions. Some improvements have been made since then.

Criterion 20.1—PCMLTFA, s.7 requires REs to report to FINTRAC every financial transaction that occurs, or that is attempted, in the course of their activities and in respect of which there are reasonable grounds to suspect that the transaction is related to the commission or attempted commission of an ML or TF offense. The scope of the PCMLTFA still excludes certain sectors (financial leasing, finance, and factoring companies), but this represents an ongoing minor deficiency. ML is defined by reference to CC, s.462.31(1), which, in turn, is defined in CC, s.462.31(1) to mean any offense that may be prosecuted as an indictable offense under this or any other Act of Parliament, other than an indictable offense prescribed by regulation. As described under c.3.2, ML now applies to a range of offenses in each FATF designated category of predicate offenses, including tax evasion.

Suspicious transactions must be reported "within 30 days" of detection of a fact that constitutes reasonable grounds to suspect that the transaction or attempted transaction is related to the commission of an ML offense or a TF offense. (PCMLTF Suspicious Transaction Reporting Regulations, s.9(2)). This does not meet the standard of reporting "promptly."

Criterion 20.2—Attempted transactions are now covered by the reporting requirement.

Weighting and Conclusion

The reporting requirement covers several, but not all elements, of the standard. **Canada is partially compliant (PC) with R.20.**

Recommendation 21—Tipping Off and Confidentiality

In the 2008 MER, Canada was rated C with R.14.

Criterion 21.1—The PCMLTFA s.10 states that no criminal or civil proceedings lie against a person or an entity for making an STR in good faith or for providing FINTRAC with information about suspicions of ML or TF activities. However, the requirement does not explicitly extend to reporting related to ML predicate offenses.

Criterion 21.2—The PCMLTFA s.8 specifies that no person or entity can disclose that they have made an STR, or disclose the contents of a report, with the intent to prejudice a criminal investigation, whether or not a criminal investigation has begun. The law does not, however, cover a situation where a person or entity is in the process of filing an STR but has not yet done so. Neither does the legal obligation explicitly extend to reporting related to ML predicate offenses.

Weighting and Conclusion

The tipping-off and confidentiality requirements do not explicitly extend to the reporting of suspicions related to ML predicate offenses. **Canada is largely compliant (LC) with R.21.**

Designated Non-Financial Businesses and Professions (DNFBPs)

Since the 2008 MER, Canada has extended the AML/CFT requirements to BC Notaries and DPMS. The following DNFBPs are now subject to AML/CFT obligations: land-based casinos, accountants (defined as chartered accountant, certified general accountant, certified management accountant)[16] and accounting firms, British Columbia Notaries Public and Notary Corporations (hereinafter referred to as BC Notaries), real estate brokers or sales representatives, dealers in precious metals and stones (hereinafter DPMS) and certain trust companies, which fall under PCMLTFA, s.5 (e). Legal counsel and legal firms are covered as obliged AML/CFT entities, pursuant to PCMLTR, s.33.3, but, on February 13, 2015,[17] the Supreme Court of Canada concluded that the AML/CFT provisions are inoperative, as they are unconstitutional, for lawyers and law firms in Canada. Canada extended the AML/CFT regime to real estate developers when, under certain conditions, they sell to the public real estate (PCMLTFR, s.39.5). Notaries in provinces other than Québec and British Columbia are

[16] PCMLTFR, Section 1. (2).

[17] The Supreme Court of Canada on February 13, 2015 has concluded that the search provisions of the Act infringe Section 8 of the Canadian Charter of Rights and Freedoms, while the information gathering and retention provisions, in combination with the search provisions, infringe Section 7 of the Charter Canada (Attorney General) v. Federation of Law Societies of Canada, 2015 SCC 7.

restricted to certifying affidavits under oath, and document certification. These notaries do not conduct any financial transactions, and the transfer of property is done exclusively through lawyers in these provinces (see 2008 MER, para. 150). TCSPs are not a distinct category under the PCMLTFA and PCMLTFR. The definition of casino (PCMLTFR, s.1(1)), which excludes registered charities authorized to perform business temporarily, provides an unclear exemption.[18]

All gambling is illegal,[19] unless specifically exempted under CC, s.207. Several provinces (British Columbia, Quebec, Manitoba Nova Scotia, Prince Edward Island, New Brunswick, and Newfoundland) have introduced online gambling through an extensive interpretation of the notion of "lottery scheme" allowed to them under CC, s.207(4)(c), which includes games operated through a computer. When these provinces introduced internet gambling, FINTRAC sent them a letter to inform them that they were considered subject to AML/CFT obligations. Subsequently, these casinos started sending to FINTRAC Casino Disbursement Reports (for example, FINTRAC has received 988 such reports in the last 24 months). Nevertheless, the amendment to the definition of casinos that makes reference to online gambling operators is not yet entered into force.[20]

There are also land-based gaming and online gambling[21] sites actually operating within Quebec, whose legal status is unclear, which are not supervised by the province and which are not subject to AML/CFT obligations. These activities are authorized by the Kahnawake Gaming Commission operating on the basis of an asserted jurisdiction by the Mohawks over their territory. They are considered illegal by the authorities. Offshore gambling sites are deemed to be illegal as each casino must be licensed by a Canadian province. The authorities clarified that these activities are a matter for law enforcement to oversee.

Cruise ships that offer gambling facilities in Canadian waters are not obliged entities for AML/CFT purposes (see 2008 MER, para. 1186–1187). Lottery schemes cannot be operated within five nautical

[18] There is no definition of "charitable purposes" and the notion of "temporary" business, does not give an exact timeframe, making unclear the reference to "not more than two consecutive days at a time," without fixing any further limit per week or per year. The exemption involving registered charities is to avoid duplication in the AML/CFT regime, as the Provincial Authority or its designate are RE of FINTRAC. Nevertheless, taking into account the possible operational models of casinos operating in Canada, the current definition of casino and the resulting AML/CFT requirements lack clarity in addressing the respective AML/CFT responsibilities of the different persons or entities that could be simultaneously involved in the business of the same casino (Crown corporations or regulators branches involved in the conduct and management of lotteries schemes, charitable organizations, First Nation organizations, casino's service providers).

[19] CC, Section 206 (1).

[20] Steps are being taken in this respect. Bill C-31 introduced legislative amendments to PCMLTFA s.5 k 1, which will come into force once the regulations are finalized, aimed at establishing AML/CFT obligations for online gambling conducted and managed by the provinces and covering those lottery schemes other than bingo and the sale of lottery tickets that are conducted and managed by provinces in accordance with CC, s.207(1)(a). These amendments will also extend the notion of relevant business to include other electronic devices similar to slot machines (such as video lottery terminals, currently excluded from the AML/CFT regime) but establishing a relevant threshold of "more than 50 machines per establishment" (PCMLTFA, s.5(k)(ii)).

[21] Online gaming operators that are licensed by the Commission must be hosted at Mohawk Internet Technologies, a data center, located within the Mohawk Territory of Kahnawake.

miles of a Canadian port at which the ship calls (s.207.1 of the CC). Of note, there are no Canadian cruise ships. The exemption of cruise ship casinos is based on a proven low risk.

Trust and company services are provided by trust companies, legal counsels, legal firms, and accountants—the PCMLTFA, therefore, does not identify TCSPs separately. Twenty-two trust companies (covered by a provincial Act, falling under of PCMLTFA, s.5(e)) are subject to AML/CFT obligations, but lawyers and accountants are not, despite the high vulnerability rating highlighted in the NRA.[22]

Recommendation 22—DNFBPs: Customer Due Diligence

In the 2008 MER, Canada was rated NC with these requirements due to deficiencies in the scope of DNFBPs covered and in CDD and record-keeping requirements. Since then, Canada has extended the scope of the AML/CFT requirements to BC Notaries and DPMS and addressed some deficiencies in CDD requirements applicable to DNFBPs.[23]

Criterion 22.1—Scope issue: Internet casinos, TCSPs are not covered and the relevant provisions are inoperative with respect to legal counsels, legal firms and Quebec notaries (PCMLTFR, ss.33.3, 33.4, 33.5, 59.4, 59.41, 59.4). As regards accountants and BC notaries, not all the relevant activities under the criterion are taken into account.

DNFBPs[24] are not required to obtain, take reasonable measures to confirm, and keep records of the information about the beneficial ownership of legal persons and legal arrangements, nor as to understand the ownership and control structure of the latter. DNFBPs are only required to confirm the existence of and ascertain the name and address of every corporation or other entity on whose behalf a transaction is being undertaken, and in the case of a corporation, the names of its directors.[25] The rule of "third party determination" (PCMLTFR, s.8) is limited to individuals and is not applied to all relevant circumstances when CDD is required under the criterion. DNFBPs are not explicitly required to establish that the person purporting to act on behalf of the customer is so authorized. There are additional deficiencies for each relevant category. Casinos can perform a large variety of financial services, including wire transfers (see 2008 MER, para. 138). The following measures for ascertaining identity are carried out in line with the following threshold: on account opening (no threshold), when dealing with EFTs (Can$1,000) and, dealing with foreign exchange or extension of credit (Can$3,000).[26] The Can$10,000 thresholds for ascertaining identity for cash

[22] NRA, p.32.

[23] In particular, introducing the obligation to collect information on the purpose and intended nature of the business relationship and ongoing due diligence, extending the circumstances in which CDD is required, providing for enhanced measures in higher-risk scenarios, excluding the exemption regime in case of suspicion.

[24] With the exception of legal counsel and legal firms for which, however, the provisions are inoperative (Section 11.1 (1) of the PCMLTFR.

[25] PMCLTFR 59.1(b) & (c), 59.2(1)(b) &(c), 59.3 (b) & (c), 59.5 (b) & (c), 60 (e) &(f).

[26] PCMLTFR, Sections 60(a), 60(b)(iv), 60(b)(iii), 60(b)(ii).

financial transactions and casinos disbursement[27] are higher than the FATF standard. Not all the range of non-cash occasional transactions are covered: in particular, the purchase of chips through checks, credit, and debit cards, as well as prepaid cards are not captured. The redemption of "tickets" under PCMLTFR, s.42(1)(a) is not included, even if some kind of tickets (TITO tickets)[28] have been detected by FINTRAC in typologies of ML. There are no enforceable provisions requiring casinos to include beneficiary information in wire transfers, and no obligation for all REs to ascertain the identity of authorized signers (PCMLTFR, ss.54(1)(a) and 62(1)(a)). As regards, accountants and BC Notaries, not all the relevant activities under the criterion are included. In particular, no requirement is provided in relation to activities related to organization of contributions for the creation, operation, and management of companies, legal persons and arrangements, and the scope of "purchasing or selling" securities, properties and assets is more limited than the notion of "management" included under the criterion. The definition of accountant (PCMLTFR, s.1(1) does not include "Chartered Professional Accountant."[29] In a real estate transaction, when the purchaser and the vendor are represented by a different real estate broker, each party to the transaction is identified by their own real estate broker. Real estate agents, in case of unrepresented party are required to take reasonable measures only to ascertain the identity of the party (PCMLTFR, s.59.2 (2, 3, and 4)), rather than applying reasonable risk-based CDD measures to the party that is not their client. DPMS are covered as required by the standards when they engage in the purchase or sale of precious metals, precious stones or jewelry in an amount of Can$10,000 or more in a single transaction, other than those pertaining to manufacturing jewelry, extracting precious metals, or precious stones from a mine, or cutting or polishing precious stones.

Criterion 22.2—Scope issue: see 22.1. The circumstances under which relevant DNFBPs have to keep records do not fully match the list of activities required under R.10 (see 22.1). Furthermore, a non-account business relationship is established when transactions are performed in respect of which obliged entities are required to ascertain the identity of the person, rather than being based on a mere element of duration. The said definition entails that, apart from the case of suspicion, the record-keeping requirements on a business relationship arise only when the prescribed thresholds for the transactions are reached. The deficiencies identified in R.11 apply also to DNFBPs.

Criteria 22.3, 22.4 and 22.5—There are no requirements for DNFBPs to comply with specific provisions covering PEPs, new technologies, and reliance on third parties.

[27] PCMLTFR, Sections 53 and 60(b)(i).

[28] Ticket in Ticket Out (TITO) "tickets" are also an increasingly popular casino value instrument used in many. Canadian casinos (FINTRAC, ML Typologies and Trends in Canadian Casino, Nov. 2009, p.8).

[29] The unified new professional designation replaces the former three (Chartered Accountants, Certified General Accountants, and Certified Management Accountants), and it is currently completed in several provinces (Quebec, New Brunswick, Saskatchewan, Newfoundland, and Labrador). Further work is underway and expected to be included in forthcoming regulatory amendments.

Weighting and Conclusion

Canada is non-compliant (NC) with R.22.

Recommendation 23—DNFBPs: Other Measures

In its 2008 MER, Canada was rated NC with these requirements due to the limited scope of DNFBPs included, as well as to deficiencies with the underlying recommendations and to concern about the effectiveness of the STR regime in these sectors. Canada has since extended the scope of DNFBPs to some extent (see R.22), included attempted transactions in the STR regime and empowered the Department of Finance to take financial countermeasures with respect to higher-risk countries.

Criterion 23.1—PCMLTFA, s.7 (transaction where reasonable grounds to suspect) does not apply to all relevant categories of DNFBPs, nor to all relevant activities of accountants and BC Notaries as described under R.22.[30] The analysis in relation to R.20 above equally applies to reporting DNFPBs. There are no key substantive differences between the reporting regime for FIs and DNFBPs. FINTRAC Guidelines no. 2 (Suspicious Transactions) includes industry-specific indicators.

Criterion 23.2—Scope issue: see 23.1. Accountants, accounting firms, legal counsels and legal firms, BC Notaries, real estate agents and developers, land-based casinos, DPMS are all required to establish and implement a compliance program (PCMLTFA, s.9.6 (1); PCMLTFR, s.71(1)). While compliance procedures must be approved by a senior officer, PCMLTFA, ss.9.6 and PCMLTFR, s.71(1)(a) do not stipulate that the designation of the compliance officer shall be at the management level. DNFBPs, other than land-based casinos, are not required to have adequate screening procedures to ensure high standards when hiring employees. Also, there is no specific requirement that review of the compliance regime be performed by an independent audit function, as it can also be carried out through a procedure of self-assessment (PCMLTFR, s.71(1)(e)).

Criterion 23.3—Scope issue: see 23.1. See R.19 for a description of this requirement.

Criterion 23.4—Scope issue: see 23.1. The requirements for DNFBPs are the same as those applied to FIs under R.21.

Weighting and Conclusion

Canada is non-compliant (NC) with R.23.

Recommendation 24—Transparency and Beneficial Ownership of Legal Persons

Canada was rated NC with former R.33 based on concerns over a lack of transparency for legal entities, the availability of bearer shares without adequate safeguards against misuse, and a lack of powers by the authorities to ensure the existence of adequate, accurate, and timely beneficial

[30] Under PCMLTA, Section 5, Part 1 of the Act (including the STRs obligations) applies while carrying out the activities described under the regulations.

ownership information for legal entities. Since 2008, the obligations for FIs to obtain information on the identity of beneficial owners and the CRA's ability to disseminate information on legal entities to the RCMP have been strengthened.

Canada's corporate legal framework consists of federal, provincial, and territorial laws: (i) Legal entities may be established at the federal level under the Canada Business Corporation Act (CBCA); the Canada Not-for-Profit Corporations Act (NFP Act), or the Canada Cooperatives Act (CCA). Federally incorporated entities are entitled to operate throughout Canada but in addition to registration at the federal level, are also subject to registration with the province or territory in which they carry out business. (ii) Each of the thirteen territories and provinces regulates the types of legal entities that can be established at the local level. Eight provinces and territories have enacted specific laws that provide for the establishment of corporations and NPOs. Prince Edward Island, Newfoundland and Labrador, Alberta, Manitoba, Quebec, and New Brunswick do not have specific NPO legislation in place but regulate NPOs through the relevant provincial company law.

Legal entities incorporated at the provincial or territorial level enjoy business name protection only in the province or territory where they are incorporated. To operate in another province in Canada, they have to register with that province, but there is no guarantee that they will be able to use their corporate name (e.g., a business entity with the same name may already be operating in that province). Federal, provincial, and territorial corporate entities may carry out business internationally if the foreign country recognizes the type of corporate entity.

In addition to legal entities, all provinces provide for the establishment of general and limited partnerships pursuant to common law rules; and all provinces, but Yukon, Prince Edward Island and Nunavut, have passed statutes to provide for the establishment of limited liability partnerships. Partnerships are not subject to registration as part of the establishment process, but most provinces and territories require registration of businesses before a partnership may operate there. Business registration obligations under provincial and territorial laws also apply to foreign entities wishing to carry out business in Canada.

Criterion 24.1—Federal legal persons: Innovation, Science and Economic Development Canada (ISED), formerly Industry Canada, provides a comprehensive overview and comparison on its internet homepage of the various legal entities available and their forms and basic features. All legal entities established at the federal level are subject to registration. Given that corporations are by far the most utilized type of legal entity in Canada, particular emphasis is put on information pertaining to federal corporations under CBCA and their incorporation and registration process, which can be initiated online or by sending all required documents to the competent registrar via email, fax, or mail. [31] ISED also offers a search tool, which makes some basic information of federal companies publicly available. The search function also indicates the legislation the corporation is incorporated under, which in turn clarifies basic regulating powers. *Provincial legal persons*: Similar information and services are provided through the homepages of all provincial governments except that of New

[31] See www.ic.gc.ca/eic/site/cd-dgc.nsf/eng/cs04843.html#articles.

Brunswick. The relevant web links are easy to find through ISED's homepage and provide public access to the relevant provincial laws that describe the various legal entities available; the name and contact information for the relevant authority competent for registration; and the procedures to be followed to establish a legal entity or to register a corporation. *Partnerships and foreign entities*: Partnerships and foreign entities operating in any of Canada's provinces or territories are subject to registration at the provincial level. The Canada Business Network maintains a homepage that provides links to the various provincial and territorial business registries.

Criterion 24.2—The NRA identified privately held corporations as being highly vulnerable to misuse for ML/TF purposes. The conclusion was reached based on the understanding that such corporations can easily be established and be used to conceal beneficial ownership. The risk assessment determines the inherent risks involved with legal persons based on factors such as the products and services offered by legal entities, the types of persons that may establish or control a legal person, the possible geographic reach of a Canadian legal entity, and taking into account FINTRAC statistics on typologies involving legal entities in Canada.

Basic Information

Criterion 24.3—Both federal and provincial corporations, NPOs with legal personality and cooperatives are established through incorporation by the relevant incorporating department or agency. *Federal legal persons*: On the federal level, ISED, as part of the incorporation and annual filing process, collects and publishes information comprising the corporation's name, type, status, corporation number, registered office address in Canada, name and address of all directors, and governing legislation. The regulating powers for federal corporations are set out in the legislation or in the corporation's articles, which are approved by the Director appointed under the relevant Act. *Provincial legal persons*: Company information including the corporate name, type, status, registered office in Canada, and name and address of directors is collected through the same process as on the federal level, which is through annual filing procedures. *Partnerships and foreign entities*: Business registration requirements vary between the different provinces and territories, but usually require the provision of the name, registered office, mailing address, place of business in the province/territory, the date and jurisdiction of incorporation (for extraterritorial companies) or type of partnership, the name and address of directors or partners and a copy of the partnership contract or the incorporation certificate or other proof of existence. Partnerships not carrying out any business in Canada are not required to register as part of the establishment process.

Criterion 24.4—Record-keeping obligations extend to the corporation's articles and by-laws and any amendments thereof, of minutes of shareholder meetings and resolutions, share registers, accounting records, and minutes of director meetings and resolutions. Pursuant to CBCA, s.50, companies must also keep a share register that indicates the names and address of each shareholder, the number and class of shares held, as well as the date and particulars of issuance and transfer for each share. Similar provisions are set out in provincial legislation. Federal as well as provincial companies are required to keep records of basic information either in a location in Canada or at a place outside Canada, provided the records are available for inspection by means of computer technology at the registered office or another place in Canada and the corporation

provides the technical assistance needed to inspect such records (CBCA, s.20). There is no legal requirement to inform the incorporating department or agency, or where applicable, the company register of the location at which such records are being kept.

Criterion 24.5—Under CBCA, s.19 (4) federal corporations are required to inform the Director appointed under the CBCA within 15 days of any change of address of the registered office. Changes in legal form, name, or status as well as amendments to the articles of incorporation take effect only after they have been filed with the Director. More or less the same updating requirements are especially provided for under provincial legislation, except in Quebec and Nova Scotia.[32] In Nova Scotia, the updating requirement applies, but changes to the registered office have to be filed within 28 days and there is only a general obligation to notify the Registrar "from time to time" of any changes among its directors, officers, or managers. Directors, shareholders, and creditors have access to these documents and are permitted at all times to check their accuracy. However, no formal mechanism is in place to ensure that shareholder registers are accurate. For partnerships and extraterritorial corporations, some provinces and territories impose an annual filing obligation, others require renewal of the license and updating of relevant information on a multi-year basis.

Beneficial Ownership Information

Criterion 24.6—Canada uses existing information to determine a legal entity's beneficial ownership, if and as needed, including as follows:

i. FIs providing financial services to legal entities, partnerships or foreign companies. Since 2014, obligations under the PCMLTFA for FIs to obtain ownership information of customers or beneficiaries that are legal entities have been strengthened. Prior to 2014, FIs identified beneficial owners of legal entities mostly based on a declaration of the customer. For those companies established prior to 2014, it is, thus, questionable whether this measure did indeed result in the availability of accurate and updated beneficial ownership information. Ongoing CDD obligation under the PCMLTFA have resulted in BO information becoming available for a number of companies that opened bank accounts in Canada prior to 2014, but most FIs interviewed by the assessors indicated that the ongoing CDD process has not yet been completed for all legal entities. For some DNFBPs as outlined in R.22, certain limited CDD obligations apply as discussed under R.22 but those do not amount to a comprehensive requirement to identify and take reasonable measures to verify beneficial ownership information and the obligations also are inoperative with regards to lawyers.

ii. The federal and provincial company registries record some basic information as discussed above, but do not generally collect information on beneficial owners. Verification mechanisms for registered information are not in place. The CRA, as part of its general obligations, collects information on legal entities that file tax returns. As indicated in the

[32] For example, Section 2 Ontario Corporations Information Act; Article 20 Alberta Business Corporation Act; Article 19 Nova Scotia Companies Act.

2008 MER, however, this information generally does not comprise beneficial ownership information. Furthermore, not all legal entities in Canada file tax returns with the CRA; and

iii. Legal entities themselves are required to collect certain information on holders of shares but no mechanisms are in place to ensure that the registered information is accurate.

iv. For public companies listed on the stock exchange, disclosure requirements exist for shareholders with direct or indirect control over more than 10 percent of the company's voting rights.

As outlined under R.9 and 31, LEAs have adequate powers to obtain information from FIs, DNFBPs, and any other types of companies and the CRA. However, the process of linking a specific FI with a legal entity or partnership subject to the investigation and accessing beneficial ownership information may not be timely in all cases. In sum, while some of the information collection mechanisms have been strengthened since 2008, deficiencies with regards to the collection and availability of full and updated beneficial ownership information remain and timely access by law enforcement authorities to such information is not guaranteed in all cases.

Criterion 24.7—As indicated under criterion 24.6, FIs are required to collect and update beneficial ownership information. The registries, the CRA, and legal entities themselves are not required to ensure that accurate and updated beneficial ownership information is collected.

Criterion 24. 8—Companies on both federal and provincial levels are obliged to grant the Director under the relevant Act access to certain information, including in relation to company share registers (Article 21 CBCA). There is no legal obligation on corporations or partnerships to authorize one or more natural person resident in Canada to provide to competent authorities all basic information and available beneficial ownership information; or for authorizing a DNFBP in Canada to provide such information to the authorities.

Criterion 24.9—Legal entities are required to maintain accounting records for six years, but not from the date of dissolution, but of the financial year to which they relate. In addition, pursuant to s.69 of the PCMLFTR FIs/some DNFBPs holding information on legal entities must keep that information for five years from termination of the business relationship or completion of the transaction. The Director retains corporate records submitted under the CBCA for a period of six years, except for articles and certificates which are kept indefinitely. In addition, s.225 of the CBCA requires a person who has been granted custody of the documents or records of a dissolved corporation to produce those records for six years following the date of its dissolution or such shorter period as ordered by a court. Non-financial documents or records must be kept by the corporation until the corporation is dissolved; and then for another six years or less period as ordered by a court. The CRA, in partnership with the National Archivist of Canada, retains documents obtained or created by the CRA for various periods of time depending on the nature of the information. In relation to questions of beneficial ownership, the relevant retention periods are five to ten years, in some instances indefinitely.

Other Requirements

Criterion 24.10—Some basic company information is publicly available on various federal and provincial government websites and is therefore available to the authorities in a timely fashion. For information that is not publicly available, a wide range of law enforcement powers are available to obtain beneficial ownership information, including search warrants, using informants, surveillance techniques, wiretaps and production orders, and public sources (e.g., law enforcement databases, city databases, corporate companies, civil proceedings, bankruptcy records, divorce records, civil judgments, land titles and purchase, building permits, credit bureau, insurance companies, liquor and gambling licenses, death records, inheritance, shipping registers, federal aviation, trash searches, automobile dealerships) and private source information searches. To be able to compel an FI to produce records pertaining to the control or ownership structure of a legal entity or legal arrangement, LEAs must first establish the link between a legal entity and a specific FI. Several tools are available to this effect (e.g., grid search request to all D-SIBs to establish if they count the target person amongst their customers, VIRs to FINTRAC, requests to Equifax, mortgage and loan checks, consultations of NEPS to obtain an economic profile of an individual or private or public company). Investigative techniques may also be used (e.g., informants, witnesses, wiretaps). The RCMP may also request information from the CRA once charges have been laid in a criminal case, and on the basis of a judicial authorization. Prior to the prosecution stage, a tax order under the CC can be obtained for the RCMP to receive tax information from the CRA on a specific entity. Since 2014, the CRA may also share information with the RCMP on its own motion in cases where the CRA considers that there are reasonable grounds to believe that the information in its possession would provide evidence of listed serious offenses, including ML, bribery, drug trafficking, and TF. In relation to tax crimes, the CRA CID may also obtain information. The relevant Director under each corporate statute—in the case of the CBCA the Director of Corporations Canada—also has the authority to inspect a corporation's records. Once it is established that a specific RE maintains a business relationship with a legal entity, LEAs may obtain a court order and deploy the measures available under criminal procedures to obtain, compel the production of, or seize relevant information—including beneficial ownership information—from any person, as discussed under R.31.

Criterion 24.11—Bearer shares are permitted both under the CBCA and several provincial company laws (for companies limited by shares).[33] While the CBCA generally requires the issuance of shares to be in registered form, the CBCA also makes provision for the issuance of certain types of shares in bearer form. In the absence of an express prohibition, the CBCA, therefore, still leaves some room for the issuance of bearer shares and no safeguards are in place to ensure that such shares are not being misused for ML or TF purposes.

Criterion 24.12—The CBCA requires corporations to keep shareholder registers in relation to registered shares, whereby the term "holder" of a security is defined as "a person in possession of a security issued or endorsed to that person." Under Part XIII of the CBCA, the holder of a share is

[33] Quebec, Prince Edward Island, North-Western Territories, and Nunavut allow for the issuance of registered shares only.

permitted to vote at a meeting using someone else to represent them. The CBCA permits a registered shareholder to authorize another person to vote on their behalf. The proxy form itself lists the registered shareholder and the name of the "proxyholder" or person acting on their behalf. The proxy is recorded at the shareholder meeting, which provides transparency in respect of the identity of these individuals. However, the outlined arrangement still allows for nominee shareholding arrangements if the relevant shares are not voted. CBCA, s.147 permits, for example, securities brokers, FIs, trustees, or any nominees of such persons or entities to hold securities on behalf of another person who is not the registered holder but beneficial owner of that security. Similar provisions are found in provincial legislation such as, for example, Alberta Business Corporations Act, s.153 and Quebec's Business Corporations Act, s.2. Corporate directors are not permitted under the CBCA and provincial statutes. Nominee director arrangements in form of one natural person formally acting as director on behalf of another person may, however, still exist. Nominees (whether shareholders or directors) are not required to be licensed, or disclose their status, or to maintain information on or disclose the identity of their nominator. However, under the PCMLFTR, legal entities when opening a bank account, are required to provide details on the natural person that owns or controls a legal entity, which would include the nominating shareholder or director. For publicly listed companies, the risk of abuse of nominee shares is properly mitigated based on rigid reporting obligations for change of shares in excess of 10 percent. In sum, for companies other than those listed on the stock exchange, there are insufficient mechanisms in place to ensure that nominee shareholders are not misused for ML or TF purposes.

Criterion 24.13—Under the CBCA and provincial company laws violation of a company's disclosure, filing or record-keeping obligations may be fined with up to Can$5,000 and/or imprisonment for up to six months in case of a violation by a natural person acting on behalf of the company. FIs and those DNFBPs covered under the law are subject to criminal (imprisonment for up to six months and/or a fine of up to Can$50,000) as well as administrative sanctions if they fail to comply with their identification obligations with regards to legal entities (PCMLTFA, ss.73.1 and 74). In addition, officers, directors, and employees of FIs and DNFBPs may be subject to sanctions regardless of whether the FI or DNFBP itself was prosecuted or convicted, as discussed under R.35. In summary, the statutory sanctions available are proportionate and dissuasive.

Criterion 24.14—Some basic information in the federal and provincial company registers is publicly available and can be directly accessed by foreign authorities. For other information, the powers and mechanisms described under criteria 37.1 and 40.9, 40.11, and 40.17 to 40.19 apply.

Criterion 24.15—Information on the quality of assistance received from other countries in the context of MLA and in response to ownership information requests is kept by the International Assistance Group (IAG) at the Department of Justice. The IAG maintains a copy of the requests made, the follow-up that takes place with regards to each request, and keeps copies of all documents and information provided in response to the request. When forwarding the relevant information to the requesting agency, the IAG inquires with that agency, whether the request should be considered fulfilled. The authorities stated that the information collected by IAG suggests that

the assistance received is generally adequate, although the result vary according to the particular component of basic/beneficial ownership sought.

Weighting and Conclusion

Serious gaps remain under Criterion 6 with respect to the availability of beneficial ownership information for legal entities and partnerships. **Canada is partially compliant (PC) with R.24.**

Recommendation 25—Transparency and Beneficial Ownership of Legal Arrangements

Canada was rated PC with former R.34 as the obligations to obtain, verify, and retain beneficial ownership information was considered to be inadequate. Since then, changes have been introduced to the PCMLTFR to strengthen FI obligations with regards to the identification and verification of beneficial ownership information for legal arrangements (whether created in Canada or elsewhere). In addition, the CRA's power to disseminate tax information to LEAs have been enhanced, taxpayer information can be shared at the discretion of the CRA if the CRA has reasonable grounds to believe that the information will afford evidence of certain designated offenses, including ML under CC s. 462.31. However, it is not clear for how many of the millions of trusts estimated to exist under Canadian law beneficial ownership information is available and access to such information is in any case difficult to obtain as there is no requirement for trustees to be licensed or registered.

Canada allows for the establishment of common law trusts as well as civil law fiducie (in Quebec). There is no general registration requirement for trusts, and trustees may but do not have to be licensed individuals or entities under the PCMLTFA. No specific statutes regulate the operation of foreign trusts in Canada, or require the registration of such foreign trusts.

Criterion 25.1—In the case of professional trustees, the customer due-diligence obligations vary depending on the trustee's profession: TCSPs are not subject to the general identification and verification obligations under the PCMLTFA as outlined under R.22. The CDD obligations applied to accountants have limitations as discussed in R.22. The requirements for lawyers are inoperative as a result of a Supreme Court decision. Trustees other than professional trustees are not subject to any statutory customer due diligence or record-keeping obligations.

Criterion 25.2—TCSPs are not covered under the scope of the PCMLFTR. Accountants are subject to basic ongoing CDD measures that do not amount to a comprehensive obligation to obtain and take reasonable measure to verify the identity of beneficial owners. Other trustees are not subject to comprehensive CDD or record-keeping requirements, as indicated under criterion 1.

Criterion 25.3—There is no obligation on trustees to disclose their status without being prompted, but under the PCMLFTR, FIs are required to determine whether a customer is acting on behalf of someone else, to establish the control and ownership structure of legal entities they are providing services to, and to obtain the names and addresses of all trustees, known beneficiaries and settlors.

Criterion 25.4—There is no prohibition under Canadian law for trustees to provide trust-related information to competent authorities, except in the case of lawyers where legal privilege may prevent authorities from accessing such information.

Criterion 25.5—Where there are suspicions of a crime, LEAs may deploy a wide range of investigative measures to obtain, compel the production of, or seize relevant information from any trustee, whether subject to the PCMLFTR or not. The extent to which the information available would include beneficial ownership information and information on the trust assets is unclear, as apart from the PCMLFTR, no legal requirements to maintain such information exist. Furthermore, linking a specific FI or DNFBP with a legal entity or partnership subject to the investigation and accessing beneficial ownership information may not be timely in all cases. With regards to FIs and accountants and trust companies acting as trustees, LEAs may also obtain information available to FINTRAC in its capacity as FIU through a request for voluntary information records. FINTRACs powers to access such information are, however, limited as outlined under criterion 29.2. In situations where a trust owes taxes and is required to file income tax returns, the CRA also has access to certain trust information, including the name and type of the trust and certain financial information on the trust. Information available to the CRA typically includes beneficiary, but not beneficial ownership information. The CRA may share taxpayer information upon request by LEAs either based on a court order or after criminal charges have been laid; or upon its own initiative if the CRA has reasonable grounds to believe that the information will afford evidence of certain designated offenses, including ML under CC, s.462.31.

Criterion 25.6—The authorities may exchange information on trusts with foreign counterparts based on the procedures outlined under criteria 37.1 and 40.9, 40.11, and 40.17 to 40.19 and 11. LEAs have wide powers to exchange information with foreign counterpart. FINTRAC as well as the CRA may also share information with foreign counterparts as part of their respective functions. Investigative measures to obtain beneficial ownership can be taken upon foreign request.

Criterion 25.7—Under the PCMLFTR, failure to comply with the identification, verification or record-keeping requirements is subject to a range of criminal and administrative sanctions (see write-up under R.35 for more details). Trustees other than accountants are not subject to the AML/CFT framework. Violations of the principles of a trustees' breach of fiduciary duties may give rise to claims by the beneficiary and legal liability of the trustee based on these claims. However, in the absence of a specific obligation to collect and maintain beneficial ownership or general trust information there are also no sanctions available to authorities for a failure of the trustee to do so.

Criterion 25.8—For accountants, a the PCMLFTR sanctions may be applied by supervisory authorities as discussed under criterion 27.4. For other trustees, however, no sanctions are in place in the case of a failure to grant competent authorities timely access to trust related information.

Weighting and Conclusion

Canada is non-compliant (NC) with R.25.

Recommendation 26—Regulation and Supervision of Financial Institutions

In the 2008 MER, Canada was rated PC with former R.23 due to the exclusion from the AML/CFT regime of certain sectors without proper risk assessments, an unequal level of supervision of AML/CFT compliance, lack of a registration regime for MSBs, and concerns around fit-and-proper screening requirements. Canada made significant progress since then.

Criterion 26.1—FINTRAC is the AML/CFT supervisor for all REs subject to the PCMLTFA. It is assisted in the regulation and supervision of FIs by other federal and provincial regulators that are responsible for prudential and conduct supervision. However, ultimate responsibility for supervision and sanctioning under the PCMLTFA remains with FINTRAC. It is estimated that 80 percent of Canada's financial sector market is controlled by FRFIs. FRFIs are under the supervision of OSFI and include six large conglomerates (DSIBs) that hold a substantial share of the financial sector and other financial entities such as banks, insurance companies, cooperative credit and retail associations, trust companies, and loan companies. OSFI's powers are mandated under the OSFI Act and governing legislation for the various financial sectors such as the *Bank Act, Trust and Loan Companies Act, Insurance Companies Act*, and *Cooperative Credit Associations Act*. Non-FRFIs (e.g., credit unions) are regulated and supervised by provincial regulators under provincial statute.

AML/CFT supervisory functions are concentrated in FINTRAC and have not been delegated to primary regulators in Canada. At the federal level, OSFI and FINTRAC concurrently assess FRFI's for compliance with AML/CFT compliance obligations and are moving to a joint examination process (see further details below). At the provincial level, FINTRAC conducts AML/CFT supervision on non-FRFIs with the cooperation of other supervisors and has signed 17 MOUs with supervisors in relation to non-FRFIs. FINTRAC is authorized to share information with primary regulators at national and provincial levels relating to AML/CFT to monitor compliance with the PCMLTFA, and such regulators are also authorized to share information with FINTRAC.

Market Entry

Criterion 26.2—Federal and provincial authorities are the primary regulators of FIs with responsibility for prudential and conduct supervision including the licensing and registration of market entrants. FINTRAC is responsible for the registration and supervision of MSBs (along with AMF for MSBs operating in Quebec).

Market entry rules for FRFIs are set out in the relevant federal governing legislation and the process is entirely under the control and direction of OSFI. The Minister of Finance is responsible for approving Letters Patent creating domestic FRFIs, and for authorizing foreign banks and life insurance companies to operate branches in Canada by means of Ministerial Orders. OSFI is responsible for managing the process leading up to Ministerial actions. Authorized banking is regulated both at the federal and provincial levels and it is not possible for the process to permit the creation or authorization of shell banks.

The following table sets out the licensing or registration requirements in Canada:

Reporting Entities	Primary Regulator	Licensed/Registered	Legislation
Banks	Federal-OSFI	Licensed. Domestic banks are created by the Minister pursuant to an incorporation process discussed below. Authorized foreign banks receive certificates to operate by one or more branches in Canada.	Bank Act
Cooperative Credit and Retail Associations[34]	Federal-OSFI for Cooperative Retail Associations; Provincial-Cooperative Credit Associations	Same as domestic banks	Cooperative Credit Associations Act
Credit Unions and caisses populaires	Provincial authorities	Registration	Legislation includes Credit Unions Act; Financial Institutions Act; Credit Union Incorporation Act; Credit Unions and Caisses Populaires Act; Deposit Insurance Act; An act respecting financial services cooperatives; An Act respecting the Mouvement Desjardins
Life Insurance Companies	Federal-OSFI Provincial authorities	Licensed[35] Either licensed or registered	Insurance Companies Act Legislation includes Insurance Act; Financial Institutions Act; Insurance Companies Act;

[34] OSFI's oversight of Cooperative Credit Associations, commonly referred to as credit union centrals, is limited and quite different from its oversight of banks and other FRFIs. Cooperative Credit Associations are organized and operated based on cooperative principles. With the exception of the Credit Union Central of Canada ('CUCC'), the Cooperative Credit Associations are provincially incorporated, and regulated and supervised at the provincial level. The CUCC, which is federally incorporated, functions as the national trade association for the Canadian credit union system and does not provide any financial services. Cooperative Retail Associations are federally incorporated and supervised by OSFI in the same way as for banks and other FRFIs.

[35] Domestic life insurance companies under OSFI's jurisdiction are created by the Minister pursuant to an incorporation process discussed below. Authorized foreign life insurance companies only operation under the federal legislation and receive Ministerial Orders permitting one or more branches in Canada.

			Life Insurance Act; Registered Insurance Brokers Act; An Act respecting insurance (Quebec); An Act respecting the distribution of financial products and services(Quebec); Saskatchewan Insurance Act
Life Insurance Brokers and Agents	Provincial authorities	Licensed or registered	Legislation includes Insurance Act; Financial Institutions Act; Insurance Companies Act; Life Insurance Act; Registered Insurance Brokers Act; Saskatchewan Insurance Act; An Act respecting insurance (Quebec); An Act respecting the distribution of financial products and services (Quebec)
Trust and Loan Companies	Federal-OSFI Provincial authorities	Licensed Licensed or registered	Trust and Loan Companies Act Legislation includes Loan and Trust Corporations Act; Financial Institutions Act; Corporations Act; Trust and Loan Companies Act; Trust and Loan Companies Act; Deposit Insurance Act; An act respecting trust companies and savings companies (Quebec)
Investment Dealers	IIROC Provincial authorities	Registration Licensed (Northwest Territories) or registered	IIROC Dealer Member Rules Legislation includes Securities Act; Commodity Futures Act; An Act pertaining to financial products and services (Quebec); Derivatives Act;
Mutual Fund Dealers	Mutual Funds Dealers Association Provincial authorities	Registered Licensed (Northwest Territories) or registered	MFDA Rules Legislation includes Securities Act; Commodity Futures Act; An Act pertaining to financial products and services (Quebec); Derivatives Act;
Investment Counsel and Portfolio Management Firms	Provincial authorities	Licensed (Northwest Territories) or registered	Legislation includes Securities Act; Commodity Futures Act; An Act pertaining to financial products and services (Quebec); Derivatives Act;
Other securities firms	Provincial authorities	Licensed (Northwest Territories) or registered	Legislation includes Securities Act; Commodity Futures Act;

			An Act pertaining to financial products and services (Quebec); Derivatives Act;
Money Service Businesses	FINTRAC Autorité des marchés financiers (Québec)	Registration Licensed	PCMLTFA and PCMLTF Registration Regulations Money-Services Business Act

Criterion 26.3—Federal and provincial regulators are responsible for carrying out fit-and-proper tests on persons concerned in the management or ownership of FIs in Canada. The measures are used to prevent criminals or their associates from holding a significant or controlling interest in an FI in Canada.

OSFI conducts fit-and-proper tests on FRFIs at the application stage to assess the fit-and-proper status of applicants, their principals (beneficial owners), senior management, and Boards of Directors. Fit-and-proper tests are conducted under the Bank Act (ss.27, 526 and 675), Trust and Loan Companies Act (s.26), Cooperative Credit Associations Act (s.27), and Insurance Companies Act (ss.27 and 712). OSFI requires that applicants provide details of whether applicants have been the subject of any criminal proceedings or administrative sanction and it conducts security screening.

OSFI has the authority to apply fit-and-proper tests during the lifetime of a FRFI but only applies this authority directly to changes of ownership and/or shareholding. To address changes in directors or senior managers, OSFI has issued Guideline E-17 "Background Checks on Directors and Senior Managers of Federally Regulated Entities" in that regard. These requirements are applied throughout the life of FRFIs. After an FRFI is licensed, fit-and-proper testing on new senior officers and Directors is conducted by the FRFI rather than by the regulator. However, OSFI continues to apply fit-and-proper checks on new shareholders. OSFI assesses FRFIs' compliance with the Guideline and has issued prudential findings on background checks conducted by FRFIs on responsible persons. Since 2014, FRFIs are required to notify OSFI of plans to appoint or replace senior managers or directors.[36]

Persons and entities operating and controlling MSBs are required to register with FINTRAC under the PCMLTF Registration Regulations. FINTRAC conducts criminal record checks when assessing applications for registration as MSBs and it can refuse or revoke registrations where a person has been convicted of certain criminal offenses.

Provincial regulators apply fit-and-proper controls to assess the suitability of persons who control, own, or are beneficial owners of provincially regulated FIs. General fit-and-proper requirements apply in the securities and insurance sectors. For example, the Investment Industry Regulatory Organization of Canada (IIROC) evaluates whether an individual appears to be "fit and proper" for

[36] OSFI issued an Advisory on Changes to the Membership of the Board or Senior Management.

approval/registration and /or whether the individual's approval is otherwise not in the public interest. Included in the criteria are the evaluation of an individual's integrity and criminal record. Provincial securities regulators apply similar criteria. In addition, MSBs located in Quebec are subjected to a "fit-and-proper" test by the Autorité des marches financiers (AMF) under the *Money Services Business Act* (Quebec).

Provincial regulators have not adopted fitness and probity requirements for persons owning or controlling financial entities after market entry to the same extent as what is achieved at federal level.

Risk-Based Approach to Supervision and Monitoring

Criterion 26.4—OSFI and provincial regulators are responsible for prudential and conduct supervision of Core Principle institutions in Canada under the OSFI Act, provincial legislation and other governing legislation. OSFI applies an AML/CFT assessment program as part of the Core Principles-based prudential supervision of FRFIs. All FRFIs are supervised by OSFI on a consolidated or group basis, as required by the Core Principles. Canada underwent an IMF FSAP in 2013 and OSFI was found to comply with the implementation of the Core Principles in the banking and insurance sectors and was rated LC.

FINTRAC is responsible for the supervision of all REs for AML/CFT compliance under the PCMLTFA, including Core Principles institutions supervised by OSFI and provincial prudential regulators. OSFI and FINTRAC have a coordinated approach to supervision of Core Principles institutions that are FRFIs. FINTRAC consults and coordinates with other federal and provincial prudential supervisors and has signed 17 MOUs with regulators to exchange compliance related information.

Both OSFI and provincial regulators adopt a risk-based approach to identify firms that have a higher risk of AML/CFT activities. In 2013, OSFI and FINTRAC adopted a concurrent approach to conduct AML/CFT examinations in the FRFI sector. Non-Core Principles institutions are supervised by FINTRAC for compliance with the PCMLTFA. FINTRAC also receives information from provincial regulators arising from their prudential/conduct supervisory activities that may be relevant to AML/CFT compliance. MSBs are registered and supervised by FINTRAC (and AMF in Quebec) for compliance with the PCMLTFA.

Criterion 26.5—AML/CFT supervision is conducted in Canada on a risk-sensitive basis. A shorter version of the NRA identifying the inherent ML/TF risks in Canada has recently been published and the findings are being incorporated into supervisors' compliance activities. Supervisors have their own operational risk assessment models and they use a range of programs, activities and tools to supervise and monitor compliance with AML/CFT requirements. There has been an increase in the frequency and intensity of onsite and offsite supervision of FIs in recent years. There has also been an increase in resources at FINTRAC to carry out compliance activities since the last MER.

FINTRAC has developed an AML/CFT Supervisory Program that is risk-based to ensure that REs are complying with their obligations under the PCMLTFA. It uses an enhanced risk-assessment model to

assign risk ratings to REs that allows the allocation of resources according to higher-risk areas. Its risk model relies on information such as media information, ML/TF intelligence, financial transaction reporting behavior, information received from law enforcement and regulatory partners that have MOUs with FINTRAC. It is updated regularly using information it collects through intelligence and examinations and is adjusted following on-site and off-site examinations. The risk assessment carried out on FRFIs is done in collaboration with OSFI.

FINTRAC's Supervisory Program is influenced and guided by a number of factors including the risk rating of the RE using the enhanced risk-assessment model and using other tools such as the examination selection strategy. FINTRAC focuses its supervisory activities on a risk-based approach using higher-intensity activities for higher-risk REs and using other lower-intensity activities for medium-and lower-risk entities. FINTRAC's primary tool to supervise for AML/CFT compliance is its examinations strategy that is well developed. The examination strategy developed by FINTRAC prioritized activities aimed at REs that have been found to be non-compliant previously and those with high-risk ratings. It also focuses on key industry players with large market shares, which are examined regularly, given the inherent risks that are associated with their size and respective business models and the consequences of non-compliance. FINTRAC also has a range of off-site mechanisms to conduct supervision of FIs including compliance assessment reports (CAR), desk-based reviews, monitoring of financial transactions, observation letters, compliance enforcement meetings, IT tools, voluntary self-disclosures of non-compliance and other awareness/assistance tools. CARs are used to segment REs within a sector, with results being used to initiate desk and on-site exams.

OSFI applies a risk-based approach to AML/CFT supervision. It has an AML/CFT risk assessment separate from its prudential risk assessment model for FRFIs and directs its assessment program at Canada's largest banks and insurance companies and other FRFIs considered at highest risk of ML and TF. OSFI's risk assessment methodology focuses on the vulnerabilities of FRFIs to ML and TF, looking at factors such as size, geographical spread, products, services and distribution channels and quality of risk management generally. It assigns a risk profile on each institution considering the risk factors and the quality of its risk management. OSFI's risk assessment results in a classification of FRFIs into categories of high, medium and low risk based on a combination of inherent risk, coupled with broader prudential views on the quality of risk management. OSFI supervises FRFIs on a group-wide basis and it conducts examinations of FRFI's on a cyclical basis depending on an FRFI's risk ratings and when information is received from prudential supervisors and other regulators including FINTRAC. OSFI also monitors major events or developments impacting the management or operations of FRFIs that informs both the content of AML/CFT assessments and also the assessment planning cycle.

FINTRAC and OSFI have agreed a concurrent approach to AML/CFT supervision of FRFIs allowing for concurrent examinations in addition to individual examinations that both supervisors can conduct of FRFIs. Both OSFI and FINTRAC exchange information that is relevant to FRFI's compliance with AML/CFT obligations. FINTRAC and provincial regulators also exchange information and FINTRAC can conduct AML/CFT follow-up activities with provincially regulated REs when AML/CFT issues are

reported to it. Other supervisors also adopt risk assessments and supervision that are related to AML/CFT. For example, IIROC uses a risk assessment model for IIROC-regulated firms to determine priority focus and can apply an AML examination module by IIROC that is judged to present an AML/CFT risk. The primary responsibility for AML/CFT supervision remains with FINTRAC and any supervisory activity conducted by other supervisors' supplements, but does not replace, FINTRAC's responsibility to ensure compliance with the PCMLTFA and Regulations made thereunder.

Criterion 26.6—FINTRAC reviews its risk model on an ongoing basis and recently reviewed its sectoral analysis. FINTRAC also reviews its understanding of ML/TF risks for individual REs through reviewing the institution's compliance history, reporting behavior and risk factors. In its ongoing review of the risk assessment, FINTRAC regularly monitors and assesses actionable intelligence, ML/TF risks and trigger events. OSFI reviews its AML/CFT risk profiles of FRFIs periodically. Risk assessments are applied to DSIBs on a continuous basis, reflecting their dominance of the FRFI sector and their very high-risk level. On-site assessments of DSIBs are conducted on a regular basis and DSIBs may be subject to more intensive supervision (staging) where deficiencies have been identified. The review of the risk profiling of other high-risk FRFIs is updated at less frequent intervals, due to their less complex risk profiles. Provincial regulators are also kept apprised of ML/TF risks by FINTRAC and through the recently published NRA.

Weighting and Conclusion

Further fitness and probity controls are required. **Canada is largely compliant (LC) with R.26.**

Recommendation 27—Powers of Supervisors

In the 2008 MER, Canada was rated LC with these requirements, notably because FINTRAC had no power to impose AMPs on REs. This has been remedied in December 2008.

Criterion 27.1—FINTRAC has authority to ensure compliance by all REs with parts 1 and 1.1 of the PCMLTFA (s.40). OSFI and provincial supervisors also have supervisory powers over REs under their own supervisory remit under federal and provincial legislation: e.g., the OSFI Act indicates the Superintendent's powers and duties in relation to the Bank Act, Trust and Loan Companies Act, the Cooperative Credit Associations Act and the Insurance Companies Act and the supervisory powers of the Superintendent are uniform under these Acts.

Criterion 27.2—FINTRAC has the authority to conduct inspections of FIs under the PCMLTFA. It can carry out on-site examinations of REs under PCMLTFA, s.62(1). Such examinations can be routine (with notice) but FINTRAC also has the authority to conduct unannounced examinations of REs under the PCMLTFA. OSFI has no mandate under PCMLTFA, but it supervises FRFIs under the OSFI Act and FRFIs' governing legislation (e.g., Bank Act) to determine whether they are in sound financial condition, are managed safely, and are complying with their governing statute law. IIROC and provincial regulators conduct audits of registered firms to ensure compliance with Canadian securities laws.

Criterion 27.3—FINTRAC is authorized under the PCMLTFA to compel production of any information relevant to monitoring compliance with AML/ATF requirements. It can enter any premises (except a dwelling house) to access any document, computer system and to reproduce any document "at any reasonable time" (PCMLTFA, ss.62(1) and (2)). FINTRAC also has the authority to require REs to provide any information that FINTRAC needs for compliance purposes (s.62). There is a 30-day period given to deliver the information (PCMLTFR, s.70). OSFI has general powers to compel information from REs under OSFI Act, s.6 and federal governing legislation. While not mandated under the PCMLTFA, other regulators have the power to compel information under provincial or governing legislation to protect the public and market integrity. FINTRAC can exchange information on compliance with Parts 1 and 1.1 of the PCMLTFA with federal and provincial agencies that regulate entities.

Criterion 27.4—FINTRAC and OSFI have a range of supervisory tools to sanction REs for non-compliance. These tools include supervisory letters, action plans for FRFIs, staging by OSFI, compliance agreements, revocation of registration of MSBs by FINTRAC, revocation of FRFIs' licenses by the AG of Canada[37] and criminal penalties. The PCMLTFA AMP Regulations provide FINTRAC with the power to apply AMPs to any FI and DNFBPs subject to the AML/CTF regime for non-compliance with the PCMLTFA. Provincial regulators, IIROC and MFDA have the power under their own governing legislation to conduct investigations and undertake enforcement action where necessary to protect the public and market integrity. They have the power to restrict, suspend, and cancel registration. Further information is provided under the analysis of R.35.

Weighting and Conclusion

Canada is compliant (C) with R.27.

Recommendation 28—Regulation and Supervision of DNFBPs

In the 2008 MER, Canada was rated NC with these requirements (pages 229–243) notably because of deficiencies in the scope of the DNFBPs covered and not subject to FINTRAC supervision, and the sanction regime and resources available to FINTRAC were considered inadequate. Since then, the scope of DNFBPs under the supervision of FINTRAC has been extended to BC Notaries and DPMS, and FINTRAC was granted the power to impose sanctions under the PCMLTF AMP Regulations.

Casinos

Criterion 28.1—

a) Gambling activities are illegal in Canada, except if conducted and managed by the province or pursuant to a license issued by the province on the basis of CC, ss.207(1)(a) to (g), and three different models are in place (charity, commercial casinos, First Nation casinos, as described in the

[37] This authority is subject to a number of conditions as set out in federal governing legislation.

2008 MER, pages 214–215). Internet gambling are not subject to AML/CFT obligations, as the amendment to the definition of casino under PCMLTFA[38] is not yet into force, as well as ship-based casinos (the latter is a very minor issue, considering that, according to the authorities, no Canadian cruise ship are currently being operated, and lottery schemes cannot be operated within 5 nautical miles of the Canadian shore). Several provinces have introduced internet gambling (British Columbia, Quebec, Manitoba, Nova Scotia, Prince Edward Island, New Brunswick, and Newfoundland). Under the provincial legislation, also lottery schemes performed through Internet are required to be licensed.

b) All provinces and territories have regulation on terms and conditions for obtaining the license and a regulatory authority empowered to administer the relevant provincial legislation. Due-diligence requirements of the applicants (casino operator, key persons associated with the applicants and executive members) are part of the licensing process, where financial, business information, information referring to criminal proceedings, and reputational elements are required and subject to a review conducted by the competent provincial regulatory authorities. The licensing provisions make reference to due-diligence procedure related to an extensive notion of "associates" of the applicant, and when the applicant is a company or a partnership controls are extended to partners, directors, as well as to any subject who directly or indirectly control the applicant or has a beneficial interest in the applicant. Notice of changes in directors, officers, associated of the registrants are submitted to the approval of the competent regulatory authority. Notification of charges and convictions of the licensee, as well as of its officers, shareholders, owners are required. In respect of charities that require a license to conduct casino events eligibility requirements must be met both where a charitable model has been adopted[39] and where a corporation model is in place.[40] Charitable events may be licensed also by First Nations Authority under the agreement with the relevant provincial legislator (Manitoba, Saskatchewan),[41] where the authority to issue license to charitable gaming has been delegated by the competent provincial authorities in favor of First Nations commissions. Under the Agreements (Part 10.1) the parties agree that the terms and conditions that apply to licenses off and on reserve are essentially the same. Audits are performed in order to ensure that the operators comply with the terms and conditions of the license.

[38] In particular, PCMLTFA, Section 5, k, (i).

[39] Pursuant to Section 20 (1) of the Gaming and Liquor Regulation in Alberta charitable or religious organization in order to qualify for the license must satisfy the board that the proceeds generated from the gaming activities must be used for charitable and religious activities. In this context, the volunteers of charities are allowed to work in key positions at the casino events only if licensed, thus being subject to criminal record checks. The Commission must ensure that the licensed organization comply with the relevant legislation.

[40] Where Lottery Corporations are empowered to conduct and manage gaming on behalf of the provincial government, group or organization can be licensed to hold a gaming event by the competent regulator. In British Columbia background investigations may be conducted also in respect of the eligible organization, its directors, officers, employees, or associated (Section 80 (1) (g) (vi) of the Gaming Control Act. Audit of the licensee are performed conducted by the Charitable Gaming Audit Team of the Gaming Policy and Enforcement Branch.

[41] In Saskatchewan the Provincial regulatory authority, SLGA, owns and manage the slot machines at six casinos operated by the Saskatchewan Indian Gaming Authority, a non-profit corporation licensed by SLGA, while the Indigenous Gaming Regulator has a delegated authority under 207 (1) (b) of the CC to issue charitable gaming licenses on designated reserves.

Under the relevant provincial legislation, the same provisions apply also to lottery schemes performed through Internet.

The table below summarizes the list of casino's regulators identified under the provincial gaming legislation and the relevant legislation. Licensing authorities do not have express AML/CFT responsibility to qualify as competent authorities.

Province	Regulator	Provincial Legislation
Alberta	Alberta Gaming and Liquor Commission	Gaming and Liquor Act
British Columbia	Gaming Policy and Enforcement Branch	Gaming Control Act
Manitoba	Liquor and Gaming Authority of Manitoba First Nations Gaming Commissions at reserve charitable gaming within the municipality or on reserve	Liquor and Gaming Control Act
New Brunswick	Gaming Control Branch-Department of Public Safety	Gaming Control Act
Nova Scotia	Nova Scotia Alcohol and Gaming Division	Gaming Control Act
Ontario	Alcohol and Gaming Commission of Ontario	Gaming Control Act Alcohol and Gaming Regulation and Public Protection Act
Quebec	Régie des alcools des courses et des jeux	Act Respecting Lotteries, Publicity Contest and Amusement Machines An Act respecting the Société des lotteries du Québec.
Saskatchewan	Saskatchewan Liquor and Gaming Authority IGR responsible for licensing and regulating charitable gaming on First Nations, operating through a Licensing Agreement with SLGA (2007).	The Alcohol and Gaming Regulation Act
Yukon	Professional Licensing and Regulatory Affairs Branch	Lottery Licensing Act Sec 2 (Eligibility) and Sec 10 (Regulations) of the Lottery Licensing Act
Newfoundland and Labrador	Department of Government Services and Lands, Trades Practices and Licensing Division (no specific provisions)	Lottery schemes-General rules
Prince Edward Island	PEI Lotteries Commission /Department of Community and Cultural Affairs for casinos charities	Lotteries Commission Act
Northwest territories	Consumer Affairs, Department of Municipal and Community Affairs	Lotteries Act Lottery Regulations

Nunavut	Department of Community and Government Services	The Lotteries Act and Regulations

c) FINTRAC is the only competent supervisory authority for compliance of casinos with AML/CFT requirements. It has signed the MOUs with the following regulators: Alcohol and Gaming Commission of Ontario (AGCO); British Columbia Gaming Policy Enforcement Branch (GPEB); Alcohol and Gaming Division of Service Nova Scotia; Saskatchewan Liquor and Gaming Authority (SLGA). Online gambling is not covered by the definition of casino currently into force under PCMLTFA.

DNFBPs Other than Casinos

Criterion 28.2—FINTRAC is the designated competent authority under PCMLTFA and PCMLTFR for the AML/CFT supervision of all DNFBPs. FINTRAC supervises 26,000 DNFBPs in total, including casinos (discussed under 28.1), trust and loan companies, accountants, dealers in precious metals and stones, BC Notaries, and real estate agents and developers. As described under R.22 lawyers and Quebec notaries, trust and company service providers that are not included among the trust and loan companies are not monitored for AML/CFT purposes.

Criterion 28.3—All the categories of DNFBPs that fall into the scope of AML/CFT regime are monitored by FINTRAC for compliance with AML/CFT requirements. Apart from real estate dealers under certain condition, the AML requirements have not been extended to other categories in addition to those provided for in the FATF standards.

Criterion 28.4—

a) FINTRAC powers to monitor and ensure compliance are the same for FIs and DNFBPs (PCMLTFA s. 62). For details, see R.27.

b) The powers to prevent criminals or their associates from being accredited, or from owning, controlling or managing a DNFBPs other than casinos are more limited. No specific measure is in place for DPMS. Referring to accountants the current process of creating a unified new professional designation, the Chartered Professional Accountant, replacing the former three (Chartered Accountants, Certified General Accountants and Certified Management Accountants), is at different stages in the various provinces. The provincial associations are in charge of ensuring high professional standards also through investigation of complaints and enforcement actions. In the admission to membership disclosure of investigations and disciplinary proceedings is required and consent must be provided permitting the Registrar to access the relevant information.[42] Members are also required to promptly inform CPA after having being convicted of criminal offenses.[43] Allegations for a wide set of crimes, included ML, financial frauds, TF, entail a rebuttable

[42] Section 2 of Reg. 4-1 of CPA Ontario.

[43] Rule 102. 1 of the Rules of professional conduct CPA Ontario.

presumption of failing to maintain good reputation of the profession.[44] Accounting firms (partnerships, limited liability partnerships and professional corporations) are required to disclose investigations involving any partners[45] or shareholders and consent shall be provided permitting the Registrar to access information regarding such investigation. Any change in partners, shareholder must be notified and failure to provide such disclosure are considered breach of memberships obligations. Regarding BC Notaries, under the Notaries Act of BC, the Society of Notaries Public of BC is empowered to maintain standards of professional conduct. The procedure for the enrolment include screening procedure conducted by the Credentials Committee of the Society, where consent for disclosure of criminal records information in favor of the RCMP must be provided. Under the Notary Act, also Notary Corporation (Notary Act, ss.57 and 58(f)) are subject to a permit and the procedure imply controls on the voting shares members (that must be members of the Society in good standing, thus having passed the screening procedures described above related to disclosure of criminal records) as well as the non-voting members (who can be only members of the Society or relatives). The Society is empowered to impose fines, as well as take disciplinary action and revoke the permits (Notary Act, s.35). In respect of real estate agents, as shown in the attached each province has suitability requirements for licensee that apply as individual,[46] which in most cases entail the provision of Certified Criminal Records Checks. Nevertheless, in some cases the relevant provisions make reference both as a condition of refusal to issuing and to suspending or cancelling a license to the notion of "public interest,"[47] which, despite the authorities, consider broad to include a large number of factors, seems to be too vague and left to the discretion of the competent regulatory authorities. The integrity requirements in respect of corporations and partnerships are not always expressly extended to partners, directors, officers.[48] Not always changes in the directors, officers, shareholders, partners must be notified to the competent provincial Authority.[49] Furthermore, the relevant legislation is essentially orientated in a perspective of consumer's protection so that in some cases the condition for refusal of the license are previous convictions of indictable offense "broker-related,"[50] as well as the notification of licensee makes reference to convictions involving a limited set of offenses.[51] Moreover, as the presence of criminal records is not

[44] Rule 201.2 of 1 of the Rules of professional conduct CPA Ontario.

[45] Regulations 4-6, Section 11, CPA Ontario.

[46] No specific integrity requirement under the Real Estate Agents Licensing Act. The convictions of offenses against the CC shall be related to qualifications, functions or duties of the agent/sales persons (Section 18, (k) and are cause for suspension or cancellation of license.

[47] Manitoba, Section 11(1) of the Real Estate Brokers Act, New Brunswick, Section 10 (2) of the Real Estate Act; Prince Edward Islands, Section 4 (3) of the Real Estate Trading Act.

[48] In Saskatchewan, for example, under Section 26.1 (b) of the Real Estate Act the integrity requirements are limited to officers and directors. The same requirement is established in Nova Scotia under 12 (1) (b) of the Real Estate Trading Act.

[49] Only change in officials and partners in New Brunswick, Section 15 (1) (b) and (c) of Real Estate Act partners in Prince Edward Island Section 14 of Real Estate Trading Act.

[50] Quebec, Section 37 of the Real Estate Brokerage Act.

[51] New Brunswick, Section 15 (2) of the Real Estate Act (frauds, theft or misrepresentation).

necessarily a bar to registration, a case-by-case approach is taken by the regulatory authority. Provincial legislation establishes an express exemption regime in favor of lawyers, trust companies,[52] and in some cases accountants from the requirement for license in respect of real estate services provided in the course of their practice.

DNFBPS Category	Designated Competent Authority	Relevant Legislation	Market Entry Safeguards
Real Estate	**Regulatory Authority**	**Provincial Legislation**	All the provinces have suitability requirements for licensee that apply as individual. The integrity requirements in respect of corporations and partnerships are not always expressly extended to partners, directors, officers. Not always changes in the directors, officers, shareholders, partners must be notified to the competent provincial Authority
Alberta	Real Estate Council of Alberta	Real Estate Act, in particular Part 2, s.17, Real estate Act Rules (20 (1) for individuals, ss.30 and 34 for real estate brokerage. s.10.3 of Real Estate Regulations	
British Columbia	Real Estate Council of British Columbia	Real Estate Services Act ss.3(1) and 10	
New Brunswick	New Brunswick Financial and Consumer Services Commission Division	New Brunswick Real Estate Act ss.3 and 4.2	
Newfoundland and Labrador	The Financial Service Regulation Division	Real Estate Trading Act, s.7	
Manitoba	Manitoba Securities Commission for licensing	The Real Estate Brokers Act and The Mortgage Brokers Act	
Nova Scotia	Nova Scotia Real Estate Commission	Real Estate Trading Act ss.4, 12	
Ontario	Real Estate Council of Ontario	Real Estate and Business Brokers Act s.9.1, 10 (19)	
Prince Edward Island	Office of the Attorney General, Consumer and Corporate and Insurance Services	Real Estate Trading Act, ss.4 (3), 8 (2) b); 14	
Quebec	Organisme d'autoréglementation	Loi sur le courtage immobilier ss.4, 6, 37	

[52] See, for example in British Columbia, Real Estate Service Act, Section 3, (3) lett. e) and f) the exemption regime in favor of FI that has a trust business authorization under the Financial Institutions Act and practicing lawyers.

	du courtage immobilier du Québec		
Saskatchewan	Real Estate Commission	The Real Estate Act s.18 (1) and 26 (1)	
Yukon Territories	Professional Licensing and Regulatory Affairs	Real Estate Agents Act, ss.6, 7	
Northwest Territories	Municipal and Community Affairs- Superintendent of Real Estate	Real Estate Agents Licensing Act, ss.2, 1; 8 (1); 18	
Nunavut	Consumer Affairs	Real Estate Agents Licensing Act	
Accountants and Accounting Firms	Chartered Professional Accountant, the Certified Management Accountant, the Certified General Accountant and provincial associations	conducts (as),	As regards admission to Membership see, for example, Certified Management Accountants of Ontario (Regulation 4-1); CMA Regulations of Alberta (s.2 (2), where it is stated that each applicant for registration shall provide evidence on conviction of a criminal offense.
DPMS	**No designated competent authority**	**-**	**No measure in place**
BC Notaries	The Society of Notaries Public	the Notary Act	The procedure for the enrolment include screening procedure conducted by the Credentials Committee of the Society, where consent for disclosure of criminal records information in favor of the RCMP. Notary Corporation (ss.57 and 58 f the Notary Act) are subject to a permit and the procedure imply controls on the voting shares members (that must be in good standing) as well as the non-voting members (who can be only members of the Society or relatives)

c) There are civil and criminal sanctions[53] available for failure to comply with AML/CFT obligations for DNFBPs as described under R.35, as well as the public notice of AMPs imposed. The AMP regime allows administrative sanctions to be applied to REs although the maximum threshold raises doubts about the dissuasiveness and/or proportionality of sanctions for serious violations or repeat offenders. However, there is a range of measures available to supervisors to ensure compliance that are both proportionate and dissuasive.

All DNFBPs

Criterion 28.5—FINTRAC has further developed its risk model that lead to a risk classification (low, medium, high) of activity sectors and entities and the frequency and intensity of supervision is a function of FINTRAC's risk assessment. FINTRAC has started to integrate the results of inherent NRA for 2015/2016. The risk model takes into account numerous sources of information in order to assess the risk factor of specific REs. Further details on how the risk profile affects the scope and frequency of controls are provided under IO.3.

Weighting and Conclusion

AML/CFT obligations are inoperative for legal counsels, legal firms, and Quebec notaries. Online gambling, ship-based casinos, trust and company service providers that are not included among the trust and loan companies are not subject to AML/CFT obligations and not monitored for AML/CFT purposes. The entry standards and fit-and-proper requirements are absent in DPMS and TCSPs, while for the real estate brokerage, they are not in line with the standards. Taking into account the deficiencies identified in the scope of DNFBPs and subsequent coverage of AML/CFT supervision, and in the fit-and-proper requirements for DPMS, TCSPs, and for the real estate brokerage, **Canada is partially compliant (PC) with R.28.**

Recommendation 29—Financial Intelligence Units

In its third MER, Canada was rated PC with former R.26 (see paragraphs 364–418) notably due to the fact that the FIU (i) had insufficient access to intelligence information from administrative and other authorities, and (ii) was not allowed to gather additional information from REs. The first deficiency has since been addressed. The FATF standard was strengthened by new requirements which focus on the FIU's strategic and operational analysis functions, and the FIU's powers to disseminate information upon request and request additional information from REs.

Criterion 29.1—In 2000, Canada established an administrative FIU—Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), which is a national center for receiving, analyzing, and disseminating information in order to assist in the detection, prevention, and deterrence of ML, associated predicate offenses, and TF activities: PCMLTFA, s.40. The definition of an ML offense

[53] Sections 73.1 to 73.24 of PCMLTFA.

under the PCMLTFA is based on the definition of the offenses established in the CC, which includes information related to associated predicate offense.[54]

Criterion 29.2—FINTRAC serves as a national agency authorized to receive STRs and other systematic reporting required by the PCMLTFA or the PCMLTF regulations, including Terrorist Property Reports, Large Cash Transaction Reports (of Can$10,000 or more), SWIFT and Non-SWIFT Electronic Funds Transfer Reports (of Can$10,000 or more), Casino Disbursement Reports (of Can$10,000 or more), physical cross-border currency or monetary instruments reports and seizures reports and any financial transaction, or any financial transaction specified in PCMLTFA. In addition, FINTRAC is authorized to receive voluntary information records (VIRs), i.e., information provided voluntarily by LEAs[55] or government institutions or agencies, any foreign agency that has powers and duties similar to those of the Centre (i.e., FINTRAC), or by the public about suspicions of ML or TF activities.[56]

Criterion 29.3—

a) FINTRAC may request the person or entity that filed a STR to correct or complete its report when there are quality issues such as errors or missing information, but not in other instances where this would be needed to perform its functions properly. According to the authorities, Canada's constitutional framework prohibits FINTRAC from requesting additional information from REs. This deficiency was highlighted in Canada's Third MER, and Canada's Sixth Follow-up Report concluded that, despite the information-sharing mechanism put in place by FINTRAC since its last evaluation, the deficiency has not been adequately addressed.

b) PCMLTFA, ss.54 (1) (a) to (c), states that FINTRAC may collect information stored in a database maintained, for purposes related to law enforcement or national security, by the federal government, a provincial government, the government of a foreign state or an international organization, if an agreement to collect such information has been concluded. FINTRAC has direct or indirect access to a wide range of law enforcement information, as the Canadian Police Information Centre (CPIC), the Public Safety Portal (PSP), CBSA's cross-border currency reports and seizure reports databases, RCMP's National Security systems and Sûreté du Québec's criminal information and the Canada Anti-Fraud Centre of the RCMP databases, as well as to the CSIS database. However, FINTRAC still has insufficient access to the information collected and/or maintained by—or on behalf of—administrative and other authorities, such as CRA databases.

[54] See subsection 462.31(1) of the criminal code where "designated offence" means "a primary designated offence or a secondary designated offence" under section 487.04 of the CC.

[55] FINTRAC receives information provided voluntarily by CSIS, CBSA, CRA—Criminal Investigation Directorate—and the RCMP, as well as provincial and municipal police.

[56] VIRs are the mechanism used by LEAs and other partners of FINTRAC to send information to and advise FINTRAC of investigative priorities without creating an obligation on FINTRAC to respond so as to respect the principle of independence of the FIU. The majority of VIRs that FINTRAC receives focus on priority investigations. VIRs are often the starting point of FINTRAC's analysis (however, FINTRAC always maintains its ability to proactively develop cases).

Criterion 29.4—

a) FINTRAC must analyze and assess the reports and information received and/or collected under PCMLTFA, ss.54(1)(a) and (b), namely, STRs, Large Cash Transaction Reports, Electronic Funds Transfer Reports, Casino Disbursement Reports, physical cross-border currency or monetary instruments reports and seizures reports, information provided voluntarily by LEAs and other regime partners (i.e., the VIRs), queries from, foreign FIUs, as well as information collected from several databases or open source information (s.54(1) (c) PCMLTFA).

b) FINTRAC is also required to conduct research into trends and developments in the area of ML and TF activities and to undertake strategic analysis (s.58(1)(b) PCMLTFA). It does so by leveraging a range of open and classified sources of information. It publishes Typologies and Trends Reports[57] on a broad array of issues. From 2010 to 2015, it produced 62 strategic intelligence and research products, which identify ML/TF methods and techniques used by listed terrorist groups and criminal networks, emerging technologies, as well as vulnerabilities in different sectors (both covered and non-covered by the PCMLTFA). These reports provide feedback to REs, respond to Canada's intelligence priorities and build the evidence base for new policy development. FINTRAC has also participated to the working out of Canada's first formal NRA.

Criterion 29.5—FINTRAC is able to disseminate "designated information,"[58] either spontaneously or in response to a VIR, to the appropriate police force,[59] the CRA, CBSA, Communications Security Establishment, Provincial Securities Regulators (as of June 23, 2015) and CSIS, through secure and protected channels (ss.55(3)(a) to (g) and 55.1(1)(a) to (d) PCMLTA). It is also able to disseminate information upon request to LEAs with a court order issued in the course of court proceedings in respect of an ML, TF, or another offense (PCMLTFA, s.59(1). This process has not been used in recent years, as LEAs obtain sufficient information from FINTRAC in response to their VIRs. FINTRAC's AML/CFT supervisory unit and FIU unit are able to exchange information in the exercise of their respective functions. As indicated under R.30, some competent authorities, such as Environment Canada or Competition Bureau, cannot request information from the FIU.

Criterion 29.6—Information held by FINTRAC is securely protected and is disseminated in accordance with the PCMLTFA (s.40(c)). FINTRAC has internal procedures (FINTRAC's Privacy framework) governing the security and confidentiality of information, the respect of the

[57] Mass Marketing Fraud: Money Laundering Methods and Techniques (January 2015), Money laundering trends and typologies in the Canadian securities sector (April 2013), Money Laundering and Terrorist Financing Trends in FINTRAC Cases Disclosed Between 2007 and 2011 (April 2012), Trends in Canadian Suspicious Transaction Reporting (STR) (April and October 2011), Money Laundering and Terrorist Financing (ML/TF) Typologies and Trends for Canadian Money Services Businesses (July 2010), Money Laundering Typologies and Trends in Canadian Casinos (November 2009), Money Laundering and Terrorist Financing Typologies and Trends in Canadian Banking (May 2009).

[58] The terms "designated information" cover a range of information, including the name and criminal records of a person or entity involved in the reported transaction, the amounts involved, etc.

[59] The appropriate police force means the police force that has jurisdiction in relation to the ML offense. This includes federal, provincial and municipal police forces, as they receive their power from the province.

confidentiality and security rules by its staff members and limiting access to information, including access to the IT system, to those who have a need to know in order to effectively perform their duties.

Criterion 29.7—FINTRAC was established as an independent agency that acts at arm's length and is independent from LEAs and other entities to which it is authorized to disclose information under ss.55(3), 55.1(1) or 56.1(1) or (2) (PCMLTFA, s.40(a)).

a) The Director of FINTRAC is appointed by the Governor in Council for a reappointed term of no more than five years with a maximum term of ten years, and has supervision over and direction of the Centre regarding the fulfilment of its mission (internal organization, decisions taken, etc.) and in administrative matters (staff and budget).

b) FINTRAC is able to make arrangements or engage independently with other domestic competent authorities. Agreements or arrangements with foreign counterparts on the exchange of information are entered either into by the Minister or by the Centre with the approval of the Minister (PCMLTFA, s.56 (2)).

c) FINTRAC is not located within an existing structure of another authority: the FIU is an independent agency under the responsibility of the Minister with legally established and distinct core functions (PCMLTFA, ss.42 and 54).

d) The Minister is responsible for FINTRAC (PCMLTFA, s.42(1)) and the director of FINTRAC is the chief executive officer of the Centre, has supervision over and direction of its work and employees and may exercise any power and perform any duty or function of the Centre (PCMLTFA, s.45(1)).

Criterion 29.8—FINTRAC has been a member of the Egmont Group since 2002.

Weighting and Conclusion

FINTRAC has limited access to some information. **Canada is partially compliant (PC) with R.29.**

Recommendation 30—Responsibilities of Law Enforcement and Investigative Authorities

In its 2008 MER, Canada was rated LC with former R.27 due to an effectiveness issue. Minor changes have since been made. There are also significant changes in the standard.

Criterion 30.1—LEAs are designated with the responsibility for investigating ML, predicate offenses and TF. There is one national police force (the RCMP) and two provincial LEAs (respectively, in Ontario and Quebec). The RCMP is a federal, provincial, and municipal policing body. All Canadian police forces are potential recipients of FINTRAC disclosures under the PCMLTFA and can investigate ML/TF offenses.

Most predicate offenses are investigated by provincial and municipal police forces, including the RCMP when they are acting as provincial police (except Ontario and Quebec). Serious or proceeds-generating crime investigations can be done by the RCMP either exclusively or in parallel with provincial or municipal forces.

The RCMP has the primary law enforcement responsibility to investigate both terrorism and TF. The Terrorist Financing Team of the RCMP's Federal Policing Criminal Operations (FPCO) is responsible for, inter alia, monitoring and coordinating major ongoing investigational projects related to terrorist organizations on financial and procurement infrastructures.

Criterion 30.2—All national, provincial, and municipal police forces are authorized, under the CC, as "peace officers" to conduct parallel financial investigations related to their criminal investigations. They may refer the ML/TF case to other police units for investigation, regardless of where the predicate offense occurred.

Criterion 30.3—All police forces are empowered to identify, trace, seize, and restrain property that is, or may subject to forfeiture, or is suspected of being proceeds of crime. They are empowered with a wide range of measures under the CC (see Criterion 4.2).

Criterion 30.4—Other agencies, including the CRA (Income Tax Act), Competition Bureau (Competition Act, ss.11–21) and Environment Canada (Environmental Protection Act 1999), have the authority to conduct financial investigations related to the predicate offenses that they respectively specialize in. In addition, law enforcement agencies in Canada have the authority under Common Law to investigate crime and criminal offenses such as ML. They may seek judicial authority to seize and freeze assets. For the CBSA, although it does not have the responsibility for pursuing financial investigations of predicate offenses included in the Immigration Refugee Protection Act (IRPA), the Customs Act and border related legislations, a referral mechanism is in place for RCMP to follow up on the financial investigations. PCMLTFA, s.18 authorizes the seizure and forfeiture of cash by CBSA. Section 36 of the same Act also authorizes the disclosure of the information to the RCMP for criminal investigations into ML or TF.

Criterion 30.5—All police forces are responsible for investigating corruption offenses (CC, ss.119–121 and Corruption of Foreign Public Officials Act, s.3). As mentioned in R.4 and above, they have the powers to identify, trace, and initiate the freezing and seizing of assets.

Weighting and Conclusion

Canada is compliant (C) with the R.30.

Recommendation 31—Powers of Law Enforcement and Investigative Authorities

In its 2008 MER, Canada was rated C with former R.28. Minor changes have since been implemented in the Canadian legal framework as well as in the standard.

Criterion 31.1—

a) CC, ss.487.014 (production order) and 487.018 (production order for financial and commercial information) empower a justice or judge to order a person other than a person under investigation to produce specified documents or data within the time to any peace or public officer. S.487.018 production order for financial data is also available to compel a particular person or entity to disclose the identity of the account holder of a given account number.

b) Search warrant under CC, s.487 is available for peace and public officers to search any prescribed places for available information.

c) Law enforcement officers are authorized to take statements from voluntary witnesses under the powers conferred by the Common Law and in accordance with the Charter of Rights and Freedoms and the Canada Evidence Act. However, a witness cannot be compelled to provide a statement to police in an investigation of ML or its associated predicate offenses. For TF investigations, witnesses are bound to provide a statement in an investigative hearing under Part II.1 of the CC (Terrorism).

d) Search warrants under CC, s.487 (search and seizure of evidence) and 462.32 (search and seizure of proceeds of crime) empower investigators to search and seize evidence. The General Warrant under CC, s.487.01 further authorizes the use of any device or means to collect evidence.

Criterion 31.2—

a) RCMP can mount undercover operations to infiltrate crime syndicates and collect evidence for prosecution. Based on the principles in common law, the police are deemed to have common law powers where such powers are reasonably necessary in order for them to execute the mandate of investigating the commission of serious offenses, and undercover operations fall into this category.

b) Law enforcement can intercept communications pursuant to an Order made under CC, s.186 without the consent of the targeted person. It applies to organized crime offenses or an offense committed for the benefit of, at the direction of, or in association with a criminal organization; or a terrorism offense. It applies to both ML and TF offenses.

c) Computer systems can only be accessed with the consent of the owner or by a search warrant/General Warrant under the CC, but the courts[60] have found that particular considerations apply to computers and the stored content therein, which may require authorities to obtain specific prior judicial authorization to search computers found within a place for which a search warrant has been issued.

d) Similar to (a) above, Canadian Police are conferred with the power to conduct controlled delivery and is subject to stringent RCMP's internal policy.

[60] R. v. Vu, 2013 SCC 60 (CanLII)—http://www.canlii.org/en/ca/scc/doc/2013/2013scc60/2013scc60.html.

Criterion 31.3—

a) CC, s.487.018 (production order for financial and commercial information) empower a justice or judge to order a FI or DNFBP other than a lawyer to produce specified data within the time to any peace or public officer. The s. 487.018 production order for financial data is also available to compel a particular person or entity to disclose the identity of the account holder of a given account number. Search warrant under the provision of CC, s.487 is also available for peace and public officers to search any prescribed places for available information. However, the mechanism used to identify whether legal or natural persons hold or control accounts is not timely and deficient. In identifying whether a subject holds or controls accounts, law enforcement agencies will apply for a court order and serve it to the FI/DNFBP they reasonably suspect of holding such information and wait for the FI/DNFBP to respond. Each order can only be served to one specified FI/DNFBP. In urgent cases, the order can be drafted to obtain an initial response within days or otherwise it will take a longer time. The time required for such identification is considered not timely enough and the mechanism is not exhaustive to identify all accounts held with FIs/DNFBPs. LEAs may also use other informal processes, such as surveillance or FINTRAC disclosures, to identify the FIs/DNFBPs. These informal processes are sometimes lengthier and again not exhaustive to identify accounts held by the subject.

b) Warrants and production orders are normally obtained on an ex parte basis. If the order is directed to a third party, a condition may be added specifically to prohibit the third party from revealing the fact of the warrant to the account holders. Assistance Order, under CC, s.487.02, can also be applied by the law enforcement agencies to seek assistance from a person and request that he/she refrain from disclosing the information to the suspect.

Criterion 31.4—Most law enforcement agencies can ask for information from FINTRAC by submitting VIRs. FINTRAC is able, under PCMLTA, ss.55(3)(a) to (q) and 55.1(1)(a), to disseminate "designated information" by responding to these VIRs. However, these provisions do not allow other competent authorities such as Environment Canada or Competition Bureau conducting investigations of ML and associated predicate offenses to ask for information held by the FINTRAC.

Weighting and Conclusion

LEAs generally have the powers that they need to investigate ML/TF but there are some shortcomings. **Canada is largely compliant (LC) with R.31.**

Recommendation 32—Cash Couriers

In its 2008 MER, Canada was rated C for former SR IX (para 559–607).

Criterion 32.1—Canada has implemented a declaration system[61] for both incoming and outgoing physical cross-border transportation of currency and bearer negotiable instrument. A declaration is

61 Part 2 of the PCMLTFA.

required for all physical cross-border transportation, whether by travelers or through mail, courier and rail or by any other means of transportation. The declaration obligation applies to both natural and legal persons acting on their own and behalf of a third party, and applies to the full range of currency and BNI, as defined in the Glossary to the FATF Recommendations.

Criterion 32.2—The reporting of currency and bearer-negotiable instrument of an amount of Can$10,000 or more must be made in writing on the appropriate form and must be signed and submitted to a CBSA officer.[62] The reporting requirements of the PCMLTFA is met once the completed report is reviewed and accepted.

Criterion 32.3—This criterion is not applicable in the context of Canada, as it only applies to disclosure systems.

Criterion 32.4—Upon discovery of a false declaration of currency or BNIs, or a failure to declare, CBSA officers have the authority to request and obtain further information from the carrier with regard to the origin of the money and its intended use, as to ask for the documents supporting the legitimacy of the source of funds (Customs Act s.11).

Criterion 32.5—Under PCMLTFA, s.18, when persons make a false declaration or fail to make a declaration, CBSA officers have the power to seize as forfeit the currency or monetary instruments and to impose an administrative fine. The officer shall, on payment of a penalty in the prescribed amount (Can$250, Can$ 2,500, or Can$5,000, depending of the circumstances, including the particular facts and circumstances of any previous seizure(s) the individual has had under the PCMLTFA), return the seized currency or monetary instruments to the individual from whom they were seized or to the lawful owner. If the officer has reasonable grounds to suspect that the currency or monetary instruments are proceeds of crime within the meaning of CC, s.462.3(1) or funds for use in TF activities, there is no terms of release and the funds are forfeited. Overall, the administrative sanctions could appear to be nor proportionate and nor dissuasive for undeclared or falsely declared cross-border transportation of cash over the threshold.

Criterion 32.6—CBSA forwards all Cross-border Reports submitted by importers or exporters as well as seizure reports to FINTRAC electronically. If the currency or monetary instruments have been seized under PCMLTFA, s.18, the report is sent without delay to FINTRAC, in order to undertake an analysis on seizure information.

Criterion 32.7—CBSA officers undertake customs as well as immigration matters. Under PCMLTFA s. 36, CBSA is allowed to communicate information to FINTRAC, to the appropriate police force and to the CRA. Reports and seizure reports are systematically sent to the FIU and reports are communicated to the RCMP. The RCMP has a formal MOU with CBSA and a Joint Border Strategy which stipulates the roles and responsibilities of each partner and how they will cooperate.

62 The PCMLTFA Sec. 12(3) outlines who must report; this applies to conveyances regardless of mode (air; marine; rail; land; or postal).

Criterion 32.8—When persons make a false declaration or fail to make a declaration, CBSA officers have the power to seize as forfeit the currency or bearer negotiable instrument. No terms of release are offered on funds that are suspected to be proceeds of crime within the meaning of CC, s.462.3(1) or TF (PCMLTFA, s.18(2)). When an individual fully complies with the requirement to report on currency above the threshold, but there are reasonable grounds to believe the funds are related to ML/TF or predicate offenses, the CBSA contacts the RCMP who may carry out a seizure under the CC. The CBSA is empowered to restrain currency or BNIs for a reasonable time in order to allow the RCMP to ascertain whether evidence of ML/TF may be found, but there is no clear process is in place to engage any authority in ascertaining these evidences following false declaration or undeclared cross-border transportation of cash, nor where there is a suspicion of ML/TF or predicate offenses.

Criterion 32.9—False declaration leading to seizures of currency and bearer negotiable instruments are entered and maintained into the Integrated Customs Enforcement System. This information is also sent by CBSA to FINTRAC, which incorporates them into its database. These reports include information that must be provided in the mandatory reports.[63] Under PCMLTFA, ss.38 and 38.1, within an agreement or arrangement signed by the Minister, cross-border seizure reports where ML/TF is suspected are provided to foreign counterparts if the CBSA has reasonable grounds to suspect that the information would be relevant to investigating or prosecuting a ML or a TF offense, or within Custom Act s. 107 in accordance with an agreement. Declaration which exceeds the prescribed threshold are not retained by CBSA, but are forwarded to FINTRAC that should be in position to disclose CBCRs to its foreign counterparts, what may complicate international cooperation between customs regarding cash couriers.

Criterion 32.10—The information collected pursuant to the declaration obligation is subject to confidentiality.[64] There are no restrictions on the amount of money that can be imported into or exported from Canada; however, once the amount has reached or exceeded the threshold it must be reported.

Criterion 32.11—When there are reasonable grounds to believe the funds are related to ML/TF or predicate offenses, the CBSA contacts the RCMP who may carry out subsequent criminal investigation and laying of charges under the CC. If the suspicion is confirmed, seizure and confiscation measures may be decided by the judicial authority under the conditions described in R.4.

Weighting and Conclusion

There are some minor deficiencies. **Canada is largely compliant (LC) with R.32.**

[63] Including amount and type of currency or BNI, identifying information on the person transporting, mailing or shipping the currency or monetary instruments, as well as information on the person or entity on behalf of which the importation or exportation is made.

[64] PCMLTFA, article 36 and followings.

Recommendation 33—Statistics

In its 2008 MER, Canada was assessed as LC with former R.32 because the absence of statistical information on ML investigations and sentencing, confiscation, response times for extradition and mutual legal assistance (MLA) requests, response times for requests to OSFI by its counterparts. Some changes were introduced in the standard as well as in Canada.

Criterion 33.1—The compilation of AML/CFT related statistics are coordinated by Finance Canada and provided by all regime partners including FINTRAC, the RCMP, the PPSC and Statistics Canada at the federal and provincial level. The authorities maintain a comprehensive set of statistics that appears suitable to assist in the evaluation of the effectiveness of its AML/CTF framework. As a consequence of the NRA process, the authorities have improved the usefulness of existing data sets and developed new ones. The authorities intend to maintain the AML/CFT related statistics with a focus on periodically measuring the effectiveness of the AML/CFT regime.

Sub-criterion 33.1a—FINTRAC keeps statistics of STRs received and disseminated. Statistics on STRs received by regions is also available. Regarding the statistics provided on the dissemination of information by FINTRAC, it is unclear whether these disclosures derive from STRs, as required by the FCFT standard statistics related to the FIU.

Sub-criterion 33.1b—Canada maintains acceptable statistics regarding ML/TF investigations, prosecutions and convictions. Statistical data on ML, proceeds of crime and TF investigations and prosecutions is generated at the national, federal and provincial levels. It is generated from various sources, such as Statistics Canada's Uniform Crime Reporting Survey (UCR), the RCMP Occurrence Data (a records management system), the Public Prosecution Service's iCase, its case management and timekeeping system. The RCMP has employed its Business Intelligence program to provide statistical information on ML/TF investigations that is more detailed than UCR. This information is derived from the RCMP's various Operational Record Management Systems.

Sub-criterion 33.1c—Canada maintains statistics on assets seized, forfeited and confiscated as proceeds of crime and offense-related property (the equivalent of "instruments" or "instrumentalities" in other countries). However, there is no legal requirement for the AG to keep statistics on seizures.

Sub-criterion 33.1d—Statistics on made and received mutual legal assistance or other international requests for cooperation are maintained by the Department of Justice Canada. These statistics are used by Justice Canada to track the timeliness of response and the nature of underlying predicate crime.

Weighting and Conclusion

Canada is compliant (C) with R.33.

Recommendation 34—Guidance and Feedback

In its 2008 MER, Canada was rated LC with these requirements due to the lack of specific guidelines intended for sectors such as life insurance companies and intermediaries, and insufficient general feedback given outside the large FIs sector. There has been a substantial increase in guidance and feedback by Canadian authorities since the last MER.

Criterion 34.1—Canada provides guidance to industry on AML/CFT principally through regulators. FINTRAC provides guidance to both FIs and DNFBPs that is accessible on its website. A range of guidance has been published in the form of guidelines, trends and typologies reports, frequently asked questions, interpretation notices, sector specific pamphlets, brochures and information sheets on general topics such as the examination process. Guidance information is tailored to the different reporting sectors and deals with reporting, record-keeping, customer due diligence, general compliance information and questionnaires. Issues such as suspicious transaction reporting, terrorist property reporting, record-keeping, client identification, and implementing compliance regime to comply with AML/CFT obligations. Global Affairs Canada has issued guidance for countering proliferation (CP) sanctions regimes.

OSFI has a dedicated section of its website for AML/CFT and sanctions issues and it has issued prudential guidance that includes guidance on AML/CFT. A number of other guidelines issued by OSFI are either directly or indirectly applicable to AML/CFT requirements of the FRFI sector. In addition, OSFI's Instruction Guide Designated Persons Listings and Sanction Laws sets out OSFI's expectations for FRFIs when implementing searching and freezing CP and sanctions reporting obligations under the Criminal Code, UN Regulations and other sanctions laws. Other regulators such as IIROC have issued AML guidance to IIROC Dealer members in 2010. OSFI's guidance for FRFIs focuses on prudent risk management and internal controls to address the risk of ML and TF. It includes guidance on deterring and detecting ML and TF, background checks on directors and senior management, oversight of outsourced AML/CFT functions, corporate governance and screening of designated persons under the CC and UN Regulations. While FINTRAC is the main authority responsible for issuing AML/CFT guidance, other regulators also provide guidance on AML issues[65] and consult FINTRAC for policy interpretations.

Feedback is given by FINTRAC to industry through an outreach and assistance program for REs. This includes participating in conferences, seminars, presentations and other events providing feedback on compliance with AML/CFT legislation. REs can liaise with FINTRAC and OSFI by email or an enquiries telephone line. Each RE has a designated FINTRAC Compliance Officer to contact with any queries. FINTRAC's guidance and feedback to REs, in particular MSBs, is also reported as having increased significantly. The RCMP provides guidance through lectures to various businesses throughout Canada on recognizing and reporting suspicious transactions and has given conferences

[65] Quebec: AMF published a notice on AML/CFT requirements of their regulated entities; Nova Scotia Credit Union Deposit Insurance Corporation, Financial Institutions Commission of British Columbia, British Columbia Gaming Policy Enforcement Branch, Deposit Insurance Corporation Ontario, Prince Edward Island Credit Union Deposit Insurance Corporation have all published guidance on their websites.

and seminars on identifying, reporting, and investigating ML and materials produced by it on AML related issues.

Since 2008, Canada has provided guidance to the life insurance sector that is very similar to what is provided to other sectors. The guidance on AML/CFT provided by OSFI is applicable to all FRFIs subject to the PCMLTFA including life insurance companies. The guidance provided by FINTRAC is relevant to FIs and DNFBPs and there is sector specific guidance for the financial sector including life insurance companies and brokers and MSBs.

Weighting and Conclusion

There is more specific guidance needed in certain sectors. **Canada is largely compliant (LC) with R.34.**

Recommendation 35—Sanctions

In its 2008 MER, Canada was rated PC because: administrative sanctions were not available to FINTRAC; OFI used a limited range of sanctions; and effective sanctions had not been used in cases of major deficiencies. Several changes occurred since then, e.g., FINTRAC was granted the power to apply AMPs for non-compliance with the PCMLTFA.

Criterion 35.1—Civil and criminal sanctions are available in addition to remedial actions. FINTRAC is responsible for imposing AMPs for non-compliance with the PCMLTFA and its regulations.

The PCMLTFA and related legislation provide for penalties for non-compliance with AML/CFT measures. Part V of the PCMLTFA sets out penalties for non-compliance with the Act. The United Nations Act provides that, when the United Nations Security Council passes a resolution imposing sanctions, such measures automatically become part of domestic law, and sets out penalties for non-compliance with its provisions.

The PCMLTFA covers a range of criminal offenses and a series of sanctions for contraventions of the provisions of the Act. Criminal penalties for non-compliance can lead up to Can$2 million in fines and up to five years in prison. The criminal sanctions regime applies to most of the law and regulations provisions in the PCMLTFA. LEAs can conduct investigations and lay criminal charges in cases of non-compliance with the PCMLTFA.

The PCMLTF AMP Regulations govern the imposition of administrative sanctions for non-compliance with the PCMLTFA and related regulations. They provide for penalties, classifying violations as minor, serious or very serious. The maximum penalty for a violation by a person is set at Can$100,000 and for a RE it is Can$500,000. The imposition of a penalty is on a per violation basis: therefore, where there are multiple violations, an entity is potentially exposed to the maximum penalty for each individual violation. The maximum AMP thresholds for serious violations raises doubts whether it is proportionate or dissuasive (notwithstanding it relates to each instance of violation), given that there may be circumstances where a single egregious breach (or a few) may

occur and the cumulative threshold might not be either a proportionate or dissuasive sanction. The threshold may also not be dissuasive in circumstances of repeat offending.

There are also other non-monetary methods used by FINTRAC, in addition to the AMP procedure, to apply corrective measures or sanction REs, including issuing deficiency letters, action plans for FRFIs, compliance meetings and enquiries, public naming, revocation of registration of MSBs and non-compliance case disclosures to LEAs.

OSFI has a range of powers as set out in OSFI Act, s.6. OSFI can apply written interventions, staging (more intense/frequent supervision), put in place compliance agreements and directions of compliance, place terms and conditions on a FRFI's business operations and direct independent auditors to extend the scope of their audit and guidance, which are enforceable. The staging process, involving more intensive supervision of an FRFI, does have a dissuasive affect, as it attracts an increase in the deposit insurance premiums paid by the FRFI concerned. OSFI can also remove directors and/or officers from office, and/or take control of an FRFI in extreme cases of non-compliance with federal legislation, including the PCMLTFA. While OSFI does have the power to impose monetary penalties for non-compliance with general prudential provisions under an FRFI's governing legislation, violations of the PCMLTFA are dealt with by FINTRAC through the AMP procedure. OSFI has regulatory guidelines for AML compliance and background checks of directors and senior managers. OSFI cannot apply AMPs for non-compliance with the PCMLTFA.

Other regulators, such as securities regulators, can impose sanctions under securities legislation in circumstances where a market intermediary fails to meet legal requirements. The measures that can be taken include terminating the intermediary's license and imposing terms and conditions that restrict the intermediary's business. Sanctions can also be imposed on members for contraventions of self-regulatory organizations' requirements, including AML and supervision requirements.

Criterion 35.2—PCMLTFA, s.78 provides that sanctions are applicable to any officer, director, or agent of the person or entity that directed, assented to, acquiesced in, or participated in its commission.

Weighting and Conclusion

The dissuasiveness and/or proportionality of some of the sanctions is unclear. **Canada is largely compliant (LC) with R.35.**

Recommendation 36—International Instruments

Canada was rated LC with former R.35 and SR I in the 2008 MER, because the ML offense did not cover all designated categories of predicate offenses and contained a purposive element that was not broad enough to meet the requirements of the Conventions, and because of inadequate measures to ascertain the identity of beneficial owners.

Criterion 36.1—Canada is party to the conventions listed in the standard.[66]

Criterion 36.2—Bill C-48 amended to the CC to meet the requirements of the Merida Convention, especially by providing for the forfeiture of property used in the commission of an act of corruption and to clarify that it may be direct or indirect, and that it is not necessary that the person who commits the corrupt act receive the benefit derived from the act. Canada also addressed the deficiencies identified in 2008 (see R.3 and 10).

Weighting and Conclusion

Canada is compliant (C) with R.36.

Recommendation 37—Mutual Legal Assistance (MLA)

In its third MER, Canada was rated LC with former R.36 and SR. V due to concerns about Canada's ability to handle MLA requests in a timely and effective manner and about the lack of adequate data that would establish effective implementation. Canada's legal framework for MLA was supplemented by Canada's new Protecting Canadians from Online Crime Act (PCOCA, in force March 9, 2015). The requirements of the (new) R.37 are more detailed.

Criterion 37.1—Canada has a sound legal framework for international cooperation. The main instruments used are the Mutual Legal Assistance in Criminal Matters Act (MLACMA); the relevant international conventions, the Extradition Act; 57 bilateral treaties on MLA in criminal matters, extradition and asset sharing; and MOUs for the other forms of assistance to exchange financial intelligence, supervisory, law enforcement or other information with counterparts. These instruments allow the country to provide rapid and wide MLA. In the absence of a treaty, Canada is able to assist in simpler measures (interviewing witnesses or providing publicly available documents), or, based in the MLACMA, to enter in specific administrative arrangements, that would provide the framework for the assistance.

Criterion 37.2—Canada uses a central authority (the Minister of Justice, assisted by the International Assistance Group—IAG) for the transmission and execution of requests. There are clear processes for the prioritization and execution of mutual legal assistance requests, and a system called "iCase" is used to manage the cases and monitor progress on requests.

Criterion 37.3—MLA is not prohibited or made subject to unduly restrictive conditions. Canada provides MLA with or without a treaty, although MLA without a treaty is less comprehensive. Requests must meet generally the "reasonable grounds to believe standard, in relation for example to MLACMA ss.12 (search warrant) and 18 (production orders). However, certain warrants (financial

[66] Canada ratified the Vienna Convention on July 5, 1990, the Palermo Convention on May 13, 2002, and the Merida Convention on October 2, 2007, the Convention on the Suppression of Terrorist Financing Convention on February 19, 2002, and the Inter-American Convention against Terrorism. It has also signed the Council of Europe Convention on Cybercrime (2001) on November 23, 2001.

information, CC, s.487.018, tracing communications, and new s.487.015) may be obtained on the lower standard of "reasonable ground to suspect."

Criterion 37.4—Canada does not impose a restriction on MLA on the grounds that the offense is also considered to involve fiscal matters, nor on the grounds of secrecy or confidentiality requirements on FIs or DNFBPs.

Criterion 37.5—MLACMA, s.22.02 (2) states that the competent authority must apply ex parte for a production order that was requested in behalf of a state of entity. In addition to that, the international Conventions signed, ratified and implemented by Canada include specific clauses requiring the confidentiality of MLA requests be maintained.

Criterion 37.6—Canada does not require dual criminality to execute MLA requests for non-coercive actions.

Criterion 37.7—Dual criminality is required for the enforcement of foreign orders for restraint, seizure and forfeiture or property situated in Canada. MLACMA, ss.9.3 (3) (a) and (b) and 9.4 (1) (3) (5) (a) (b) and (c) allow the Attorney General of Canada to file the order so that it can be entered as a judgment that can be executed anywhere in Canada if the person has been charged with an offense within the jurisdiction of the requesting state, and the offense would be an indictable offense if it were committed in Canada. This applies regardless of the denomination and the category of offenses used.

Criterion 37.8—Most, but not all of the powers and investigative techniques that are at the Canadian LEAs' disposal are made available for use in response to requests for MLA. The relevant powers listed in core issue 37.1 are available to foreign authorities via an MLA request, including the compulsory taking of a witness statement (according to MLACMA, s.18). Search warrants are not possible to obtain via letters rogatory. However, the Minister may approve a request of a state or entity to have a search or a seizure, or to use any device of investigative technique (MLACMA, s.11). The competent authority who is provided with the documents of information shall apply *ex parte* for the warrant to a judge of the province in which the competent authority believes evidence may be found. Regarding the investigative techniques under core issue 37.2, undercover operations and controlled delivery are possible through direct assistance between LEAs from the foreign country and Canada. Production orders to trace specified communication, transmission data, tracking data and financial data are possible by approval of the Minister in response to a foreign request. The authorities will not grant interception of communications (either telephone, emails or messaging) solely on the basis of a foreign request (this special investigative technique is not provided for in the MLACMA and will not be provided for in bilateral agreements. According to MLACMA, s.8.1, requests made under an agreement may only relate to the measures provided for in the bilateral agreement). The only possibility to intercept communications is within a Canadian investigation in the case of organized crime, or a terrorism offense, which would require that the criminal conduct occurred, at least in part, in Canadian territory (including a conspiracy to commit an offense abroad). Foreign orders for restraint, seizure and confiscation can be directly enforced by the Attorney General before a superior court, as if it were a Canadian judicial order.

Weighting and Conclusion

The range of investigative measures available is insufficient. **Canada is largely compliant (LC) with R.37.**

Recommendation 38—Mutual Legal Assistance: Freezing and Confiscation

Canada was rated LC with R.38 in the 2008 MER due to the limited evidence of effective confiscation assistance, the rare occurrence of sharing of assets and the fact that Canada executed requests to enforce corresponding value judgments as fines. The framework remains the same.

Criterion 38.1—Canada has the authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize or confiscate laundered property and proceeds from crime (MLACMA, ss.9.3, 9.4 and CC, ss.462.32, 462.33), and instrumentalities used in or intended for use in ML, predicate offenses or TF. There is, however, no legal basis for the confiscation of property of corresponding value. As was the case during its previous assessment, Canada still treats value-based forfeiture judgement as fines, which has limitations and cannot be executed against the property. If the fine is not paid, it can be converted into a prison sentence. Regarding the identification of financial assets new CC, s.487.018 allows the production of financial registration data in response to requests from foreign states.

Criterion 38.2—In Canada, MLA is based on the federal power in relation to criminal law. Therefore, the enforcement of some foreign non-conviction based confiscation orders is not possible under the MLACMA because they were not issued by a "court of criminal jurisdiction." However, in cases where the accused has died or absconded before the end of the foreign criminal proceedings, the MLACMA applies because the matter would still be criminal in nature. Due to Canada's constitutional division of powers, the Government of Canada cannot respond to a request for civil forfeiture as such requests fall within the jurisdiction of Canada's provinces. However, most of the Canadian provinces have already adopted legislation on a civil confiscation regime. Even if Canada is not able to provide assistance to requests for cooperation based on NCB proceedings, non-conviction based confiscation is possible under Canadian law. Should a foreign state seek to recover assets from Canada though NCB asset forfeiture, it must hire private counsel to act on its behalf in the province where the property or asset is located.

Criterion 38.3—

a) No particular legal basis is required in Canada for the coordination of seizure and confiscation actions. It is a matter primarily for national and foreign police authorities at the stage of seizure. Thus, via direct police-to-police contact, arrangements are made in relation to any relevant case.

b) The Seized Property Management Act sets out the mechanisms for the management and, when necessary, the disposition of property restrained, seized and forfeited. The Minister of Public Works and Government Services is responsible for the custody and management of all property

seized at the federal level. The Minister may make an interlocutory sale of the property that is perishable or rapidly depreciating, or destroy property that has little or no value. Property seized in the provincial level is managed by the provincial prosecution services.

Criterion 38.4—Canada shares confiscated property on a mutual agreement basis, under the Seized Property Management Act, s.11. Canada has 19 bilateral treaties regarding the sharing and transfer of forfeited or confiscated assets and equivalent funds.

Weighting and Conclusion

The seizure and confiscation regime has a deficiency, which is the impossibility of confiscation of equivalent value. **Canada is largely compliant (LC) with R.38.**

Recommendation 39—Extradition

Canada was rated LC with R.39 in the 2008 MER, mostly because of the difficulties in establishing the delay element, due to insufficient statistical data. The legal framework remains unchanged.

Criterion 39.1—Canada is able to execute extradition requests in relation to ML/TF without undue delay. Statistics provided to this assessment have shown that at least 40 percent of the requests are executed on a timely basis, what shows that the existing legal framework allows for extraditions without delay.

a) Both ML and TF are extraditable offenses (Extradition Act, ss.3(1)(a) and (b) of the combined with CC, ss.83.02, 83.03, 83.04 and 462.31).

b) Canada has a case management system (iCase) and clear processes in place for timely execution of extradition including prioritization of urgent cases. The Extradition Act sets out timelines for specific steps to ensure minimal delays, and requires judges to set an early date for the extradition hearing when the person has been provisionally arrested (s.21(1)(b)(3)).

c) Canada does not place unreasonable or unduly conditions on the execution of extradition requests.

Criterion 39.2—Nationality does not constitute grounds for refusal to extradite under the Extradition Act, ss.44, 46, and 47 of the, but the Charter of Fundamental Rights and Freedoms gives Canadian citizens the right to remain in Canada. The Supreme Court decided in *U.S. v. Cotroni* that extradition is a reasonable limitation of the right to remain in Canada, and the decision whether to prosecute or not in Canada and allow the authorities in another country to seek extradition is made following consultations between the appropriate authorities in the two countries when various factors, including nationality, are considered in weighing the interests of the two countries in the prosecution. Historically, the result of most of these assessments has been to favor extradition, but when it is not, the Canadian citizen can be prosecuted in Canada.

Criterion 39.3—Dual criminality is required for extradition. It is not relevant whether the extraditable conduct is named, defined or characterized by the extradition partner in the same way as it is in Canada (Extradition Act, s.3(2)).

Criterion 39.4—Direct transmission of an extradition request to Canada's IAG or via Interpol is possible unless a treaty provides otherwise. Requests for provisional arrest may be made via Interpol by virtually all of Canada's extradition partners. The extradition process is simplified when the person consents to commit and surrender. Canada does not grant extradition based solely on a foreign warrant for arrest, such as in an Interpol Red Notice, or a foreign judgment, or in the absence of a treaty, based on reciprocity. There must be an assessment of the evidence, which takes place in the course of the judicial phase, which is followed by the Ministerial phase of the extradition proceedings.

Weighting and Conclusion

Canada is compliant (C) with R.39.

Recommendation 40—Other Forms of International Cooperation

In the 2008 MER, Canada was rated LC with these requirements (para. 1551–1612). The main deficiency raised was related to FINTRAC as a supervisory authority.[67]

General Principles

Criterion 40.1—Canada's competent authorities can broadly provide international cooperation spontaneously or upon request related to ML/TF.[68] Referring to FINTRAC as FIU, PCMLTFA allows the Centre to disclose information to a foreign FIU spontaneously and makes reference to a disclosure of designated information "*in response to a request*."

Criterion 40.2—

a) Competent authorities have the legal basis to provide international cooperation (see criterion 40.1).

b) Nothing prevents competent authorities from using the most efficient means to cooperate.

c) FINTRAC as a FIU and as a supervisor, OSFI, CBSA, and RCMP use clear and secure gateways, mechanism or channels for the transmission and execution of requests.

[67] *FINTRAC* as a supervisory authority had the legal capacity to exchange information with foreign counterparts but had not put the arrangements and agreements in place.

[68] FINTRAC as a FIU: *PCMLTFA*, section56; FINTRAC as a supervisory authority: *PCMLTFA*, section.65.1; RCMP: *Privacy Act and Memoranda of understanding or Letters of agreements*; CBSA: *PCMLTFA*, art.38 and 38.1 and *Custom Act*; OSFI: OSFI Act, section 22.

d) FINTRAC as an FIU has put in place processes for prioritizing and executing requests and answers in five business days if the Centre has transaction information in its database and FINTRAC as a supervisory authority processes the request and provides a response in a matter of days. In regard to TF, RCMP prioritize, assign and respond to such requests in the most efficient and effective manner on a National Level. It has not been established that LEA and supervisor authorities have clear procedures for the prioritization and timely execution of bilateral requests.

e) Competent authorities have clear processes for safeguarding the information received. FINTRAC policies and procedures for the safeguard of information apply to both the FIU and the supervisory side of FINTRAC. All supervisory information received by OSFI is subject to the same standard of confidentiality as domestic information (OSFI Act, s.22). RCMP has policies for handling requests and sharing or exchanging criminal intelligence and information with foreign partners and agencies (RCMP Operational Manual Chapter 44.1s).

Criterion 40.3—Under the Privacy Act, competent authorities need bilateral or multilateral arrangements to cooperate with foreign counterparts where a disclosure of personal information about an individual is involved. FINTRAC as a FIU, RCMP, and CBSA have signed a comprehensive network of MOUs and letters of agreement with foreign counterparts, but FINTRAC as a supervisory authority has entered into two MOUs so far. The Canadian authorities indicated that these bilateral agreements were signed mostly in a timely way. Examples of MOUs signed promptly have been provided to the assessors. The OSFI Act does not require that the Superintendent enter into a MOU with a foreign counterpart in order to be able to cooperate.

Criterion 40.4—FINTRAC provides feedback upon requests to its foreign counterparts on the use and usefulness of the information obtained (PCMLTFA, ss.56.2 and 65.1(3)). Canadian authorities indicated that FINTRAC generally provides feedback to its foreign counterparts on the usefulness of the information obtained within five to seven days. There is no restriction on OSFI's ability to provide feedback. There is no general impediment, which prevents Canada's LEAs from providing feedback regarding assistance received.

Criterion 40.5—Competent authorities do not prohibit or place unreasonable or unduly restrictive conditions on information exchange or assistance on any of the four grounds listed in this criterion.

Criterion 40.6—Competent authorities have controls and safeguards to ensure that information exchanged is used for the intended purpose for, and by the authorities, for whom the information was provided.[69]

Criterion 40.7—Competent authorities are required to maintain appropriate confidentiality for any request for cooperation and the information exchanged, consistent with data protection obligations

[69] *Privacy Act*—FINTRAC as a FIU: PCMLTFA, para 56 (3) and MOUs template; FINTRAC as a supervisory authority: PCMLTFA, s.65.1 (1) (b) and MOUs template; RCMP: Operational manual on information sharing; OSFI: OSFI Act, s.22.

Criterion 40.8—FINTRAC as an FIU, may conduct inquiries on behalf of foreign counterparts, by accessing its databases (all report types, federal and provincial databases maintained for purposes related to law enforcement information or national security, and publicly available information), under PCMLTFA, s.56.1(2.1). FINTRAC as a supervisory authority can conduct inquiries on behalf of foreign counterparts with which it has an MOU under PCMLTFA, ss.65.1(1)(a) and 65.1(2), but only two MOUs have been signed so far. The RCMP can use a number of criminal intelligence and police databases to conduct inquiries on behalf of foreign counterparts, under sharing protocols that aim at protecting the right to privacy of the individuals mentioned in the databases.

Exchange of Information Between FIUs

Criterion 40.9—FINTRAC exchanges information with foreign FIUs in accordance with the Egmont Group principles or under the terms of the relevant MOU, regardless of the type of its counterpart FIU. The legal basis for providing cooperation is in PCMLTFA, s.56(1), which stipulates that the Centre exchanges information if it has reasonable grounds to suspect that the information would be relevant to investigating or prosecuting a ML or TF offense, or an offense that is "*substantially similar to either offense*."

Criterion 40.10—FINTRAC provides feedback on the usefulness of information obtained, when feedback is specifically requested by foreign FIUs (PCMLTFA, s.56), and whenever possible as well as on the outcome of the analysis conducted, based on the information provided.

Criterion 40.11—FINTRAC have the power to exchange:

a) The information held in its database (c.40.8), which does not cover the scope of the information required to be accessible or obtainable directly or indirectly under R.29, as it does not include additional information from REs.

b) The information FINTRAC has the power to obtain or access directly or indirectly at the domestic level (c.40.8), subject to the principle of reciprocity.

Exchange of Information Between Financial Supervisors

Criterion 40.12—PCMLTFA, allows FINTRAC to enter into information sharing arrangements or agreements under new s.65(2) with any agency in a foreign state that has responsibility for verifying AML/CFT. OSFI has broad authority to share supervisory information with domestic and foreign regulators or supervisors of FIs, including SROs.

Criterion 40.13—FINTRAC, as the AML/CTF supervisor for entities covered by the PCMLTFA, has the authority to share with foreign supervisors the compliance-related information that FINTRAC has in its direct possession about the compliance of persons and entities. The information that FINTRAC may exchange with foreign supervisors is defined by "FINTRAC supervisory MOU Template." Canadian authorities indicated that FINTRAC can exchange information domestically available, including information held by FIs. As regards OSFI, under the OSFI Act a broad exemption is

provided under s.22(2) in favor of the exchange of supervisory information with any government agency or body that regulates or supervises FIs.

Criterion 40.14—

a) FINTRAC and OSFI do not require legislation to exchange regulatory information, and that they currently exchange such information. Examples were given by FINTRAC of cross-border cooperation with other regulators.

b) OSFI, under OSFI Act, s.22 can exchange supervisory information with foreign government agency or body that regulates or supervises FIs which meets this Criterion.

c) PCMLTFA, subsection 65.1 enables FINTRAC to exchange supervisory information with other supervisors about the compliance of persons and entities, record-keeping, and reports. Through its supervisory examinations and compliance assessment reports, FINTRAC normally obtains information on REs' internal AML/CFT procedures and policies, CDD, customer files and sample accounts and transaction information. FINTRAC is able to exchange this information with other supervisors. However, this possibility is limited to exchanges with counterparts who are MOU partners.

Criterion 40.15—FINTRAC can conduct inquiries on behalf of foreign counterparts with which it has an MOU under PCMLTFA, ss.65.1(1)(a) and 65.1(2).

Criterion 40.16—FINTRAC can enter into agreements or arrangement with other supervisors to exchange information pursuant to the PCMLTF.[70] Under such agreements or arrangements, there is an obligation to keep such information confidential and not further disclose the information. FINTRAC's tactical MOU sets out the requirements for use and release and confidentiality of information exchanged between financial supervisors. It is provided in the tactical MOU that information that has been exchanged will not be disclosed without the express consent of the requested authority. It is also provided that if an authority has a legal obligation to disclose information, it will notify and seek the consent of the other authority. OSFI can exchange information with other supervisors on the basis that such information satisfies the requirements of the Act and will be kept confidential.

Exchange of Information Between Law Enforcement Authorities (LEAs)

Criterion 40.17—Under article 44.1 of the RCMP Operational Manual on "Sharing of information with Foreign Law Enforcement," RCMP and other Canadian LEAs are able to exchange domestically available information with foreign counterparts for intelligence or investigative purposes relating to ML, associated predicate offenses or TF, including the identification and the tracing of proceeds and instrumentalities of crime. Nevertheless, CBSA does not retain CBCRs, which have to be obtained

[70] PCMLTFA, s.40 (c). PCMLTFA, s.65.1 (1) (b) also provides a limit on how the information can be used by both parties to a supervisory MOU. MOU Supervisory Template, Section 6 on Permitted Uses and Release of Exchanged Information, and Section 7 on Confidentiality are also relevant.

through international cooperation between FIUs, what could complicate their access by CBSA's foreign counterparts. PS works with other countries on national security, border strategies and countering crime, including ML and TF. PS also participates in a number of fora and initiatives to foster its international cooperation, including violent extremism and foreign fighters.

Criterion 40.18—Canadian LEAs can use the legislative powers available under the CC[71] and other Acts[72] including investigative techniques available in accordance with domestic law, to conduct inquiries and obtain information on behalf of foreign counterparts. However, it appears than the range of powers and investigative techniques that can be used by LEA to conduct enquiries and obtain information on behalf of foreign counterparts are very limited.[73] Both the PPOC and ML offense definitions allow that the offense need not to have occurred in Canada "so long as the act or omission anywhere that, if it had occurred in Canada, would have constituted a designated offence." Canada extensively cooperates with foreign law enforcement counterparts based on multilateral agreements in the context of Interpol and on bilateral MOUs.

Criterion 40.19—Canadian LEAs are able to form joint investigative teams to conduct cooperative investigations, and, when necessary, establish bilateral or multilateral arrangement to enable such joint investigations on the basis of RCMP Act (and the RCMP Operational Policy Chapter 15 provides guidance on joint forces operation). Joint Forces Operations (JFO) involve one or more police/enforcement agencies working with the RCMP on a continuing basis over a definite period. A JFO should be considered in major multi-jurisdictional cases that are in support of national priorities and must be consistent with the mandated responsibility of the particular resource.

Exchange of Information Between Non-Counterparts

Criterion 40.20—Under PCMLTFA, FINTRAC as a FIU and a supervisor may enter into an agreement or arrangement, in writing, with an institution or agency of a foreign state that "*has powers and duties, similar to those of the Centre*," which seems to exclude diagonal cooperation. Nevertheless, Canadian authorities indicate than when FINTRAC receives a request from a non-counterpart, the Centre address it either through its domestic partners or through the foreign FIU or supervisor. RCMP operational manual 44.1 outlines that sharing information will be managed on a case-by-case basis and there is no element that prevents RCMP to exchange information indirectly. OSFI has a broad ability to share information diagonally based on the wording of the OSFI Act, s.22. The "*any government agency that regulates or supervises FIs*" wording does not seem to limit disclosure to prudential regulators. However, OSFI would have to determine on a case-by-case basis whether such agency "*regulates or supervises FIs*." OSFI has shared information with foreign FIUs where they are also AML/CFT supervisors.

[71] CC, s.462.31 allows police to perform reverse sting operations to obtain information on ML cases and CC, s.462.32 to seize POC.

[72] Mutual Legal Assistance in Criminal Matters Act, RCMP Act and Canada Evidence Act.

[73] The only provisions which can be used allows police to perform reverse sting operations to obtain information on ML cases and to seize POC (CC, ss.462.31 and 462.32).

Weighting and Conclusion

There is room for improvement in regard to non-MLA international cooperation. **Canada is largely compliant (LC) with R.40.**

Summary of Technical Compliance—Key Deficiencies

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) Underlying the Rating**
1. Assessing risks and applying a risk-based approach	LC	• Lawyers, legal firms and Quebec notaries are not legally required to take enhanced measures to manage and mitigate risks identified in the NRA.
2. National cooperation and coordination	C	• The Recommendation is fully met.
3. Money laundering offense	C	• The Recommendation is fully met.
4. Confiscation and provisional measures	LC	• The legal provisions do not allow for the confiscation of property equivalent in value to POC.
5. Terrorist financing offense	LC	• CC, s.83.03 does not criminalize the collection or provision of funds with the intention to finance an individual terrorist or terrorist organization.
6. Targeted financial sanctions related to terrorism and TF	LC	• Persons in Canada are not prohibited from providing financial services to entities owned or controlled by a designated person or persons acting on behalf or at the discretion of a designated person. • No authority has been designated for monitoring compliance by FIs and DNFBPs with the provisions of the UNAQTR, CC and RIUNRST.
7. Targeted financial sanctions related to proliferation	LC	• No mechanisms for monitoring and ensuring compliance by FIs and DNFBPs with the provisions of the RIUNRI and RIUNRDPRK. • Little information provided to the public on the procedures applied by the Minister to submit delisting requests to the UN on behalf of a designated person or entity.
8. Non-profit organizations	C	• The Recommendation is fully met.
9. Financial institution secrecy laws	C	• The Recommendation is fully met.
10. Customer due diligence	LC	• Exclusion of financial leasing, factoring and finance companies from scope of AML/CTF regime. • Minor deficiency of existence of numbered accounts whose use is governed only by regulatory guidance. • Minor deficiency of limited application, to natural persons only, of requirements to reconfirm identity where doubts arise about the information collected. • No explicit legal requirements to check source of funds. • No requirement to identify the beneficiary of a life insurance payout. • Minor deficiency of exceptions to the timing requirements for verifying identity are not clearly

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) Underlying the Rating**
		justified in terms of what is reasonably practicable or necessary to facilitate the normal conduct of business. • Minor deficiency of the lack of a requirement to obtain the address and principal place of business of non-corporate legal persons and legal arrangements such as trusts.
11. Record keeping	LC	• The legal obligation requiring REs to provide records to FINTRAC within 30 days does not constitute "swiftly," as the standard specifies.
12. Politically exposed persons	NC	• Only one element of the FATF standard is currently largely met, although new legislation covering domestic PEPs will come into force in July 2016.
13. Correspondent banking	LC	• No requirement for a FI to assess the quality of AML/CFT supervision to which its respondent institutions are subject.
14. Money or value transfer services	C	• The Recommendation is fully met.
15. New technologies	NC	• No explicit legal or regulatory obligation to risk assess new products, technologies and business practices, before or after their launch.
16. Wire transfers	PC	• No specific requirements for intermediary and beneficiary FIs to identify cross-border EFTs that contain inadequate originator information, and take appropriate follow-up action. These are significant deficiencies.
17. Reliance on third parties	PC	• No explicit requirements on life insurance entities and securities dealers in relation to either necessary CDD information to be provided by the relied-upon entity or supervision of that entity's compliance with CDD and record-keeping obligations. • No requirements on life insurance entities or securities dealers to assess which countries are high risk for third party reliance.
18. Internal controls and foreign branches and subsidiaries	LC	• No specific legal requirements in relation to screening procedures when hiring employees.
19. Higher-risk countries	C	• The Recommendation is fully met.
20. Reporting of suspicious transactions	PC	• Minor deficiency that financial leasing, finance and factoring companies are not required to report suspicious activity to FINTRAC. • Lack of a prompt timeframe for making reports.
21. Tipping off and confidentiality	LC	• The tipping off and confidentiality requirements do not explicitly extend to the reporting of suspicions related to ML predicate offenses.

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) Underlying the Rating**
22. DNFBPs: Customer due diligence	NC	• AML/CFT obligations are inoperative for legal counsels, legal firms and Quebec notaries. • On line gambling, TCSPs that are not trust companies are not obliged entities. • No requirement on beneficial owner, PEP, new technologies, reliance on third parties. With the exception of a limited set of transactions the fixed threshold (Can$10,000) of cash financial transactions and casinos disbursement exceeds that provided in the Recommendation. • The circumstances in which accountants and BC notaries are required to perform CDD are not in line with the FATF requirement.
23. DNFBPs: Other measures	NC	• AML/CFT obligations are inoperative for legal counsels, legal firms and Quebec notaries. • TSCPs that are not trust and loan companies and on line gambling are not subject to the AML/CFT obligations; the circumstances under which accountants and BC notaries are required to comply with STRs are too limitative. • Further deficiencies identified under R.20 for DNFBPs that are subject to the requirements.
24. Transparency and beneficial ownership of legal persons	PC	• No appropriate mechanism to ensure that updated and accurate beneficial ownership information is collected for all legal entities in Canada, whether established under provincial or federal legislation. • Timely access by competent authorities to all beneficial ownership information is not warranted, in particular in cases where such information is held by a smaller or provincial FI, or a DNFBP. • Insufficient risk mitigating measures in place to address the ML/TF risk posed by bearer shares and nominee shareholder arrangements. • No obligation for legal entities to notify the registry of the location at which company records are held. • In some provinces, there is no legal obligation to update registered information within a designated timeframe. • No legal obligation on legal entities to authorize one or more natural person resident in Canada to provide to competent authorities all basic information and available beneficial ownership information; or to authorize a DNFBP in Canada to provide such information to the authorities.

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) Underlying the Rating**
25. Transparency and beneficial ownership of legal arrangements	NC	• No obligation for trustees to obtain and hold adequate, accurate and current beneficial ownership information for all legal arrangements in Canada, whether established under provincial or federal legislation, or basic information on other regulated agents or and service providers to the trust. • Professional trustees, including lawyers, are not required to maintain beneficial ownership information for at least five years. • Insufficient mechanism in place to facilitate timely access by competent authorities to all beneficial ownership information and any trust assets held or managed by the FI or DNFBP. • No requirement for trustees to proactively disclose their status to FIs and DNFBPs when forming a business relationship or carrying out a financial transaction for the trust. • Proportionate and dissuasive sanctions for a failure by the trustee to perform his duties are not available in most cases.
26. Regulation and supervision of financial institutions	LC	• There are further fitness and probity controls needed for persons owning or controlling financial entities after market entry at provincial level.
27. Powers of supervisors	C	• The Recommendation is fully met.
28. Regulation and supervision of DNFBPs	PC	• AML/CFT obligations are inoperative for legal counsels, legal firms and Quebec notaries. • Online gambling, cruise ship casinos, TSCPs not included among trust and loan companies are not subject to AML/CFT obligations and thus not monitored for AML/CFT purposes. • The entry standards and fit and proper requirements are absent in DPMS and TCSPs than trust companies, and they are not in line with the standards for real estate brokerage.
29. Financial intelligence units	PC	• FINTRAC is not empowered to request further information to REs. • FINTRAC has a limited or incomplete access to some administrative information (e.g., fiscal information). • FINTRAC is not able to disseminate upon request information to some authorities (e.g., Environment Canada, Competition Bureau).
30. Responsibilities of law enforcement and investigative authorities	C	• The Recommendation is fully met.

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) Underlying the Rating**
31. Powers of law enforcement and investigative authorities	LC	• No mechanism in place to timely identify whether a natural or legal person holds / controls accounts. • No power to compel a witness to give statement in ML investigation. • Only LEAs can ask for designated information from FINTRAC.
32. Cash couriers	LC	• Administrative sanctions are not proportionate, nor dissuasive. • It has not been established that a clear process was in place to analyze or investigate cross-border seizures. • Cross-border currency reports are not retained by CBSA and can only be exchanged with foreign Customs authorities through FIUs' international cooperation.
33. Statistics	C	• The Recommendation is fully met.
34. Guidance and feedback	LC	• There is more specific guidance needed in certain sectors such as DNFBPs to ensure that they are aware of their AML/CFT obligations, the risks of ML/TF and ways to mitigate those risks. There is also further feedback required arising out of the submitting of STRs.
35. Sanctions	LC	• The maximum threshold of administrative sanctions raises doubts about the dissuasiveness of sanctions for serious violations or repeat offenders.
36. International instruments	C	• This Recommendation is fully met.
37. Mutual legal assistance	LC	• The MLACMA does not allow for the interception of communications (either telephone or messaging) based solely on a foreign request, what hampers foreign investigations.
38. Mutual legal assistance: freezing and confiscation	LC	• Canada cannot respond to requests for the seizure and confiscation of property of corresponding value.
39. Extradition	C	• The Recommendation is fully met.
40. Other forms of international cooperation	LC	• The impediments raised in R.29 for FINTRAC, notably the fact that the FIU is not empowered to request further information from REs and the fact that some RE are not requested to fulfil STRs, impacts negatively the international cooperation with its counterparts. • LEAs are not able to use a large range of powers and investigative techniques to conduct inquiries and obtain information on behalf of foreign counterparts.