Future of Financial Intelligence Sharing (FFIS)

FFIS Briefing Paper – Canada in Context:

Canadian Legislation, Supervision and Operational Processes for Information-Sharing to Detect Money Laundering and Underlying Crime, set in the Context of International Practices

A briefing paper submission to the Commission of Inquiry into Money Laundering in British Columbia

Author. Nick J Maxwell, Head of the FFIS Programme

Submission on: 4 January 2021, updated 11 December 2021

This Briefing Paper is produced by the Future of Financial Intelligence Sharing (FFIS) programme at the invitation of the Commission of Inquiry into Money Laundering in British Columbia.

This document contains:

- An 'Overview of Findings', which brings together all the report's key points and recommendations (pages 3 - 33);
- A 'Reference Annex', with comprehensive supporting material, individual key points raised in interviews, additional contextual analysis of the Canadian regime, national and international case studies to support the key points and recommendations (pages 34 - 124); and
- A reproduction of a 2018 FFIS survey of Canadian AML/ATF information sharing permissibility (pages 126 to 133).

'Section 4 Principal challenges in the Canadian AML/ATF information-sharing regime and relevant international practices addressing similar challenges in comparable jurisdictions.' (page 9 to 27) effectively summarises the entire report.

Every effort has been made to verify the accuracy of the information contained in this report. All information was believed to be correct as of 18 December 2020. Nevertheless, the FFIS programme cannot accept responsibility for the consequences of its use for other purposes or in other contexts. The views and recommendations expressed in this publication are those of the author and do not reflect the views of any other institution.

Contents

OVERVIEW OF FINDINGS **3**

1. About the FFIS programme 3
2. Background to this policy paper 4
3. Methodology: 5
4. Principal challenges in the Canadian AML/ATF information-sharing regime and comparable international practices. 9
5. Key themes relevant to enhancing the Canadian AML/ATF information-sharing framework. 27
6. Inter-relationship of financial information-sharing themes: 29
7. Opportunities to enhance the Canadian framework 30

REFERENCE ANNEX **34**

A1. What are public–private financial information-sharing partnerships? 34

A2. Why focus on information sharing? 34

A3. How have partnerships developed around the world? 35

A4. What type of information is shared? 36

A5. How are AML supervisors involved? 37

A6. Overview of Canadian financial information-sharing partnership arrangements 39

A7. The Canadian Proceeds of Crime (Money Laundering) and Terrorist Financing Legislative Landscape 43

A8. The Canadian privacy regime 44

A9. Key identified strengths within the Canadian AML/ATF financial information sharing regime 48

A10. Overview of challenges to the effectiveness of the Canadian regime identified in this paper 49

Theme 1. Data to understand the effectiveness and efficiency of the AML/ATF system 52

Theme 2. A strategic understanding of threats and a strategic approach to addressing economic crime 65

Theme 3. Prioritisation of economic crime threats 81

Theme 4. Public-private tactical financial information-sharing 92

Theme 5. The extent of public/private co-production of strategic financial intelligence 103

Theme 6. Relevance to law enforcement outcomes 108

Theme 7. Private-private financial information sharing to detect crime 115

Theme 8. Mitigation of the negative impacts of account closures. 120

Supplementary Information: Reproduction of public sector responses to RUSI FFIS survey on AML/ATF information sharing permissibility in Canada (May 2018) 126

OVERVIEW OF FINDINGS

1. About the FFIS programme and previous relevant research and events in Canada:

The FFIS research programme is partnership between NJM Advisory and the Royal United Services Institute (RUSI) Centre for Financial Crime and Security Studies. Since 2017, the role of the FFIS programme has been to support research and events that examine evidence related to the effectiveness, proportionality and efficiency of public–private financial information-sharing partnerships and share good practice between existing partnership models around the world.

The FFIS programme has published four international comparative studies of public–private financial information-sharing partnerships, produced a number of national-level papers and convened over 50 events worldwide, as part of its research agenda.

In the most recent paper, "Five years of growth in public–private financial information-sharing partnerships to tackle crime"[1], published in August 2020, the FFIS programme surveyed public–private financial information-sharing initiatives developed around the world between 2015 and 2020.

The FFIS programme has a significant background of research and events in Canada and all FFIS international comparative publications since 2017 have included case studies from Canada.

FFIS major research events convened in Canada include:

i) In December 2019, the FFIS programme hosted a cross-government workshop in Ottawa to investigate the potential of advances in privacy preserving analytics in the Canadian context.

ii) On 10 June 2019, FFIS hosted a major conference in Toronto on bringing together:

- Financial Transactions and Reports Analysis Centre of Canada (FINTRAC); Department of Finance Canada; Royal Canadian Mounted Police, Office of the Superintendent of Financial Institutions, Government of Canada; Canada Revenue Agency; Canadian Centre for Cyber Security; Department of Public Safety and Emergency Preparedness; Canadian Security Intelligence Service (CSIS); Statistics Canada; Department of Justice Canada, Government of Canada; Innovation, Science and Economic Development Canada; Office of the Privacy Commissioner of Canada; Canadian Bankers Association (CBA); and a wide range of private sector entities and major financial institutions.

[1] https://www.gcffc.org/survey-report-five-years-of-growth-in-public-private-financial-information-sharing-to-tackle-crime/

The conference provided a forum for:

- Recent developments to improve public/private information sharing in Canada to detect, analyse, deter and disrupt crime.
- Exploring examples from international experiences of public/private information-sharing and the relevance to the Canadian domestic context.
- Sharing perspectives on the impact, value, limitations and challenges arising from recent Canadian information-sharing initiatives.
- Identifying lessons from both Canadian and international public/private information-sharing to instruct future activity.
- Clarifying understanding about technological developments relevant to financial information sharing and advanced analytics, including related to privacy preserving analytics and machine learning.
- Exploring comparable examples of information-sharing capabilities related to cyber security and fraud prevention.
- Identifying the opportunity for greater coherence across financial crime, fraud and cyber information-sharing processes.
- Achieving a common understanding of threats, shared priorities and coordinated action;
- Collaborative development of strategic understanding to financial crime threats;
- Tactical information-sharing (public/private and private/private information-sharing); and
- The potential of a whole of government approach to tackling financial crime through information-sharing in accordance with basic Canadian Charter rights.

iii) In April and May 2018, the FFIS programme conducted a wide-ranging survey, with the support of the Department of Finance, covering public sector interpretations of the legal and regulatory framework for information sharing in Canada. This survey was discussed over two roundtable events, in Toronto and Ottawa respectively, in May 2018.

2. Background to this policy paper:

The study has been prepared at the request of the Commission of Inquiry into Money Laundering in British Columbia (‘The Commission’).

The Commission responds to a perception amongst the public that “money laundering is flourishing” in British Columbia with a mandate is to make findings of fact related to:[2]

i. the extent, growth, evolution and methods of money laundering in British Columbia, with regard to specific economic sectors;
ii. the acts or omissions of responsible regulatory agencies and individuals, and whether those have contributed to money laundering in the province or amount to corruption;
iii. the scope and effectiveness of the anti-money laundering powers, duties and functions of these regulatory agencies and individuals; and
iv. the barriers to effective law enforcement in relation to money laundering.

In addition, the Commission has the responsibility to make recommendations to address the conditions which have enabled money laundering to flourish.

[2] https://cullencommission.ca/comm-statements/

In response to the Commission’s mandate, this paper aims to achieve the following objectives:

a) To describe recent international developments to enhance the effectiveness of national Anti-Money Laundering/Anti-Terror Financing (AML/ATF) regimes, with a particular emphasis on the systemic challenges that have been identified and the role of public–private and private–private financial information sharing to respond to those challenges;
b) To analyse Canada’s current processes, regulatory regime and legislative provisions for information-sharing to detect money laundering and underlying crime;
c) To identify both strengths and limitations of the Canadian AML/ATF regime to leverage public–private collaboration to address crime, relative to current practices in similar countries; and
d) To raise key opportunities to enhance the Canadian national AML/ATF regime.

3. Methodology:

Between September and December 2020, this paper has been developed through the following research process:

- Literature review, open-source research and updating previous Canada-focused FFIS research material including the 2018 survey and 2019 workshop events;

- Research interviews throughout November and December 2020 with:
    - Covering all ‘Big 6’ financial institutions in Canada, interviews with 7 senior decision-makers in respective AML/Financial Crime departments;
    - 2 senior individuals from multi-national reporting entities operating in Canada (non-‘Big 6’);
    - 7 senior individuals from financial crime consultancy firms, including with smaller financial institutions, credit unions, and non-financial sectors as clients in AML advisory programmes.

  The study largely revolves around effectiveness challenges identified by private-sector reporting entities or AML consultants in Canada.

- In reference to non-Canadian case studies included in this report, the author again conducted a literature review and led 12 interviews with decision-makers involved in non-Canadian financial crime detection, information-sharing or economic crime policy reform projects. Over the course of this research period, the author participated in a large number of virtual workshop and roundtable events relevant to international case studies referenced in this document.

- Desktop analysis of the Canadian AML/ATF information-sharing framework, in relation to key themes relevant to the Commission’s interest and in comparison to international practices and case studies.

The initial scope of AML/ATF information-sharing effectiveness topics for this research was informed by the 12 key themes previously identified in the FFIS 2020 international survey of public-private financial information-sharing partnerships.

Key themes relevant to information-sharing partnership growth and related AML/ATF effectiveness, as identified in the FFIS 2020 international survey.[3]

i. The adequacy of legal gateways for information-sharing and respective policy reform processes;
ii. How partnerships prioritise threats and how knowledge is exchanged within and between partnerships on specific threats;
iii. Opportunities to enhance the impact of partnership strategic intelligence products, including options for supervisory recognition of partnership strategic intelligence products;
iv. Partnership status within mainstream AML/ATF supervision, including the implications of partnership membership from a supervisory perspective, the integration of priorities of partnerships in a risk-based approach and the potential implications of mandatory participation in partnership activities;
v. The capacity for membership growth within partnerships and corresponding information-security considerations, including across multiple regulated sectors;
vi. The use of technology in partnerships, including privacy preserving analysis;
vii. Pathways to enhance the benefit of partnerships to other regulated entities, outside of partnership members;
viii. Managing risk-displacement brought about by partnerships to non-partnership members;
ix. Measuring and evaluating the performance of partnerships;
x. The link between public–private partnerships with private–private information sharing;
xi. Governance, accountability and transparency of partnerships; and
xii. Cross border collaboration between public–private financial information sharing partnerships.

During the course of the research, the scope of this study was refined further to be responsive to the challenges raised during interviews by key stakeholders in reporting entities (REs) in Canada.

As a result of that process, the challenges and international comparisons in this study are framed around the following **themes of AML/ATF information-sharing**:

- Theme 1. Data to understand the effectiveness and efficiency of the AML/ATF system;
- Theme 2. A strategic understanding of threats and a strategic approach to addressing economic crime;
- Theme 3. Prioritisation of economic crime threats;
- Theme 4. Public-private tactical financial information-sharing;
- Theme 5. The extent of public/private co-production of strategic financial intelligence;
- Theme 6. Relevance to law enforcement outcomes;
- Theme 7. Private-private financial information sharing to detect crime; and
- Theme 8. Mitigating the negative impacts of account closures.

[3] https://www.gcffc.org/survey-report-five-years-of-growth-in-public-private-financial-information-sharing-to-tackle-crime/

Due to these choices relating to the scope of the study, the author recognises that a wide range of relevant factors to AML/ATF effectiveness fall outside of the scope of the report, such as:

a) Firm-level preventative measures, including as relevant to onboarding process, know your customer checks (KYC), ongoing Customer Due Diligence (CDD), Enhanced Due Diligence (EDD), and related data quality issues within REs;
b) Corporate and trust beneficial ownership transparency;
c) The regulation of Designated Non-Financial Businesses and Professions (DNFBPs) in Canada;
d) The Canadian (foreign policy) sanctions regime;
e) Law enforcement and FINTRAC resources;
f) Law enforcement and FINTRAC technical and personnel resources and capacity building;
g) The adequacy of coercive powers for law enforcement or offences related to money laundering;
h) Cross-border information sharing arrangements;
i) The range of sector specific issues that may be relevant outside of retail banking and money service businesses (MSBs);
j) Specific policy issues related to new fintech, virtual assets or payments technologies;
k) Any threat specific considerations, such as terrorist financing, proliferation financing, human trafficking etc.

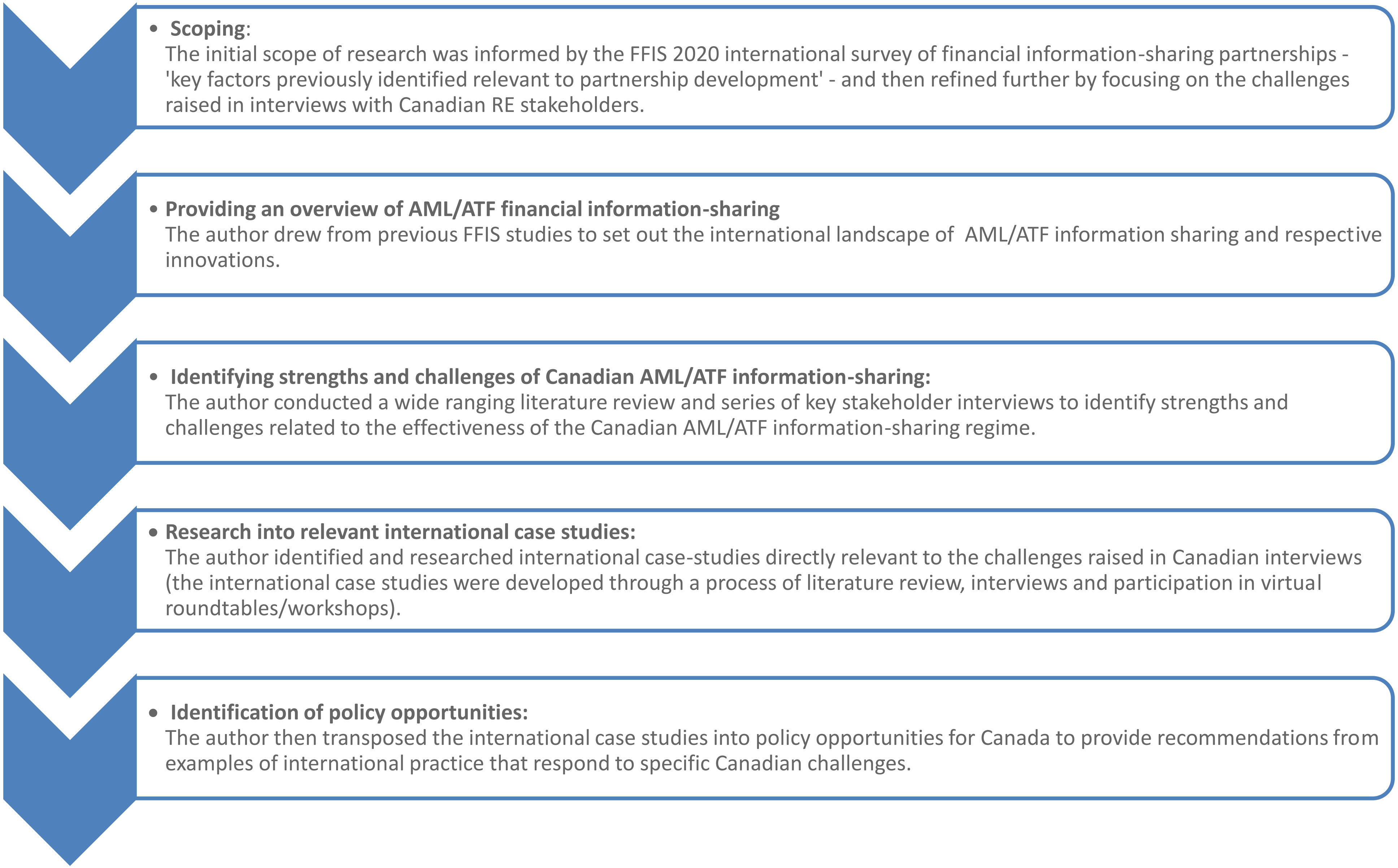
In general, the scope of threat activity that we consider in this paper is **'economic crime',** and we use the same definition as laid out in the 'UK Economic Crime Plan 2019-2022'[4], i.e. that economic crime refers to a broad category of activity involving money, finance or assets, the purpose of which is to unlawfully obtain a profit or advantage for the perpetrator or cause loss to others. The definition is broader than 'financial crime' or 'white-collar crime' and is used to provide a holistic response to the following types of criminality:

- fraud against the individual, private sector and public sector
- terrorist financing
- sanctions contravention
- market abuse
- corruption and bribery
- the laundering of proceeds of all crimes
- The recovery of criminal and terrorist assets is also in scope.

In terms of sectoral coverage, the paper is primarily concerned with the banking and MSB sectors and how regulated entities (REs) within those sectors interact with public sector agencies through public/private and private/private financial information sharing within the domestic Canadian AML/ATF regime. In the study we refer to "RE" ('RE' for one or 'REs' for two or more) interviewee comments to mean either a reporting entity directly or a perspective shared by an AML consultancy representing insights formed from advising multiple REs across different sectors in Canada. Recommendations or 'opportunities' expressed in this paper reflect the authors' proposals and opinions only and should not be taken to reflect the views of RUSI, the institutions, or specific individuals that participated in this research process.

[4] https://www.gov.uk/government/publications/economic-crime-plan-2019-to-2022/economic-crime-plan-2019-to-2022-accessible-version

Our approach in this study:



- **Scoping**:
The initial scope of research was informed by the FFIS 2020 international survey of financial information-sharing partnerships - 'key factors previously identified relevant to partnership development' - and then refined further by focusing on the challenges raised in interviews with Canadian RE stakeholders.

- **Providing an overview of AML/ATF financial information-sharing**
The author drew from previous FFIS studies to set out the international landscape of AML/ATF information sharing and respective innovations.

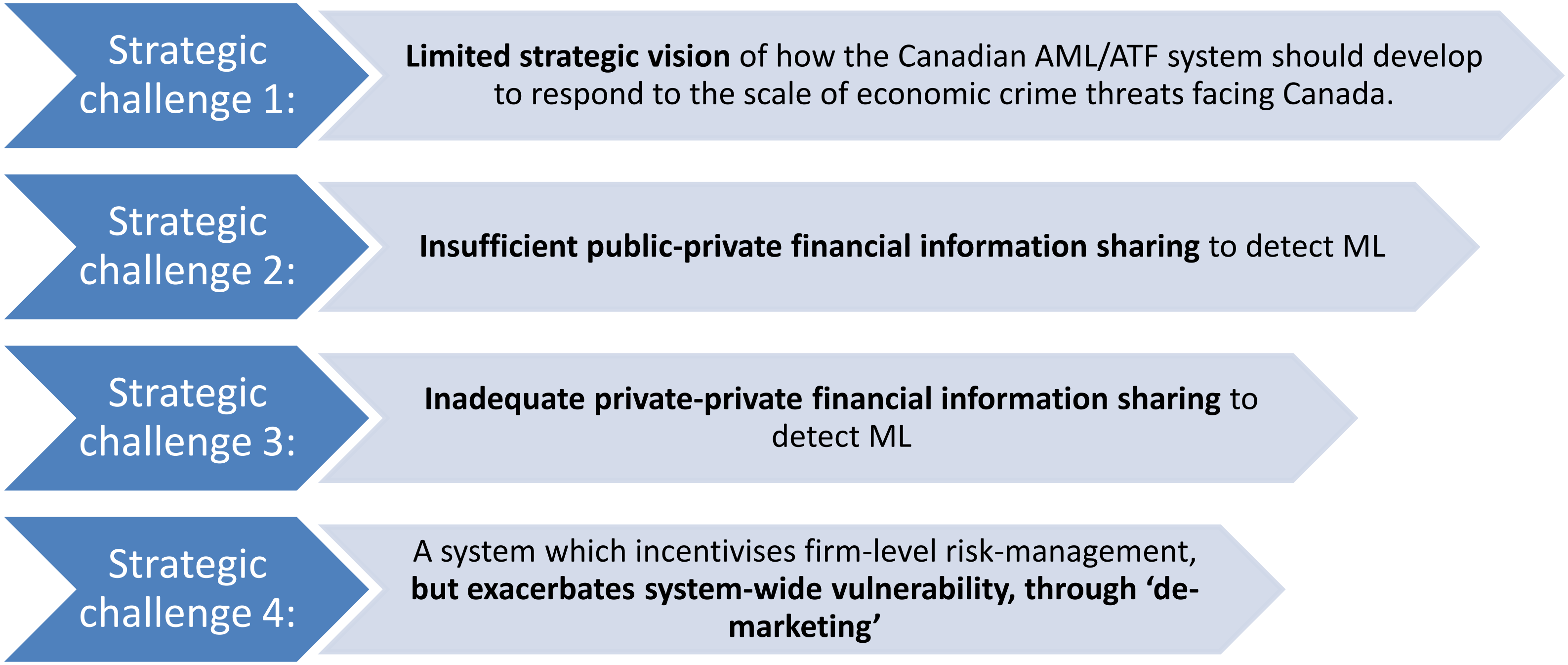
- **Identifying strengths and challenges of Canadian AML/ATF information-sharing:**
The author conducted a wide ranging literature review and series of key stakeholder interviews to identify strengths and challenges related to the effectiveness of the Canadian AML/ATF information-sharing regime.

- **Research into relevant international case studies:**
The author identified and researched international case-studies directly relevant to the challenges raised in Canadian interviews (the international case studies were developed through a process of literature review, interviews and participation in virtual roundtables/workshops).

- **Identification of policy opportunities:**
The author then transposed the international case studies into policy opportunities for Canada to provide recommendations from examples of international practice that respond to specific Canadian challenges.

4. Principal challenges in the Canadian AML/ATF information-sharing regime and relevant international practices addressing similar challenges in comparable jurisdictions.

Overall, the principal challenges in the Canadian AML/ATF information-sharing regime identified in this study are as follows:



Strategic challenge 1: **Limited strategic vision** of how the Canadian AML/ATF system should develop to respond to the scale of economic crime threats facing Canada.

Strategic challenge 2: **Insufficient public-private financial information sharing** to detect ML

Strategic challenge 3: **Inadequate private-private financial information sharing** to detect ML

Strategic challenge 4: A system which incentivises firm-level risk-management, **but exacerbates system-wide vulnerability, through 'de-marketing'**

The following section summarises key points identified in this study through interview and additional desktop analysis of available published material; including Canadian factors contributing towards the respective strategic challenges, set against any qualifications or recent developments relevant to that factor. Following each strategic challenge, international case studies relating to how comparable jurisdictions have addressed a similar challenge factor (or information-sharing theme) are set out in summary. Full reference information for both challenge factors and case studies are included in the Reference Annex.

Strategic challenge 1: Limited strategic vision

Limited strategic vision of how the Canadian AML/ATF system should develop to respond to the scale of economic crime threats, recognising the effectiveness and efficiency challenges in the AML/ATF system and clarifying the associated public-private and private-private information-sharing requirements to reach a target operating model.

Factors contributing to the strategic challenge	Qualifications / additional context / recent developments
The national AML/AFT system is evaluated by FATF, approximately once a decade, and by Parliamentary scrutiny once every five years. Outside of the FATF evaluation, existing publicly-available performance information on the Canadian AML/ATF regime is not sufficient to inform an understanding of the effectiveness of the regime (on an outcomes-basis).	However, FINTRAC has delivered year-on-year improvements to the level of detail and scope of its reporting in the FINTRAC Annual Report. The strategic information gaps in the effectiveness of the Canadian regime are largely outside of FINTRAC's organisational responsibility. The Department of Finance reports annually to Parliament on spending and largely activity-based performance of various agencies in the AML/ATF Regime from 2000-2019. The most recent Canadian Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) statutory review 'Confronting Money Laundering and Terrorist Financing: Moving Canada Forward' (published in 2018)[5] is a wide-ranging document that identifies many areas for strategic improvement. The Canadian government describes this as the "roadmap to respond to current and future threats."[6] To support the statutory review, the government of Canada published a consultation paper in 2018 to strengthen Canada's AML/ATF regime 'Reviewing Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime'.[7] The Canadian 2019 budget provided funding to the ACE (Anti-money laundering action and co-ordination) Fusion Team of CAD$24 million. FFIS understands that ACE Fusion will be prioritising the development of a performance measurement framework that strengthens reporting of activities and outcomes. FINTRAC facilitated brainstorming session at outreach sessions with key stakeholders during the sixth Major Reporters Forum (in February 2020) to improve the effectiveness of the AML/ATF regime.[8]

[5] https://www.ourcommons.ca/Content/Committee/421/FINA/Reports/RP10170742/finarp24/finarp24-e.pdf

[6] https://www.budget.gc.ca/2019/docs/plan/budget-2019-en.pdf

[7] https://www.dentons.com/en/insights/articles/2018/march/15/reviewing-canadas-anti-money-laundering-and-anti-terrorist-financing-regime

[8] https://www.fintrac-canafe.gc.ca/publications/drr-rrm/2019-2020/drr-rrm-eng

The most recent National Inherent Risk Assessment in Canada pre-dates the FATF evaluation and has not been revised since the FATF evaluation (and is five years out of date). The range of publicly available threat assessments produced by the government of Canada about economic crime threats facing Canada is inadequate to understand the scale and nature of economic crime threats facing Canada.	However, according to the FINTRAC Department Results Report 2019-20, FINTRAC, through the National Inherent Risk Assessment Working Group, has focused on sectoral risk assessments. FINTRAC's 2018 Terrorist Financing Threat Assessment, Operational Alerts and Briefs, STR Guidance and Risk-Based Assessment Guidance have all been published on its website. These documents all inform reporting entities on the various threats, typologies and indicators of ML/TF.
Beyond industry estimates, there are no official estimates for the cost of compliance by the private sector with the Canadian AML/ATF regime. Accordingly, there is no evidence of Canadian authorities seeking to ensure the cost-effectiveness of the Canadian AML/ATF regime, nor seeking to encourage private sector resources to be allocated in the most efficient way to support the desired outcomes of the AML/ATF system.	There are regulatory cost estimates made available by the Department of Finance through the Canada Gazette in relation to recent PCMLTFA reforms, but these are considered not robust by REs interviewed in this study. Total cost estimates calculated by Department of Finance for the 2019 PCMLTFA regulatory amendments are CAD$18,069,097 in costs over a 10-year period in 2018.[9]
No cross-government economic crime strategy exists which identifies system-wide shortcomings, and sets out a policy and operational response which is commensurate with the assessed threats.	However, there are a wide range of more operational-level working groups that support public/private and operational level coordination. In addition, a large body of cross-government activity has been engaged in the delivery of the latest set of regulatory amendments for the PCMLTFA/R[10]. FINTRAC states in its Departmental Results Report that, in 2019–20, that it co-Chairs a new Public Private Collaboration Steering Committee (PPCSC). The main objective of the PPCSC is to improve anti-money laundering effectiveness within existing authorities and will build on existing Regime committees.[11] A special joint meeting of federal, provincial and territorial Finance Ministers and Ministers responsible for AML and beneficial ownership was held on June 13, 2019 during which strategic, joint priorities for combatting money laundering and terrorist financing were discussed and agreed at a high level.[12]

[9] http://gazette.gc.ca/rp-pr/p1/2020/2020-02-15/html/reg1-eng.html

[10] https://www.fintrac-canafe.gc.ca/publications/drr-rrm/2019-2020/drr-rrm-eng

[11] https://www.fintrac-canafe.gc.ca/publications/drr-rrm/2019-2020/drr-rrm-eng

[12] https://www.canada.ca/en/department-finance/news/2019/06/joint-statement--federal-provincial-and-territorial-governments-working-together-to-combat-money-laundering-and-terrorist-financing-in-canada.html

	The new ACE Fusion Team has a mandate to identify system-wide shortcomings and support an appropriate policy response.
No future target operating model has been defined by the Canadian Government for what a more effective and efficient AML/CFT regime in Canada looks like, including setting out how public agencies and REs should share information to achieve the desired capabilities.	The relatively new national/provincial Counter-Illicit Finance Alliance (CIFA) forum, established by the RCMP and evolved from the lessons of Project Athena, may provide a greater sense of strategic national prioritisation and help inform policy reform, based on operational needs.
Cross-government national economic crime threats are not identified nor communicated to REs in any consistent manner that could inform the allocation of resources against those threats by REs.	However, FINTRAC produce a range of operational alerts related to public/private partnership (PPP) 'project initiatives', and makes clear in the FINTRAC assessment manual[13] that these documents should have a bearing on a RE's assessment of risk.
Canada is currently driving one of the most extensive AML/ATF data collection regimes in the world, encouraging massive volumes of reporting of Canadian transactions to FINTRAC. FINTRAC receive almost 10million more reports per year than their U.S. counterpart.	FINTRAC place a heavy emphasis on privacy in all its corporate documentation. FINTRAC is the only federal agency whose governing legislation requires a biennial audit by the Office of the Privacy Commissioner on the measures it takes to safeguard the personal information that it receives and collects under the PCMLTFA.
The available evidence suggests that the current Canadian AML/ATF regime is deficient; unable to demonstrate an effective impact relative to the likely scale of economic crime in Canada, very costly to implement; and resulting in a very high data collection footprint on Canadian society.	

[13] https://www.fintrac-canafe.gc.ca/guidance-directives/exam-examen/cam/cams-eng

Relevant international practices to the strategic challenge 1: Limited strategic vision		
Understanding the effectiveness and efficiency of the AML/ATF regime.	🇺🇸	The U.S. Bank Secrecy Act “Value Project” organised by the Financial Crimes Enforcement Network (FinCEN, U.S. Treasury) was established in early 2019 and is still underway. It aims to identify what value individual AML policy instruments from the Bank Secrecy Act have for specific stakeholders in terms of outputs, outcomes and costs.
	🇳🇱	In the 2019 “Joint Action Plan”, endorsed by Justice and Security and the Finance Ministers, the Dutch government has committed to regular evaluations of the AML/CFT policy framework to identify vulnerabilities of the current regime so that “policy is risk-oriented and can be adjusted”.
	🇬🇧	The UK has developed a National Serious and Organised Crime Performance Framework, produced by the Home Office and National Crime Agency (NCA) in conjunction with private stakeholders to identify a quantitative and qualitative approach to understanding the impact of the UK’s overseas and domestic response to serious and organised crime. Overall, the UK Economic Crime Plan is accountable against the following 7 Key Performance Questions: ● KPQ 1: How comprehensive is our understanding of economic crime threats and vulnerabilities? ● KPQ 2: How effectively are we pursuing serious and organised economic criminals in the UK, online and overseas? ● KPQ 3: How effectively are we building resilience in the public and private sector against economic crime? ● KPQ 4: How effectively are we supporting those impacted by economic crime? ● KPQ 5: How effectively are we deterring people from involvement in economic crime? ● KPQ 6: How effectively are we developing core capabilities to address emerging economic crime threats? ● KPQ 7: How effectively and efficiently are we managing our resources in countering economic crime?

Understanding economic crime threats	🇳🇱	The 2019 Dutch "Joint Action Plan", with a suite of over 40 specific actions, committed to the regular execution of National Risk Assessments to support policy making and called for cross-government collaboration on threat understanding to be reinforced through the national 'Financial Expertise Centre' to understand threats and share trends across the range of relevant agencies
	🇺🇸	The U.S. Department of the Treasury "2020 National Strategy for Combating Terrorist and Other Illicit Financing", alongside the 2018 National Risk Assessments, identify the most significant illicit finance threats, vulnerabilities, and risks facing the United States. The documents are specifically produced to support financial institutions in informing their own risk assessments. Moreover, AML/CFT examiners are expected to refer to them when assessing whether AML/CFT compliance is tailored to the risks faced by their supervised entities.
	🇬🇧	The UK committed to addressing gaps in the UK evidence base for different types of economic crimes and limitations in the data and statistics collected though the National Risk Assessment process, supported by a National Assessments Centre which conducts public-private economic crime threat assessments.

Developing a national strategy to address economic crime	🇪🇺	The European Commission published the “EU AML Action Plan 2020” in May 2020 to address fragmentation of AML regulations, uneven supervision, limitations in cooperation among financial intelligence units and inadequate information-sharing across the EU.
	🇺🇸	In 2020, in the “National Illicit Finance Strategy”, the U.S. Treasury announced its intention to both identify key threats and establish “a roadmap to modernize the U.S. counter-illicit finance regime”. The Strategy provided the framework for a whole-of-government multi-agency approach and laid out policy and regulatory reforms covering three strategic priorities: 1. Increasing transparency and closing gaps in the U.S. AML/CFT legal framework; 2. Improving the efficiency and effectiveness of the U.S. AML/CFT regulatory and supervisory framework for financial institutions; and 3. Enhancing current AML/CFT operational capabilities.
	🇳🇱	In 2019, the Dutch Ministers of Finance and Justice and Security submitted a “Joint action plan for the prevention of money laundering through the Dutch financial system and for tracking and prosecuting criminals and their enablers” to the Dutch parliament. The plan set out a strategic intent to support various forms of sharing information, including increasing the effectiveness of joint transaction monitoring by banks by means of a “TM utility” able to analyse transaction flows across multiple financial institutions. The strategy also supports the development of public-public information sharing by increasing the scope for AML regulators to share information with bodies within the Financial Expertise Centre (a partnership between authorities charged with combatting, detecting, and prosecuting money laundering).

(Cont…) Developing a national strategy to address economic crime	🇳🇱	The Dutch “Joint Action Plan” sees a commitment for funding to support the new framework with EUR 29 million from 2021 onwards. The broad set of measures proposed in the plan are grouped into three main categories, aimed at (i) increasing the barriers against criminals channelling illegally obtained income into the financial system; (ii) increasing the effectiveness of the “gatekeeper” function and how it is supervised, thus excluding the proceeds of crime from the financial system; and (iii) reinforcing investigation and prosecution, so that criminals can be dealt with even more quickly and effectively.
	🇬🇧	The “UK Economic Crime Plan 2019-2022” provides a wide ranging and cross-government plan and builds from the UK’s 7 priority areas for reform which were published in January 2019, covering the need to: 1) develop a better understanding of the threat posed by economic crime and our performance in combatting economic crime; 2) pursue better sharing and usage of information to combat economic crime within and between the public and private sectors across all participants; 3) ensure the powers, procedures and tools of law enforcement, the justice system and the private sector are as effective as possible; 4) strengthen the capabilities of law enforcement, the justice system and private sector to detect, deter and disrupt economic crime; 5) build greater resilience to economic crime by enhancing the management of economic crime risk in the private sector and the risk-based approach to supervision; 6) improve our systems for transparency of ownership of legal entities and legal arrangements; and 7) deliver an ambitious international strategy to enhance security, prosperity and the UK’s global influence.

Prioritising economic crime threats at a cross-government level	🇺🇸	The U.S. Treasury Financial Crimes Enforcement Network (FinCEN) issued an advanced notice of rulemaking (ANPRM) in September 2020 for regulatory changes under the Bank Secrecy Act in the U.S. The proposed amendments raise the prospect of specific priority national economic crime threats being communicated to financial institutions by the Director of FinCEN on a biennial basis to support financial institutions to build up technical and personal expertise and invest in public-private partnership collaboration in relation to prioritised threats, proportionate to the financial institutions' exposure to the respective threats.
	🇳🇱	The Netherlands established the 'Financial Expertise Centre' (FEC) as a central national public-public coordinating authority, with oversight of cross-government coordination on financial crime and oversight of all national public-private financial information sharing partnerships. The FEC is a cooperative association of the Netherlands Authority for the Financial Markets (AFM), General Intelligence and Security Service, Tax and Customs Administration, De Nederlandsche Bank (DNB), Fiscal Intelligence and Information Service and Economic Investigation Service, Public Prosecution Service and the Police Force. The Dutch 2019 'Joint Action Plan' requires the FEC to set crime threat priorities, to conduct research into coordination and prioritisation, encourages cross-agency collaboration and the development of joint projects targeting specific risks, such as prevent abuse by or through foundations, cash (illegal payment), trust sector and investment fraud.
	🇬🇧	The UK National Economic Crime Centre (NECC) provides an additional model for an integrated approach to national AML/CTF coordination or prioritisation. On October 2018, the UK launched the NECC within the NCA, which includes representation from the UK FIU, City of London Police, Serious Fraud Office, Financial Conduct Authority, Home Office, Crown Prosecution Service and HM Revenue & Customs. The multi-agency centre has responsibility for planning and coordinating the operational responses across agencies, with the stated intent to bring together the UK's capabilities to tackle economic crime more effectively. The NECC has a mandate to define a set of national financial crime priorities, with supervisor and law enforcement support, and FIU and private sector engagement.

Strategic challenge 2: Insufficient public-private financial information sharing to detect ML

In terms of public/private collaboration, Canada has sought to achieve as much as possible within the current legal regime, including five years of national effort applied to public and private sector collaboration on typology and indicator 'project initiatives'. However, without tactical (entity-level) public/private information sharing, Canada likely faces a low ceiling on the effectiveness of its AML/ATF regime.

Characteristics in the Canadian AML/ATF regime contributing to the strategic challenge	Qualifications / additional context / recent developments
Canadian public-private tactical financial information sharing does not benefit from a specific enabling legal framework which is designed for purpose. As a result, Canadian public-private financial information-sharing suffers from limitations due legal uncertainty or legal constraints.	The most recent Canadian PCMLTFA statutory review 'Confronting Money Laundering and Terrorist Financing: Moving Canada Forward' (published in 2018)[14] made specific commitments to strengthen public-private financial information sharing and consider a JMLIT style tactical partnership arrangement in Canada. The Canadian Government's Fall Economic Statement 2020 (FES) makes commitments to support greater public-private financial information-sharing, though falling short of the ambition of the statutory review.[15]
Most significantly, current Canadian public-private financial information-sharing 'project initiatives' have not facilitated the sharing of 'tactical' information; i.e. specific names or entities (identifiable information) of relevance to law enforcement investigations. As such, the impact of public-private information sharing for direct benefit to law enforcement investigation is substantially reduced compared with arrangements in other similar countries.	However, project initiatives have demonstrated significant results in terms of stimulating STR reporting in relation to the threats prioritised in these projects.

[14] https://www.ourcommons.ca/Content/Committee/421/FINA/Reports/RP10170742/finarp24/finarp24-e.pdf

[15] https://www.budget.gc.ca/fes-eea/2020/report-rapport/toc-tdm-en.html

Out of all countries with a public/private financial information sharing partnership approach to tackling economic crime, Canada is the only common-law country that does not allow public-private tactical-level information sharing to support law enforcement investigations (i.e. outside public/private exchange of information in an STR, from RE to FINTRAC; and outside of a production order, from law enforcement to REs).	However, regardless, Canada has sought to promote 'global leadership'[16] in relation to the lessons identified from strategic typology development, including and, in particular, through 'Project Protect'.
At the FIU level, FINTRAC is unable to share tactical information related to their STR intelligence back to regulated entities or to request follow up information from regulated entities on the STRs filed.	However, FINTRAC aims to support high levels of outreach to RE communities to explain trends and typologies FINTRAC is seeing, including with regard to STR trends and generic challenges or quality problems they observe across all STRs.
Viewed as a traditional intelligence cycle, the AML/ATF regime is fundamentally broken and 'built backwards', with law enforcement end-users of AML intelligence at least two-steps removed from collection. There is no direction of intelligence collection, and therefore no planning in an intelligence sense. 30,000+[17] REs form their own view of collection requirements for STRs and report tremendous volumes through to FINTRAC, over 30 million transactions per year in total. While FINTRAC analyses STR reporting and produced intelligence material, disseminated through disclosures to law enforcement on a proactive or reactive basis, there is no tactical-level feedback to REs from either end-users or FINTRAC.	However, law enforcement agencies can request responses from FINTRAC through voluntary information records. This process guides FINTRAC to draw from the historic database of transactions that is held by FINTRAC to produce 'reactive' intelligence reports, though this process may take time.
Despite their success, the tempo and bandwidth of public-private co-production of strategic intelligence typologies in Canada is low compared to similar foreign jurisdictions, with 'project initiatives' historically taking a year to produce indicators.	However, FINTRAC, RCMP and major reporting REs – in particular – have established high levels of trust and there is now a deep bedrock of public/private collaboration and enthusiasm to collaborate to draw from.

[16] https://www.fintrac-canafe.gc.ca/publications/ar/2020/1-eng#s7

[17] A comprehensive number of reporting entities in the Canadian AML/ATF system is not clear to the author from public material. Though multiple FINTRAC references from 2016 to 2019 refer to the number of regulated entities as 31,000)

Relevant international practices to the strategic challenge 2: Inadequate public/private financial information-sharing		
Strengthening the legislative basis for public-private financial information sharing as designed for purpose	🇳🇱	In the Netherlands, the Terrorist Financing Taskforce was initially founded with authority under a general article in The Netherlands Police Information Act, which requires that three conditions be met before police can share investigative information with third parties in the Netherlands: • A pressing need. • Substantial public interest. • Prevention or investigation of criminal activity. Following the success of the partnership models in the Netherlands, the Dutch government – in line with the 'Joint Action Plan' – is expected to lay new legislation before Q1 2021 specifically to enable public-private and private-private information sharing to support financial crime and terrorist financing investigations. An additional government research paper was published alongside the inter-Ministerial "Joint Action Plan", which surveyed international models of public-private financial information sharing and described the key features of a target operating model that would be the priority for The Netherlands. The paper highlighted the relationship of the proposals in the Action Plan in terms current Dutch AML/CFT legislation, data protection law (GDPR), competition law and regulation (describing what is currently permissible within the law, what reforms would be required to achieve the ambition of the Action plan, and outlining the design conditions required to be compliant with data protection and competition law.)
	🇬🇧	UK Joint Money Laundering Intelligence Taskforce (JMLIT), the Crime and Courts Act 2013, Section 7, provided a pre-existing legal gateway that was used to support the development of UK JMLIT partnership. Section 7 provides a wide legislative gateway for the UK National Crime Agency (NCA) to share information for the purpose of supporting its functions. As such, the partnership tactical sharing in the UK must be convened by the NCA. However, this legal framework was updated under the 2017 Criminal Finances Act and is also subject to legislative enhancements to enable policy objectives set out in the UK Economic Crime Plan of 2019.

Developing a high-capacity public/private co-production capability for strategic financial intelligence	🇬🇧 🇩🇪 +	Both the UK JMLIT and German Anti-Financial Crime Alliance (AFCA) average production of 10 risk indicator / typology products per year. UK JMLIT stands out in the sheer volume of products produced; being responsible for 49 'JMLIT Alert' reports between its establishment in April 2015 and June 2020. Overall, partnerships around the world have developed strategic alerts have produced strategic intelligence from topics as diverse as: terrorist financing; tax evasion; drug trafficking; fraud; corruption; human trafficking; virtual assets; casinos, real estate and high-value goods; misuse of legal persons (shell companies and trusts); trade-based money laundering; wildlife and environmental crime; money laundering in capital markets; and illegal mining.
	🇺🇸	In the U.S. 2020 National Illicit Finance Strategy highlighted the importance of producing alerts and advisories that reach beyond the largest financial institutions to include, small banks, money transmitters, and broker-dealers, as well as other sectors that have an important role with respect of being gatekeepers or otherwise having valuable information or insights into risks. As an example, the strategy highlights "targeted advisories to the shipping, insurance, and aviation industry to assist them in identifying potential sanctions evasion activity" and how "Treasury has also engaged with key participants in the real estate market about sale and purchase trends and illicit finance risks identified in the real estate in the national risk assessments and other Treasury advisories".
	🇸🇬	In Singapore, ACIP typology products have been actively leveraged to inform and enhance the quality of compliance in regulated entities outside of partnerships. As one of the few partnerships designed and led from a supervisory perspective, the Singapore ACIP specifically set out to highlight red flags, typologies and set out industry best practices for the identification and mitigation of risks that would have standing as a compliance education tool. The partnership does not enable tactical information-sharing, but partnership typologies have supported training sessions for regulated entities, been incorporated into broader training provided by the banking association and now form part of a university compliance elective module.

Achieving an orientation towards law enforcement priorities for post-suspicion information-sharing	🇺🇸	The U.S. FinCEN Exchange model is entirely directed around a law enforcement customer, with variable RE membership on a case-by-case basis, at the determination of FinCEN. Participation in FinCEN Exchange meetings is by invitation only, as determined by FinCEN and relevant law enforcement agencies specific to the case at hand. More broadly, the general proposed reforms to AML supervision as laid out in the September 2020 FinCEN ANPRM include a proposal that “the reporting of information with a high degree of usefulness to government authorities” is included as principal part of what constitutes and effective AML program and, therefore, forms the basis for what REs will be supervised against.
	🇭🇰 🇳🇱 🇬🇧 🇸🇪	A number of partnerships around the world are directly led by law enforcement agencies, which has the advantage of ensuring a stronger link between partnership projects and law enforcement appetite for progressing the intelligence through to an investigation. While still providing a significant opportunity for private-sector led project, the following partnerships have law enforcement investigative interests as a primary driver for post-suspicion information-sharing: the Hong Kong Fraud and Money Laundering Intelligence Taskforce (FMLIT); the Netherlands Terrorist Financing Taskforce (NL-TFTF); the Netherlands Serious Crime Taskforce (NL-SCTF); UK Joint Money Laundering Intelligence Taskforce (JMLIT); and the Swedish Anti-Money Laundering Intelligence Taskforce (SAMLIT).

Strategic challenge 3: Inadequate private-private financial information sharing to detect ML

In contrast to fraud, tactical information-sharing to detect or prevent money laundering in Canada is limited to instances in where there is ‘knowledge’ of a crime taking place, and as such does not take place.

Characteristics in the Canadian AML/ATF regime contributing to the strategic challenge	Qualifications / additional context / recent developments
There is no clear legal gateway for regulated entities in Canada to permit the sharing of information with counterpart financial institutions relating to financial crime risks, beyond fraud (prior to the determination of suspicion).	However, in contrast the private-to-private frameworks for information-sharing for the suppression of fraud are believed to be strong and there are also examples of successful interaction between REs and the RCMP in anti-fraud and anti-cyber threat campaigns.
The lack of a legal provision in Canada to support private-to-private sector information sharing to determine ML suspicion undermines the detection of economic crime that spans multiple financial institutions, which is believed to be a basic characteristic of professional money laundering.	
While PIPEDA allows for private-to-private information sharing for the suppression of fraud, there is no such exemption for money laundering.	
Canada falls short of the U.S., UK and Netherlands regimes to enable collaborative analytics across multiple REs in order to detect crime.	

Relevant international practices to the strategic challenge 3: Inadequate private-private financial information sharing to detect ML		
Establishing a legal basis for private-private financial information sharing to detect crime. (pre-suspicion)	🇺🇸	In the US, there has been considerable progress and innovation in the use of existing legal provisions for private–private sharing under the provisions of the U.S. PATRIOT Act. The PATRIOT Act, section 314(b), created a voluntary programme that enables pre-SAR sharing and gives legal authority for REs to share information with one another for purposes of identifying, and, where appropriate, reporting activities that may involve possible terrorist activity or money laundering. The number of institutions engaged in the 314(b) process has nearly doubled between 2014 and 2018.
	🇺🇸	In 2015, a group of major banks in the US initiated a partnership to better exploit the legal provision of 314(b) and develop a more effective network intelligence picture of financial crime threats across participating entities. The private–private partnership supports co-location of analysts and real-time exchange of information. The partnership has reportedly worked on a large number of major cases, covering human trafficking, corruption, narcotics trafficking, trade-based money laundering, proliferation and sanctions evasion. Members report the benefits to include a more holistic view of criminal networks and supporting arrests, convictions, asset seizures and forfeiture, though no public performance statistics are available for the partnership.
	🇳🇱	In the Netherlands, Transaction Monitoring NL (TMNL) is being developed as a platform for a new approach to transaction monitoring by the banking association. The Netherlands has a policy mandate through the 'Joint Action Plan' for the national regulator to support KYC and TM functions as a utility for regulated entities and TMNL is being established by the five largest banks in the Netherlands as a Joint Venture. The objective is to provide a platform to collect and analyse all the members' transaction information and apply typologies and algorithms to the combined data.
	🇪🇪	In 2020 in Estonia, an FIU and supervisor supported private-private sector information sharing platform was created in a pilot project entitled "the AML bridge", which enables private-private sharing between four of Estonia's largest banks – LHV, SEB Estonia, Swedbank Estonia, and Luminor. This project benefits from a legal regime in Estonia that enables private-private financial information sharing for pre-suspicion concern.

Strategic challenge 4: A system which incentivises firm-level risk management, but exacerbates system-wide vulnerability, through ‘de-marketing’

A principal outcome in the Canadian AML/ATF regime, when an RE identifies suspicion is to ‘de-market’ the customer – i.e. to close an account unilaterally and uncoordinated with law enforcement interests. This process creates system-wide vulnerabilities with limited credible preventative or deterrent effect against money launderers.

Characteristics in the Canadian AML/ATF regime contributing to the strategic challenge	Qualifications / additional context / recent developments
Canada does not have a formal account ‘keep open request’ process. When a law enforcement agency shares information with an RE in Canada, which in Canada is largely limited to the process of sending a production order for information on an account holder, it may result in the RE closing the account, which could undermine or disrupt the law enforcement investigation.	However, some REs do report that they are comfortable to abide by informal ‘keep open requests’ that law enforcement do issue and that they would expect FINTRAC not to punish them for doing so.
There is no facility or legal gateway in Canada to allow financial institutions to share information related to financial crime investigations post-suspicion. As a result, it is believed to be a regular occurrence that a ‘de-marketed’ customer who has been exited for financial crime reasons, will re-enter the financial system at an alternative point. In many cases, the financial institution that de-marketed the client will be able to observe the new financial institution which takes receipt of any remaining credit in the account being closed, but will not be able to provide any reference information to the new financial institution on that client.	However, it is unclear whether it is a policy objective in Canada to deny an individual’s access to the financial system based on suspicion of ML alone.

Relevant international practices to the strategic challenge 4: Unilateral account closures and system-wide vulnerability

Streamlining the process for law enforcement 'keep open' requests	🇺🇸	The US FinCEN has guidance on keep open procedures dating from 2007, which states that law enforcement agency requests to maintain an account should be in a written form, and the requirement should last no longer than six months and be recorded by the financial institution for five years. Keep open letters should be issued by a supervisory agent or by an attorney within the respective US attorney or state prosecutor's office. In the US, if a regulated entity is made aware through a FinCEN Exchange Briefing that an account is under investigation, then 'FinCEN recommends that the financial institution notify law enforcement before making any decision regarding the status of the account'. However, the FinCEN guidance confirms that keep open letters are essentially voluntary requests, stating: 'Ultimately, the decision to maintain or close an account should be made by a financial institution in accordance with its own standards and guidelines'. It remains possible that current US keep open letters also do not protect regulated entities from all supervisory, criminal or reputational risks in maintaining an account suspected of links to financial crime or terrorist activity.
	🇳🇱	In the Netherlands, there are strict laws that, in general, prevent a financial institution from closing an individual's account and thereby denying the individual a right to financial services. As such, upon determination of suspicion, banking clients in the Netherlands are typically moved to 'limited service accounts', which provide only basic banking services, and the regulated entity continues to report to the national financial intelligence unit as appropriate.
Enabling post-suspicion private-private information sharing, in line with fraud and cyber information sharing	🇳🇱	The Netherlands 2019 "Joint Action Plan" sets out an ambition to remove existing legal barriers to inter-bank data sharing of 'black listing' information related to risky entities and provide a review of the legal basis for such a mechanism in the context of GDPR data privacy obligations and providing opportunities for redress and correction for individuals to challenges their designation on such a list.
	🇬🇧	In the context of the UK Economic Crime Plan, a specific cross-government and industry working group has been developing a UK model for 'post-suspicion' fincrime information-sharing, similar to the confirmed fraud information-sharing platform in the UK, to avoid risk displacement when customers are exited by REs.

5. Key themes relevant to enhancing the Canadian AML/ATF information-sharing framework.

In the reference annex of this document, the author sets out various details behind the challenges raised in interview, additional contextual analysis of the Canadian regime, international case studies and opportunities to enhance the Canadian AML/ATF information-sharing regime.

This material is framed around the following AML/ATF information-sharing themes:

Theme 1. Data to understand the effectiveness and efficiency of the AML/ATF system;

Theme 2. A strategic understanding of threats and a strategic approach to addressing economic crime;

Theme 3. Prioritisation of economic crime threats at a cross-government level;

Theme 4. Public-private tactical financial information-sharing;

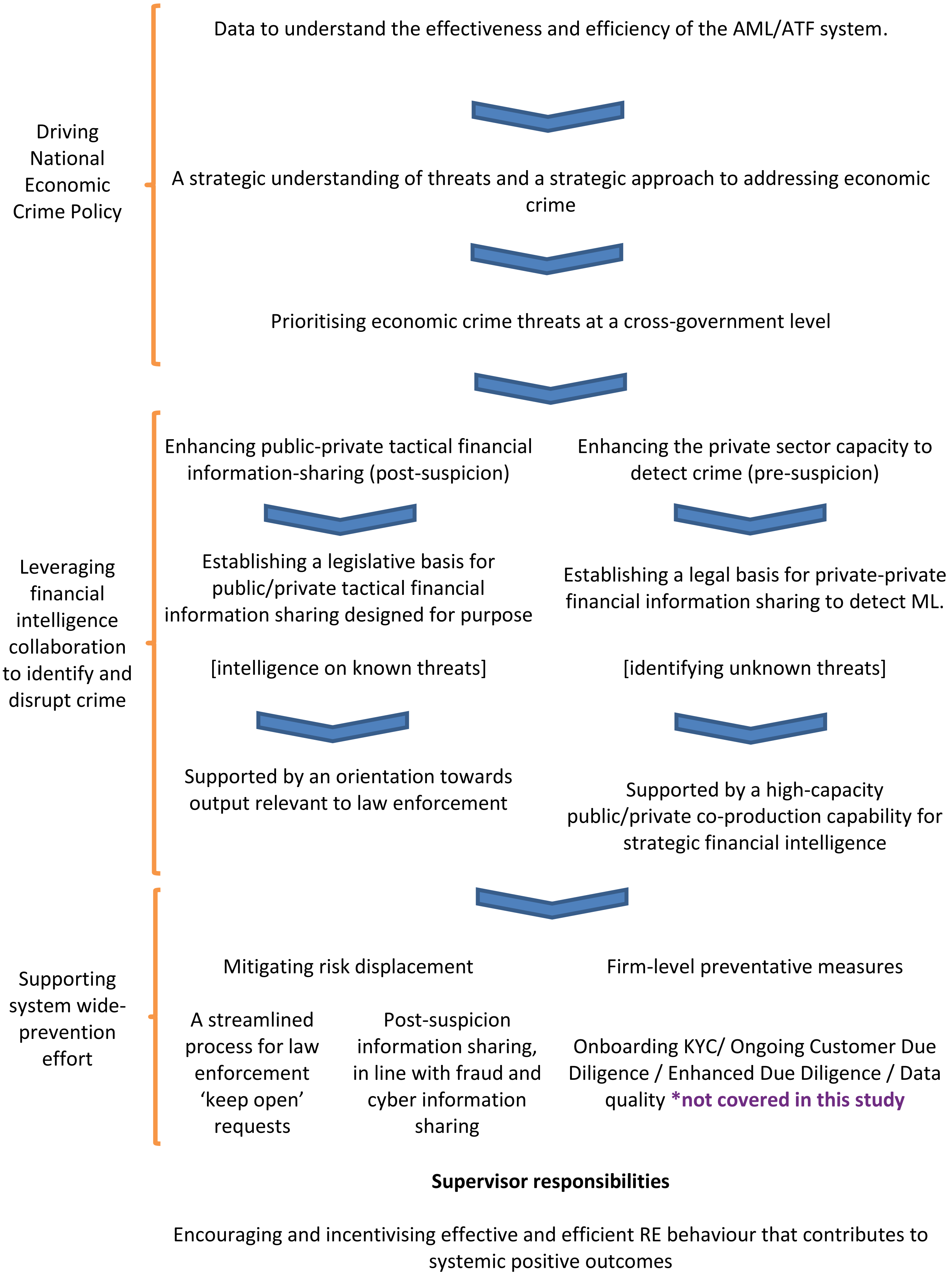
Theme 5. The extent of public/private co-production of strategic financial intelligence;

Theme 6. Relevance to law enforcement outcomes;

Theme 7. Private-private financial information sharing to detect crime; and

Theme 8. Mitigating the negative impacts of account closures.

6. Inter-relationship of financial information-sharing themes:



Driving National Economic Crime Policy

Data to understand the effectiveness and efficiency of the AML/ATF system.

A strategic understanding of threats and a strategic approach to addressing economic crime

Prioritising economic crime threats at a cross-government level

Leveraging financial intelligence collaboration to identify and disrupt crime

Enhancing public-private tactical financial information-sharing (post-suspicion)

Establishing a legislative basis for public/private tactical financial information sharing designed for purpose

[intelligence on known threats]

Supported by an orientation towards output relevant to law enforcement

Enhancing the private sector capacity to detect crime (pre-suspicion)

Establishing a legal basis for private-private financial information sharing to detect ML.

[identifying unknown threats]

Supported by a high-capacity public/private co-production capability for strategic financial intelligence

Supporting system wide-prevention effort

Mitigating risk displacement

A streamlined process for law enforcement ‘keep open’ requests

Post-suspicion information sharing, in line with fraud and cyber information sharing

Firm-level preventative measures

Onboarding KYC/ Ongoing Customer Due Diligence / Enhanced Due Diligence / Data quality ***not covered in this study**

Supervisor responsibilities

Encouraging and incentivising effective and efficient RE behaviour that contributes to systemic positive outcomes

7. Opportunities to enhance the Canadian framework

Theme 1. Data to understand the effectiveness and efficiency of the AML/ATF system

Opportunities to enhance the Canadian framework:

- Canada can benefit from a more comprehensive understanding of the effectiveness, efficiency and data privacy costs and benefits of the various components of the AML/ATF system.
- Canadian departments can collaborate to elevate performance reporting on the Canadian AML/ATF framework to a national cross-government exercise. FINTRAC's mandate is too limited to publish performance metrics that adequately reflect the inputs, outputs and outcomes to understand 'end-to-end' effectiveness in the AML/ATF system.
- An Economic Crime Disruption Annual Report could usefully be published to include relevant performance data from FINTRAC, law enforcement agencies, the Public Prosecution Service of Canada and, as far as possible, from regulated entities to understand outcomes from the AML/ATF system. Potentially, the ACE Fusion Team may be in a strong position to provide this function.
- In the absence of the above, FINTRAC may be able to extend the coverage of its annual performance monitoring to include greater coverage of outcome indicators from the use of intelligence and to include an official estimate of the cost of the reporting regime on the regulated sector. Such performance data will empower strategic decision making in Canada, and support accountability, to ensure that the AML/ATF system is delivering outcomes effectively and efficiently.
- Improved outcome data relating to effectiveness and efficiency can drive a more effective response to crime in Canada at the policy level and inform changes at the operational level to improve investigations and asset recovery and achieve more efficient use of public and private sector resources within the AML/ATF system;
- In time, Canada can demonstrate a response from the outcomes in the AML/ATF system which is commensurate with the level of national economic crime threats.

Theme 2. A strategic understanding of threats and a strategic approach to addressing economic crime

Opportunities to enhance the Canadian framework:

- Economic crime threats in Canada can be assessed at a higher frequency, potentially annually, and contribute to a robust and more regular National Threat Assessment and broader National Risk Assessment (NRA) process.
- Canada can develop a clear strategy for economic crime policy and operational reform, which is founded in current economic crime threat assessments, incorporates the latest learning from the effectiveness of public-private partnership efforts and sets out a vision for the desired operating model for both public-private and private-private financial information sharing in Canada.
- The economic crime strategy can set out clear targets which are commensurate with the assessed economic crime threats and present a credible as a response to those threats.

Theme 3. Prioritisation of economic crime threats

Opportunities to enhance the Canadian framework:

- The cross-government national economic crime strategy (outlined in theme 2) can support public-private collaboration in the development of threat-specific intelligence relating to economic crime, to inform a more regular National Threat Assessment process.
- FINTRAC, or another appropriate agency, can publish clear national economic crime threat priorities which should have relevance to a financial institutions' AML programme design and be recognised by supervisors.
- Short of the previous proposal, law enforcement agencies might consider proactive steps to communicate priorities to regulated entities through regular updates.
- FINTRAC could recognise the importance of regulated entities being responsive to law enforcement priority interests and that this should, in part, inform a risk-based approach within regulated entities.
- National economic crime threat priorities can be established and reviewed on a regular basis, in line with the economic crime strategy. REs can be made aware of and understand national economic crime threat priorities and reflect those priorities in resource allocation risk-based decisions, incentivised to do so through AML/ATF supervision.
- REs could benefit from understanding of the impact that Canada is having in relation to the priority threats, including disruption associated to RE engagement in addressing the threat.

Theme 4. Public-private tactical financial information-sharing

Opportunities to enhance the Canadian framework:

- Under an appropriate strategic national economic crime strategy (see theme 2), the ambition for public-private financial information sharing should be established more clearly. A legislative enabling environment should be created to reflect that ambition, creating a legal basis to achieve the desired capability with regard to:

    - The number of regulated entities involved
    - The range of regulated sectors involved
    - The number of law enforcement agencies/investigators participating
    - The range of financial crime threats addressed by the partnership
    - The speed in which information can be transferred
    - The rate (and volume) of which tactical-level cases and typology-level projects can be processed through the partnership
    - The rate, volume and nature of cross-border information sharing connected to partnerships
    - The extent of partnership contributions to informing policy or regulatory developments

- If there can be greater clarity established around the permissibility for the RCMP to share information with financial institutions, it is possible that a law enforcement-led model of public/private partnership could be used Canada. This could follow the model of UK Joint Money Laundering Intelligence Taskforce, which operates under the legal authority entrusted to the National Crime Agency to share information.
- The RCMP and other agencies can explore means to provide greater clarity over the current legal permissibility of law enforcement to bank information sharing, optimising use of the current framework. Public entities and major reporters may consider establishing a pilot information-sharing model, founded on the legal gateway to share both strategic and tactical information between the RCMP and regulated entities.

- However, given the feedback of financial sector stakeholders, it is more likely that a new legal provision which provides a specific enabling clause for the public-private financial information-sharing will be required to support law enforcement-led information-sharing, either through reforms to the AML law or the privacy regime. The author notes that on 17 November 2020, the Canadian Minister of Innovation, Science and Industry, tabled proposed legislation in Parliament that aims to overhaul Canada's data privacy law: "Bill C-11, entitled An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Act".
- It is understood by the author that the new Bill aims to emulated some aspects of the data protection rights regime established under GDPR. GDPR is the privacy legal framework for many jurisdictions that support tactical-level public-private AML/ATF information-sharing. Intrinsic in FATF Recommendation 2 is a requirement to ensure that countries establish compatibility of AML/CTF requirements and data protection. Canadian policy-makers have an opportunity to fulfil this mandate from FATF to ensure that the new privacy law adequately reflect policy-intent with regard to the AML/ATF regime and associated information sharing requirements.
- Looking to the future, rather than simply emulating other countries innovations of five years ago, Canada may wish to establish a more direct, real-time and digital relationship between the FIU and transactions of major reporters, in a privacy preserving manner (as described in theme 2) and in line with the Australian intent raised above through the 'Alerting Project'.
- Outside of legal reform, FINTRAC may be able to support greater public-private financial information sharing by providing more direct feedback on the quality and relevance of STR reporting to regulated entities. However, without legislative reform, FINTRAC will be highly constrained in the kind of information it can share and will not be able to facilitate a robust public-private sharing.
- Canadian public agencies should consider whether a facility could be established that discloses the names of charged individuals on a real-time and confidential basis to RE designed persons, allowing REs to investigate and report back to FINTRAC and LE with additional transaction and counterparties.

Theme 5. The extent of public/private co-production of strategic financial intelligence

Opportunities to enhance the Canadian framework:

- Canadian public and private stakeholders should increase the ambition for the rate and extent of development of strategic intelligence typology products. As resources allow, this partnership forum may consider how to enhance:

  - The rate of production of typology products;
  - The number of financial crime threats covered;
  - The number of regulated sectors and entities participating in the knowledge exchange process;
  - The number of localised typology products to reflect the unique characteristics of certain regions, or certain criminal networks;
  - The responsiveness and timeliness of the development of the knowledge products;

- This effort could leverage the increasing library of strategic intelligence products produced in other jurisdictions and re-evaluate them in the Canadian context, thereby building on previous analytic efforts rather than duplicating international effort.
- FINTRAC might seek to support the 'industrialisation' of typology papers and embed them into the supervisory processes.
- To complement human analyst generated typologies FINTRAC could support the digitisation and sharing of typologies as data models, developed through machine learning techniques, that can be integrated and overlayed onto digital systems.

Theme 6. Relevance to law enforcement outcomes

- As appropriate to the Canadian broader economic crime strategy (theme 2), Canada can achieve a legal framework which provides for the desired level of information-sharing between REs in response to law enforcement requests and live investigations.
- The legal provisions for public-private financial information sharing achieve the strategic target operating model, developed through consultation and articulated in a policy and operational economic crime reform strategy.
- Law enforcement investigative interests, as part of the delivery of the economic crime strategy for disruption, are the principal orientation for AML/ATF activity which is intended to achieve or support 'disruption'. 'Prevention' functions of the AML/ATF regime are also geared around broader crime prevention strategies.

Theme 7. Private-private financial information sharing to detect crime

- Policy makers could consider expanding the information-sharing legal provisions beyond PIPEDA to also allow for private-private sharing relevant to investigations relating to money laundering offenses, terrorist financing offenses, and any other predicate offense included in the PCMTLFA/R.
- PCMLTFA/R may also be updated to broaden its scope for information sharing (e.g. to share information that an STR has been filed on a particular customer) and include "safe-harbour" protections similar to those in section 314(b) of the USA Patriot Act, which permit information to be shared between banks for AML/ATF investigative purposes. Additionally, the scope to share information could be expanded to include the fact that a bank has chosen to exit a customer to limit risk displacement.
- The Office of the Privacy Commissioner may consider developing additional guidance relating to pre-suspicion information sharing.

Theme 8. Mitigation of the negative impacts of account closures.

- Canadian 'keep open' processes could be formally established and benefit from clear guidelines (to both REs and law enforcement agencies), including clarity over roles and responsibilities for the account and expectations in terms of the duration of the request.
- The requirement to abide by a 'keep open' request could be given a high priority from a supervisory perspective, such an incident of an RE still closing an account despite a 'keep open request' is rare or non-occurring. As a result, law enforcement would be able to achieve a high level of confidence that an account will not be closed outside of a coordinated disruptive plan of action and the AML/ATF system removes a perverse incentive to undermine law enforcement investigations.
- Canada could establish a legal gateway to share ML information post-suspicion, through an appropriate governance model with an opportunity for redress for innocent parties. The post-suspicion ML framework could support preventative outcomes for ML risks comparable to that available for fraud and cyber threat sharing.
- AML/ATF 'preventative measures' in Canada can be encouraged to be effective at a sector or system wide level, not just a firm-level (which may otherwise incentivise risk-displacement and harm to other REs).
- REs could benefit from cost savings in terms of reduced duplication in AML activity to repeatedly identify risk relating to the same entity, (which may potentially be provided through a centralised utility with statutory underpinning) and effectiveness gains.

Reference Annex

A1. What are public–private financial information-sharing partnerships?

In this paper, we refer to financial information-sharing partnerships or 'partnerships' to mean:

> Collaborative public and private sector forums that:
>
> - Provide regularly convened dynamic public–private dialogue on financial crime threats, based on shared and agreed objectives and priorities;
> - Act within the law by making use of available information-sharing legislation, based on a shared public–private understanding of the legal gateways and boundaries of sharing information;
> - Can enable, to some degree, private–private sharing of information and knowledge between certain regulated entities; and
> - Address one or more of the following issues:
>   - Sharing of tactical information, including the identities of entities of concern, to enhance ongoing investigations.
>   - Collaborative knowledge management processes to build understanding of threats and risks, for example through the co-development of typologies (sometimes referred to as 'alerts') and the development and testing of indicators, to improve reporting from the private sector.

We also use the term 'partnerships', more generally, to refer to the public and private decision-makers behind financial information-sharing partnerships.

A2. Why focus on information sharing?

According to FATF, 'effective information-sharing is [a] cornerstone of a well-functioning AML/CFT framework'.[18] Under the FATF international standards, AML/ATF regimes are based on a set of legal and supervisory obligations for financial institutions and other private sector service providers to proactively identify and report suspicions of the laundering of criminal proceeds and/or the facilitation of terrorist financing to government Financial Intelligence Units (FIUs). In order to produce these suspicious activity reports, regulated entities are required to identify suspicion of criminality within their business, using insight that they can develop or procure within their own institution.

While the intention of the AML/ATF regime may be for regulated entities to identify suspicions of crime within their business, there are practical challenges in doing so outside of a partnership environment. Regulated entities can find it challenging to identify potential criminality without guidance from public agencies about patterns and trends in criminal behaviour and, indeed, which specific entities are under investigation for criminal activity. In addition, while criminal networks seek to conceal money laundering schemes through the use of multiple accounts, spanning multiple financial institutions, regulated entities are not generally permitted to share information with their counterpart financial institutions about financial crime risk.

Since 2015, several jurisdictions have developed legislation and enhanced processes to address these challenges through information-sharing. Canada has supported some level of public–private financial information sharing since 2016.

[18] https://www.fatf-gafi.org/media/fatf/documents/recommendations/Private-Sector-Information-Sharing.pdf

A3. How have partnerships developed around the world?

Public–private financial information-sharing partnerships have grown from being a relatively outlying innovation in 2015, to becoming a mainstream component of the architecture to tackle financial crime in liberal democracies in 2020.

As at June 2020:

18	18 countries[19] covered in this paper have established operational public–private financial information-sharing partnerships.
23	23 partnerships are included in this reference paper in total; including multiple partnerships within a single country and also trans-national partnerships.
41%	Countries with a national public–private financial information-sharing partnership account for 41% of world GDP.[20]
20 / 30	20 out of the top 30 global financial centres are covered by a public–private financial information-sharing partnership.[21]

Fig 1. Timeline of partnership development:

2015	The UK Joint Money Laundering Intelligence Taskforce (JMLIT) (Pilot in 2015, formally established in April 2016)
2016	First Canadian 'Project' partnership initiative launched
Mar 2017	The Australian Fintel Alliance
Apr 2017	The Singapore Anti-Money Laundering and Countering the Financing of Terrorism Industry Partnership (ACIP)
May 2017	Hong Kong Fraud and Money Laundering Intelligence Taskforce (FMLIT)
Jun 2017	Joint Intelligence Group (JIG) Ireland
Jul 2017	The Netherlands Terrorist Financing Taskforce (NL-TFTF)
Dec 2017	The Europol Financial Intelligence Public Private Partnership (EFIPPP)
Dec 2017	The US FinCEN Exchange
Dec 2017	New Zealand Financial Crime Prevention Network (NZ-FCPN)
Jan 2018	The Global Coalition to Fight Financial Crime
May 2018	Latvia Cooperation Coordination Group (CCG)
Sep 2018	Austrian Public–Private Partnership Initiative (APPPI)
Oct 2018	United for Wildlife - Illegal Wildlife Trade (IWT) Financial Taskforce
Oct 2018	The Netherlands Fintell Alliance (FA-NL)
Aug 2019	The Netherlands Serious Crime Taskforce (NL-SCTF)
Sep 2019	Germany Anti Financial Crime Alliance (AFCA)
Nov 2019	Argentina Fintel-AR
Nov 2019	The Malaysia Financial Intelligence Network (MyFINet)
Dec 2019	South African Anti-Money Laundering Integrated Taskforce (SAMLIT)
Jun 2020	Finnish AML/ATF Expert Working Group on a PPP basis
Jun 2020	The Swedish Anti-Money Laundering Intelligence Taskforce (SAMLIT)
	Lithuania - Centre of Excellence in Anti-Money Laundering

[19] 17 countries and 1 autonomous region (Hong Kong).

[20] Based on "GDP (current US$)". World Development Indicators. World Bank.

[21] As defined in the twenty-seventh edition of the Global Financial Centres Index (GFCI 27) published on 26 March 2020. - https://www.longfinance.net/publications/long-finance-reports/global-financial-centres-index-27/

A4. What type of information is shared?

In general, partnerships support two major types of information sharing and respective outputs:

1. **Strategic intelligence sharing.** Public and private members of the partnership co-develop typologies or knowledge products covering financial crime threats and highlighting relevant behavioural indicators. Typically, these products do not contain confidential identifying information about specific suspects or entities, or individual clients or customers of financial institutions and, as such, do not require enabling legislation. It is generally intended that these knowledge products are made available to non-members of partnerships and are either published and accessible online (such as in the US or in Singapore), or are released through non-public distribution channels to regulated entities (such as in the UK or Hong Kong).

2. **Tactical information sharing.** Where legislation allows, partnerships have facilitated sensitive information relevant to law enforcement or national intelligence investigations to be shared with regulated entities. This information might include the names of specific individuals, legal entities or other identifying information relevant to a case. Member regulated entities can then use this awareness of priority threats, from the perspective of law enforcement or other public agencies, to search their systems in response to that identified suspicion or indicator. Depending on the legal gateway and format of the partnership, regulated entities can share sensitive information back with law enforcement either through formal reports or dynamically within the partnership.

Fig 2. The nature of information exchange within current partnerships:

Tactically focused	The US FinCEN Exchange
	Joint Intelligence Group (JIG) Ireland
Tactical and strategic intelligence co-development	The UK Joint Money Laundering Intelligence Taskforce (JMLIT)
	The Australian Fintel Alliance
	The Singapore Anti-Money Laundering and Countering the Financing of Terrorism Industry Partnership (ACIP)
	Hong Kong Fraud and Money Laundering Intelligence Taskforce (FMLIT)
	The Netherlands Terrorist Financing Taskforce (NL-TFTF)
	The Netherlands Serious Crime Taskforce (NL-SCTF)
	The Netherlands Fintell Alliance (FA-NL)
	Latvia Cooperation Coordination Group (CCG)
	The Malaysia Financial Intelligence Network (MyFINet)
	South African Anti-Money Laundering Integrated Taskforce (SAMLIT).
	The Swedish Anti-Money Laundering Intelligence Taskforce (SAMLIT)
	New Zealand Financial Crime Prevention Network (NZ-FCPN)
Strategic, with some support to tactical exchange	The Europol Financial Intelligence Public Private Partnership (EFIPPP)
	United for Wildlife - Illegal Wildlife Trade (IWT) Financial Taskforce
Strategic intelligence co-development only	Finnish AML/ATF Expert Working Group on a PPP basis
	Lithuania - Centre of Excellence in Anti-Money Laundering
	Argentina Fintel-AR
	Germany Anti Financial Crime Alliance (AFCA)
	Austrian Public–Private Partnership Initiative (APPPI)
	Canadian 'Project' Initiatives to Combat Financial Crimes through Partnerships
Strategic / Policy	The Global Coalition to Fight Financial Crime

Partnerships vary in terms of their legal basis, their membership structures and their financial crime priorities and objectives. They also differ in the format of how they meet and exchange information.

In relation to the partnerships covered in this paper, there are three major types of partnership format:

1. **Co-location of analysts / Secondment model** – In this format, public and private sector analysts sit side by side, typically in dedicated office space, and work collaboratively in real-time to support partnership objectives. Often, co-located analysts from the private sector are restricted from sharing information that they are exposed to, by virtue of their participation in partnership operations, back with their home financial institution.
2. **Convened meetings with non-permanent membership, at the direction of the FIU** – In this format, the FIU convenes the partnership on an irregular basis with no permanent membership from the private sector. Meetings typically focus on specific cases or financial crime threats, and membership for each meeting or project is chosen in response to the case at hand.
3. **Regularly convened meetings** – In this format, partnership members convene on a regular basis, but do not co-locate for a prolonged amount of time. Participants involved in meetings in this model are typically more senior, than compared to co-location models. In contrast to co-location models, in general, private sector members of regularly convened meetings have the opportunity to share the information, that they receive during the partnership meetings, back to appropriate colleagues in their financial crime intelligence or risk function at their home institution.

A5. How are AML supervisors involved?

Partnerships differ in their organisational composition, including with regard to the status of AML supervisors in partnerships.

Some partnerships refer to the importance of AML supervisors being members of the partnership. Such membership can help ensure that the AML supervisor has a comprehensive view of the AML/ATF system and that supervisors are comfortable with the nature of information-sharing occurring within the partnership. To an extent, supervisors have an opportunity to encourage and incentivise the use of partnerships and can resolve uncertainties by issuing guidance or other communications about their expectations. Further, supervisors have a system-wide responsibility, beyond partnership members. As such, they can help ensure that valuable learning, being generated within partnerships, is shared with a broader community of regulated entities outside of the partnership.

However, supervisors may also have a ‘dampening effect’ on information sharing within a partnership. Regulated entities may experience an increased risk of regulatory compliance enforcement action if the AML supervisor is party to the information being exchanged. There is a risk for regulated entities that information and openness about their exposure to financial crime risk, which may have been shared in good faith to support a law enforcement investigation of underlying crime, may then be used in a regulatory compliance enforcement action against them. This balance in the role of supervisors is a principal issue to address in the design of a partnership; in line with national circumstances, respective priorities and stakeholder perspectives.

Table 1: Different partnership arrangements for supervisors, FIUs and law enforcement agencies:

	Supervisors participate as permanent operational members	Supervisors do not participate as permanent operational members
FIU-hosted partnership (where the FIU is not also the AML supervisor)	- Austrian Public–Private Partnership Initiative (APPPI) - Finnish AML/ATF Expert Working Group on a PPP basis - South African Anti-Money Laundering Integrated Taskforce (SAMLIT)	- Joint Intelligence Group (JIG) Ireland - Latvia Cooperation Coordination Group (CCG) - The Netherlands Fintell Alliance (FA-NL) - New Zealand Financial Crime Prevention Network (NZ-FCPN)
FIU-hosted (where the FIU is also the AML supervisor)	- The US FinCEN Exchange - The Australian Fintel Alliance - The Malaysia Financial Intelligence Network (MyFINet) - Argentina Fintel-AR - Canadian 'Project' Initiatives to Combat Financial Crimes through Partnerships	N/A
LEA or prosecutor hosted[22]	- The UK Joint Money Laundering Intelligence Taskforce (JMLIT) - Hong Kong Fraud and Money Laundering Intelligence Taskforce (FMLIT) - The Netherlands Terrorist Financing Taskforce (NL-TFTF) - The Netherlands Serious Crime Taskforce (NL-SCTF)	- The Swedish Anti-Money Laundering Intelligence Taskforce (SAMLIT) - The Europol Financial Intelligence Public Private Partnership (EFIPPP)
AML supervisor as a principal partnership host	- The Singapore Anti-Money Laundering and Countering the Financing of Terrorism Industry Partnership (ACIP) - Lithuania - Centre of Excellence in Anti-Money Laundering	N/A

A6. Overview of Canadian financial information-sharing partnership arrangements

The following reproduces the overview of the awareness and targeted collaborative projects that were reported by Canadian public agencies in June 2020, as part of the FFIS international survey of financial information-sharing partnerships worldwide.[23]

Awareness Projects:

Awareness projects leverage a public–private model and typically employ a dual mandate of heightening general awareness amongst relevant groups (e.g. regulatory, anti-money laundering professionals, etc.) and increasing the number of STRs filed to FINTRAC on potential money laundering related to a specific predicate offence (e.g. human trafficking in the sex trade, fentanyl trafficking, etc.). These projects are designed with a vision to investigate the crime from a specific financial angle given the increased complexity of the predicate offences chosen.

The composition of the partners who participate in public–private awareness projects may vary based on the underlying predicate offence that is being addressed.

For example, Project Protect includes participation from non-governmental organisations (NGOs) that provide front line services to survivors of human trafficking. While Project Chameleon benefits from the participation of the Canadian Anti-Fraud Centre.

However, although certain participants can vary, major reporting entities in Canada, such as banks, the federal police (RCMP) and the national FIU (FINTRAC), are considered foundational partners for all awareness projects.

[23] https://www.gcffc.org/survey-report-five-years-of-growth-in-public-private-financial-information-sharing-to-tackle-crime/

Table 2. Overview of Canadian awareness projects: **All projects are public–private.

Project Code Name	Year Launched	Focal Predicate Offence	Targeted Underlying Activity	Project Outputs (disclosure data up to June 2020)
Protect	2016	Human Trafficking	Sexual Slavery and Forced Labour	• Indicators Published • Partnership Overview Published • In 2019-20, FINTRAC provided 251 disclosures of financial intelligence to Canada's police forces in relation to Project Protect • New Indicators to be published in 2020
Chameleon	2017	Fraud	Romance Fraud	• Partnership formed between FINTRAC and the Canadian Anti-Fraud Centre • Indicators Published • In 2019-20, FINTRAC provided 74 disclosures of financial intelligence to Canada's police forces in relation to Project Chameleon
Organ	2017	Organ Trafficking	Organ Trafficking or trafficking of persons for the purpose of organ removal.	• Derivative of Project Protect. • Indicators published via industry partner. • Project Organ will be presented at the OSCE's Expert Meeting On Combating Trafficking in Human Beings for the Removal of Organs in July 2020.
Guardian	2018	Drug Trafficking	Fentanyl Trafficking	• Partnership Overview Published • Indicators Published • In 2019-20, FINTRAC provided 134 disclosures of financial intelligence to Canada's police forces in relation to Project Guardian.
Athena[24]	2019	Fraud / Drug Trafficking	Money Laundering via underground banking in casinos/ real estate, luxury vehicles and high-value goods.	• Partnership Overview Published • Indicators Published (December 2019) • In 2019/2020, FINTRAC provided 52 disclosures of financial intelligence to Canada's police forces in relation to Project Athena.
Shadow	2020	child sexual exploitation material (CSEM/CSAM)	Child pornography	• Partnership Overview (Published) • Indicators (December 2020) • 30 Disclosures at time of the Operational Alert[25]

[24] See below a further description of the development of Project Athena to the Counter-Illicit Finance Alliance (CIFA) BC initiative.

[25] https://www.fintrac-canafe.gc.ca/intel/operation/exploitation-eng

Targeted projects in Canada:

Targeted projects in Canada refer to investigations traditionally launched by law enforcement for the purpose of investigating specific criminal organisations, enterprises or activities. These projects tend to flow in reverse of awareness projects; awareness projects begin with research and indicator creation to enhance reporting on underreported predicate offences and cumulate with targeted investigations, while targeted investigations are specifically launched to address a specific criminal offence suspected of being perpetrated. However, like awareness projects, targeted projects also leverage public–private or public-public partnerships to assist with investigations due to their transnational and/or complex nature. Additionally, targeted projects can also conclude with the creation of typologies or indicators that could spawn new investigations of a similar nature. Targeted projects see various forms of interaction between the public and private sectors, ranging from FINTRAC's proactive disclosure of STRs to law enforcement agencies, the issuance of court orders by law enforcement to private sector entities to obtain information directly and finally, briefings from law enforcement agencies on certain disclosable pieces of information pertaining to open investigations, to entities such as banks, to enhance the quality of intelligence submitted via STR.

Table 3. Overview of successful 'Targeted Projects' executed in 2019/20:

Project Name	Targeted Predicate Offence	Primary Agencies Involved	Overview (correct as at June 2020)
Hobart	Fraud, illegal gambling	Ontario Provincial Police (OPP), Canada Revenue Agency (CRA), FINTRAC	28 individuals charged with 228 offences including Hells Angels Seizure included: Seven residences and two vacation properties valued at just over CAD$8.1-million; financial accounts holding a total of more than CAD$1.2-million; 18 vehicles. Official Press Release http://opp.ca/news/#/viewmediakit/5dfb8083e1ba8
Octavia	Fraud/ (telephone scam)	RCMP, Canada Revenue Agency (CRA), FINTRAC	Media – Official Press Release. https://www.rcmp-grc.gc.ca/en/news/2020/rcmp-arrest-scammers
Highland	Trafficking multiple kilograms of cocaine, opioids	Winnipeg Police Service, OPP, FINTRAC	Ten adults were arrested and charged with 34 criminal code offences related to conspiracy and trafficking of a controlled substance, proceeds of crime, unlawful possession of cannabis. Media – Official Press Release https://winnipeg.ca/police/press/2019/12dec/2019_12_23.aspx
Cairnes	Trafficking of cannabis, fentanyl, cocaine, contraband tobacco	OPP, the Royal Canadian Mounted Police, Ontario and British Columbia finance ministries, and FINTRAC.	16 charged in OPP-led probe into trafficking of cannabis, fentanyl, cocaine, contraband tobacco http://media.zuza.com/f/2/f2a978a7-f9a7-4f03-891b-f279b2f7c127/ADDENDUM_OF_CHARGED_PERSONS_-_CAIRNES_FINAL.pdf

			https://www.toronto.com/news-story/10020899-16-charged-in-opp-led-probe-into-trafficking-of-cannabis-fentanyl-cocaine-contraband-tobacco/
Declass	Drug trafficking network	RCMP, FINTRAC, the Manitoba Liquor & Lotteries Corporation, the Seized Property Management Directorate, Health Canada, the Calgary Police Service, the Regina Police Service, as well as RCMP investigators in British-Columbia, Alberta, Saskatchewan, and Ontario. In addition to the DEA and CBSA.	The 16-month investigation led to nine search warrants, the arrest of eleven individuals, the seizure of five vehicles and over CAD$100 000 in financial seizures. It also resulted in the seizure of 22 kilograms of methamphetamine and 43 kilograms of cocaine, which have an estimated street value of CAD$6.5 million dollars. This represents the largest amount of methamphetamine seized in an organised crime investigation in Manitoba history. http://www.rcmp.gc.ca/en/news/2019/federal-rcmp-execute-nine-search-warrants-seize-substantial-amount-meth-and-cocaine

In addition, New Integrated Money Laundering Investigative Teams (IMLITs) were announced in the June 2019 Communique[26], covering British Columbia, Alberta, Ontario, and Quebec.

[26] https://www.canada.ca/en/department-finance/news/2019/06/joint-statement--federal-provincial-and-territorial-governments-working-together-to-combat-money-laundering-and-terrorist-financing-in-canada.html

A7. The Canadian Proceeds of Crime (Money Laundering) and Terrorist Financing Legislative Landscape[27]

The Canadian Charter of Rights and Freedoms guarantees the right to be secure from unreasonable searches and seizures. Parliament is, however, permitted to authorise reasonable searches and seizures in furtherance of legitimate public concerns, with reasonableness being assessed contextually by reference to objective notions of reasonable expectations of privacy. Respecting this fundamental right, the Canadian AML/ATF Regime is designed to deter criminals and terrorist financiers from using financial institutions and other entities for their criminal purposes and to provide appropriate tools to law enforcement to combat money laundering and terrorist financing, while also respecting the privacy rights of individuals and minimising the compliance burden on reporting entities.

As set out in Canada's Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA), Financial Transactions and Reports Analysis Centre (FINTRAC) was created as a stand-alone agency, separate from police, whose function is to receive reports from reporting entities, to analyse these reports and other information and, subsequently, to disclose financial intelligence to police. FINTRAC does not have any investigative authority with respect to money laundering, and therefore does not have the authority to compel reporting entities to provide information that is not reported. However, similar to frameworks in other geographical locations, law enforcement has the capability to gather additional information through separate methods such as production orders or subpoenas.

FINTRAC is an intermediary, created to ensure and safeguard the privacy provisions of citizens, so that there is vetting of information and that only high-level information will be submitted to police. Regarding Suspicious Transactions Reports (STRs), the Proceeds of Crime (Money Laundering) and Terrorist Financing Suspicious Transaction Reporting Regulations prescribe:

- the entities that are subject to Part 1 of the Act;
- the information that must be in a suspicious transaction report and a terrorist property report;
- the time limits and the format of the reports; and
- the 'designated information' which FINTRAC can disclose.

FINTRAC provides guidance to reporting entities on their transaction reporting requirements[28] and there are mechanisms for reporting entities to seek clarifications from FINTRAC on specific questions relating to legislative and regulatory requirements. The following excerpts from the Guidance further explain when an STR must be filed and what information must be included:

> *The requirement for you to report a suspicious transaction applies if you have reasonable grounds to suspect. "Reasonable grounds to suspect" is determined by what is reasonable in your circumstances, including normal business practices and systems within your industry. This applies not only when the financial transaction has been completed, but also when it has been attempted. There is no monetary threshold for making a report on a suspicious transaction. A suspicious transaction may involve several factors that may on their own seem insignificant, but together may raise suspicion that the transaction is related to the commission or attempted commission of a money laundering offence, a terrorist activity financing offence, or both. The context in which the transaction occurs or is attempted is a significant factor in assessing suspicion. This will vary from business to business, and from one client to another. An assessment of suspicion should be based on a reasonable evaluation of relevant factors, including the knowledge of the customer's business, financial history, background and behaviour. All circumstances surrounding a transaction should be reviewed.*

[27] The following section is reproduced from an unpublished FFIS survey and report into interpretations of Canadian AML/CFT information sharing, originally prepared in April 2018.

[28] http://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/1-eng.asp

A8. The Canadian privacy regime[29]

The Canadian Charter of Rights and Freedoms ("the Charter") is a fundamental law that provides constitutional protection for human rights. This includes the right to life, liberty and security of the person under section 7, the right to be free from unreasonable searches and seizures under section 8, and equality before and under the law under section 15. All laws and government actions at both the federal and provincial levels must conform to the Charter, which can be enforced by the courts. As a part of Canada's Constitution, the Charter takes precedence over other laws and sets limits on government action.

At the federal level, Canada's privacy framework includes two central privacy statutes. The Personal Information Protection and Electronic Documents Act (PIPEDA) provides the basic legal framework for the private sector, setting out how companies are to protect and manage personal information in the context of commercial activities. The Privacy Act provides the basic legal framework for the collection, retention, use and disclosure of personal information by government institutions.

All government activity, whether authorised by statute or by common law, are subject to the restrictions in the Charter. In addition, Government treatment of personal information is always subject to a framework of public sector laws. Some of these laws provide specific authorities for government to collect, use, retain or disclose personal information for particular purposes.

The independent judiciary provides jurisprudence interpreting government authorities and civil rights. Individuals have access to specialised oversight mechanisms such as the Office of the Privacy Commissioner of Canada, the Office of the Auditor General of Canada, as well as the several bodies that review the actions of core national security agencies (e.g. the Security Intelligence Review Committee, and the Civilian Review and Complaints Commission of the Royal Canadian Mounted Police).

Government departments are required to exercise their legal authorities in accordance with policies and guidelines established by the President of Treasury Board, as designated Minister, and in compliance with regulations, if any are promulgated under statutes. In Canada's legal system, decisions of courts on matters of public law are considered binding precedents that must be followed by future instances of courts, and by officials charged with applying the law. As a result, over time, courts develop binding interpretations of legislative text that are often more restrictive than what the apparently broad language of a statute might suggest. These interpretations are influenced by both the common-law principle that laws that have the effect of limiting rights tend to be interpreted restrictively, and that interpretation should be informed by the Charter. Canadian legislation must therefore be read in conjunction with applicable jurisprudence in order to ascertain the true effect of a given provision.

In short, Canada features a data protection framework governing the private sector and also a framework governing the public sector which are best understood in light of the Canadian legal system where activities of government are subject to the Rule of Law, requirements of reasonableness, compliance with balanced statutory limits, oversight institutions and internal compliance mechanisms.

[29] The following section is reproduced from an unpublished FFIS survey and report into interpretations of Canadian AML/CFT information sharing, originally prepared in April 2018.

Canada’s Private Sector Privacy Law (PIPEDA)

The Personal Information Protection and Electronic Documents (PIPEDA) is Canada’s federal statute for privacy and data protection in the private sector and establishes legal equivalence for electronic documents. Part I of the Act sets the legal requirements for the protection of personal information in Canada. It applies to every organisation that collects, uses or discloses personal information in the course of commercial activities. The Act does not apply to public sector organisations, which are governed by the Privacy Act, or to those that are regulated by the public sector at the provincial level.

PIPEDA sets limits on the collection, use and disclosure of personal information by organisations. It also sets out limited and specific conditions under which organisations disclose personal information to government institutions and law enforcement. Enforcement of PIPEDA relies on an ombudsman model, with oversight and redress mechanisms provided through the Office of the Privacy Commissioner of Canada (OPC) and the Federal Court. The OPC operates as the federal data protection authority with the mandate to protect and promote the privacy rights of individuals.

PIPEDA came into force on January 1, 2001. The Act balances the individual’s right to privacy with the need of organisations to collect, use or disclose information for legitimate business purposes. It is based on a set of ten privacy principles. Like the OECD Privacy Guidelines on which it was based, PIPEDA is a principles-based framework that has remained intact with legislative amendments made to only specific aspects to improve its effectiveness. New legislation has been proposed that would replace PIPEDA, if implemented (Bill C-11, tabled November 17, 2020).

“Substantially Similar”

In order to facilitate the development of harmonised federal and provincial privacy laws, PIPEDA includes a provision allowing for provincial statutes to be deemed “substantially similar” under the Act. A formal process for the determination of substantially similar laws has been established whereby laws are deemed substantially similar to PIPEDA if they “provide privacy protection that is consistent with and equivalent to that found under PIPEDA, incorporate the ten principles in Schedule 1 of PIPEDA, provide for an independent and effective oversight and redress mechanism with powers to investigate, and restrict the collection, use and disclosure of personal information to purposes that are appropriate or legitimate.”

Provinces with such legislation are exempt from PIPEDA which allows for the collection, use or disclosure of personal information to be governed by provincial law. However, PIPEDA continues to apply to the collection, use or disclosure of personal information with respect to federal undertakings and to the collection, use or disclosure of personal information outside of the province. Several provincial laws have been granted the substantially similar designation, applying either generally to personal information holdings of organisations within the province, or to personal health information only.

Quebec, Alberta and British Columbia have passed their own private sector privacy laws. Quebec’s law was deemed substantially similar to PIPEDA in 2003 with Alberta and British Columbia’s laws being recognised in 2004. On this basis, any discussion of information sharing involving financial institutions that are not federally regulated, should factor in privacy legislation in those provinces with substantially similar legislation.

Provisions in PIPEDA Related to Information Sharing – General

PIPEDA allows organisations to collect and use personal information without consent whenever such collection and use is reasonable for purposes related to investigating a breach of an agreement or a contravention of Canadian law; and it is reasonable to expect that obtaining consent would compromise the investigation (see paragraphs 7(1)(b) and 7(2)(d) of PIPEDA). However, the Act has different rules when it comes to the ability of an organisation to disclose personal information without consent for these purposes.

Specifically, it provides that an organisation may disclose personal information without consent if the following conditions are met. First, the disclosure may only be made to another organisation – not a government organisation or part thereof. Disclosures of personal information without consent to government organisations (such as law enforcement) are covered by paragraphs 7(3)(c); 7(3)(c.1); and 7(3)(d). Second, the information being disclosed must be for the purpose of conducting an investigation into a breach of Canadian law or into the breach of an agreement (such as a contract), and it must be reasonable for these purposes. Third, the investigation must be legitimate; it must pertain to a contravention or breach that has occurred, is occurring, or is about to occur. Finally, it must be reasonable to believe that informing the individual involved and obtaining their consent for the disclosure would compromise the investigation.

Also to note is that, even though information-sharing may occur in specified circumstances without consent, an organisation is still required to fulfill its other PIPEDA obligations, including but not limited to, limiting the disclosure of personal information, safeguarding it, and ensuring that any disclosure of personal information is only for purposes that a reasonable person would consider are appropriate in the circumstances.

PIPEDA Exceptions to Consent for Information Sharing - Additional Detail and Historical Context

In 2015, there were changes made to section 7 of the Act with respect to disclosure of personal information between organisations without the knowledge and consent of the individual. Previously, information sharing between organisations was governed by an investigative bodies regime, where organisations designated under the Act as an investigative body were able to disclose personal information to other investigative bodies. This regime was repealed and replaced with specific circumstances under which information can be shared. These include disclosures for the purposes of investigating a breach of agreement, contravention of law, or for detecting, suppressing or preventing fraud.

Paragraphs 7(3)(d.1) and 7(3)(d.2) of the Act, which respectively pertain to conducting private sector investigations and anti-fraud activities, provide that an organisation can disclose personal information without consent to another organisation, as distinct from a government institution. PIPEDA provides for conditions to be satisfied to lawfully make use of any of these exceptions.

Regarding paragraph 7(3)(d.1), the information being disclosed must be for the purpose of conducting an investigation into a breach of an agreement or a contravention of the laws of Canada or a province and, it must be reasonable to expect that informing the individual involved and obtaining their consent for the disclosure would compromise the investigation. It must pertain to a contravention or breach that has occurred, is occurring, or is about to occur. Information cannot be disclosed simply because the contract or agreement may be violated or contravened. As with various other terms used in PIPEDA, there is no specific definition for the "purposes of investigating". Therefore, as with all terms not defined in legislation, the rules of statutory interpretation would apply. Also to note is that the provision does not oblige organisations to survey their personal data collections with a view to finding criminal activity, but merely ensures that the data protection provisions do not preclude them from acting on reasonable grounds.

With respect to paragraph 7(3)(d.2), the information being disclosed without consent must be for the purpose of legitimate prevention, detection, or suppression of fraud that is likely to be committed, and, second, it must be reasonable to expect that informing the individual and obtaining their consent for the disclosure would compromise the ability to combat fraud.

In March 2017, the federal Office of the Privacy Commissioner (OPC) issued guidance that focusses on sections 7(3)(d.1) and (d.2.) of the Act. See https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/gd_d1-d2_201703/. The guidance states that paragraphs 7(3)(d.1) and 7(3)(d.2) are not to be applied in an overly broad manner, do not allow for widespread disclosures and casual sharing of personal information and are limited to certain purposes, under defined circumstances, and given specific conditions. It further states that in overseeing these provisions, the OPC will expect organisations to carry out due diligence and exercise good judgment when availing themselves of these exceptions, carefully consider each of the requirements explicitly outlined in the provisions and take care to ensure the limits set out in these provisions are respected. The guidance also indicates that organisations should demonstrate due diligence, ensure accountability and openness, identify procedures for handling access requests, and consider other PIPEDA requirements, as well as ways to improve transparency and consumer trust.

The OPC has also issued some PCMLTFA related guidance materials offering information to help customer-facing staff balance customers' privacy rights with the organisation's PCMLTFA reporting requirements (https://www.priv.gc.ca/en/privacy-topics/public-safety-and-law-enforcement/financial-transaction-reporting/faqs_pcmltfa_02/) and a Q&A for businesses on how the PCMLTFA affects privacy obligations under PIPEDA (https://www.priv.gc.ca/en/privacy-topics/public-safety-and-law-enforcement/financial-transaction-reporting/faqs_pcmltfa_01/.)

Relevant Jurisprudence

In 2013, in R. v. Vu, the Supreme Court of Canada confirmed that a warrant to search a physical location cannot implicitly authorise the searches of electronic devices such as computers found at that location. Because of the significant amounts of personal data that they can contain, computers and similar devices may only be searched if the judge issuing the search warrant has specifically authorised this. That is to say, the judge must be satisfied that there are reasonable grounds to believe that the computer to be searched will afford evidence of an offence.

In 2014, in R. v. Spencer, the Supreme Court of Canada examined whether internet service providers could provide police with the identity of a subscriber associated with the use of a particular Internet Protocol address at a particular time, in response to a non-binding request from police officers. The Court found that the reasonable expectations of privacy enjoyed by internet users included an expectation of anonymity, given that an IP address can, when associated with an identity, reveal highly personal information about an individual. Since the obtaining of subscriber identity information engaged a reasonable expectation of privacy, reasonable lawful authority was required. The court found that subparagraph 7(3)(c.1)(ii) of PIPEDA did not constitute lawful authority, as it only allowed organisations to release data to police where the police had lawful authority to acquire it. In other words, police require independent reasonable lawful authority to obtain such information from ISPs.

In 2017, in R. v. Orlandis-Habsburgo the Ontario Court of Appeal revisited the Supreme Court of Canada decisions in R. v. Spencer, R. v. Gomboc and R. v. Plant. The case involved the routine sharing of energy consumption data between an electricity provider and the police. The Court found that, contrary to a situation where a company took specific data to the police with concerns that it revealed a crime had been committed, the informal nature of the information-sharing arrangement that Horizon had with the police did not comply with PIPEDA. In this case the police and Horizon had an ongoing relationship when it came to the sharing of customer data. Justice Doherty noted that until the proceedings in this case commenced, Horizon had never refused a request from the police for information and found that this established that the police and Horizon were working in tandem. He noted this was important as this distinguished the situation from one where a company or whistleblower took specific data to the police with concerns that it revealed a crime had been committed. In its decision, the Court considered the exception in subparagraph 7(3)(c.1)(ii) of PIPEDA and found that the informal information-sharing arrangement between the energy provider and the police failed to conform with that requirement. Furthermore, the Court found the exception in subparagraph 7(3)(d)(i) of PIPEDA, which allows an organisation on its own initiative to disclose personal information to a government institution on "reasonable grounds to believe that the information relates to a contravention of the laws of Canada," does not permit informal information sharing with police.

A9. Key identified strengths within the Canadian AML/ATF financial information sharing regime

This briefing paper is generally focused on highlighting AML/ATF information-sharing challenges, with corresponding examples of how similar challenges have been, or are being, addressed in other countries. However, through the course of identifying information-sharing challenges, FFIS identified a wide range of strengths in the Canadian AML/ATF information-sharing regime, both those raised in interview and in literature review.

The list below represents highlights of those findings. The list is not intended to be an exhaustive review of strengths of the Canadian AML/ATF information-sharing regime. Key strengths identified include:

a) Over the course of recent FINTRAC Annual Reports, there is clear evidence that FINTRAC are continually striving to improve the availability of information with which to understand the Canadian AML/ATF regime;
b) In particular, FINTRAC has substantially increased the number of case-studies within its Annual Report to identify the law enforcement outcomes associated to AML/ATF financial intelligence and to highlight relevant law enforcement action (associated to financial intelligence) in email alerts to REs;
c) The major performance data gaps for the AML/ATF regime relate to activity which is outside of FINTRAC's mandate.
d) Particularly in 2019, the Canadian federal budget put forward a wide range of new funding and cross-government initiatives to address various aspects of economic crime.
e) The PCAMLTFA statutory review is a wide-ranging and robust strategic process for identifying recommendations to enhance the AML/ATF regime. Much of this FFIS study raises challenges that the statutory review had identified in 2018.
f) The Department of Finance 'Departmental Results' annual filings to the Parliament of Canada provide a relatively detailed description of cross-government expenditure and (activity-based) results.
g) Canada benefits from numerous operational or working group forums that bring together key government stakeholders relevant to an economic crime threat.
h) FINTRAC supervisory assessment guidance makes clear that the Operational Alerts, many of which are linked to public/private partnership project initiatives have significance from a supervisory/examination perspective.
i) Canadian PPP 'project initiatives' have fostered a strong culture of collaboration between public and private sectors and cross-government engagement in the concept of public/private financial information-sharing;
j) Individual PPP project initiatives are associated to significant results in terms of stimulating a response in STR reporting;
k) Project Athena, in particular, has demonstrated the viability of creative and innovative forms of information-sharing, bringing together a wide range of public agencies and multiple regulated sectors to achieve results of direct relevance to law enforcement.
l) RCMP are highly engaged in a range of industry and PPP initiatives to address economic crime threats;
m) Large REs report very collaborative engagement with RCMP.
n) CAMLOs in the largest REs in Canada engage in regular dialogue to share information at a strategic level on financial crime threats and have created a highly collaborative environment between the largest REs.
o) Canada has achieved successful arrangements tackling in cyber and fraud threats, including through private/private sharing and RCMP to financial institution sharing.
p) FINTRAC has published an over-arching strategy 2019-24, which – at a level of ambition at least – engages with many of the challenges identified in this study.
q) The ACE Fusion initiative is well positioned to respond to many of the information-sharing and strategic direction concerns that have been raised in this study. There are high levels of industry enthusiasm for what the ACE Fusion Team could achieve in Canada.
r) The CIFA demonstrates RCMP commitment, in particular, to supporting more coordinated activity at both federal and provincial level to engage with REs and support operational outcomes (and potentially inform policy)

FINTRAC Annual Reports offer a wider understanding of a range of activity and innovation with regard to international level leadership and engagement in trans-national projects, internal capacity building within FINTRAC, compliance outreach and FINTRAC's broader supervisory activities, all of which fall outside of the scope of this study into information-sharing.

A10. Overview of challenges to the effectiveness of the Canadian regime identified in this paper

Over the course of this research and, in particular, through the 16 interviews with senior individuals in REs or advising REs across multiple sectors, the following key challenges for Canadian AML/ATF information-sharing were identified in relation to the following eight themes.

- Theme 1. Data to understand the effectiveness and efficiency of the AML/ATF system;
- Theme 2. A strategic understanding of threats and a strategic approach to addressing economic crime;
- Theme 3. Prioritisation of economic crime threats;
- Theme 4. Public-private tactical financial information-sharing;
- Theme 5. The extent of public/private co-production of strategic financial intelligence;
- Theme 6. Relevance to law enforcement outcomes;
- Theme 7. Private-private financial information sharing to detect crime; and
- Theme 8. Mitigating the negative impacts of account closures.

Table 4. AML/ATF information-sharing theme and key challenges identified in Canada.

Theme	Current key challenges identified
Theme 1. Data to understand the effectiveness and efficiency of the AML/ATF system;	There is very limited data available to understand the outcome effectiveness of the Canadian AML/ATF system or to guide policy making and supervisory direction to ensure that regulated activity is contributing towards intended outcomes. Beyond industry estimates, there is no official estimate for the cost of compliance by the private sector with the Canadian AML/ATF regime. Accordingly, there is no evidence of Canadian authorities seeking to ensure the cost-effectiveness of the Canadian AML/ATF regime nor seeking to encourage private sector resources to be allocated in the most efficient way to support the desired outcomes of the AML/ATF system. Where performance monitoring does take place, it does not look at the AML/ATF system as a whole eco-system; considering private sector activity, the role of supervision and intelligence development, and law enforcement/criminal justice outcomes collectively.
Theme 2. A strategic understanding of threats and a strategic approach to addressing economic crime;	Publicly available economic crime threat assessments in Canada are scarce. The available evidence suggests that the current Canadian AML/ATF regime is deficient; unable to demonstrate an effective impact relative to the likely scale of economic crime in Canada, very costly to implement and resulting in a very high data collection footprint on Canadian society. Beyond the 2018 PCMLTFA statutory review recommendations, the Government of Canada has not published economic crime strategy for policy reform, nor an operational target operating model for how the range of relevant public agencies and REs should operate and share information in the AML/ATF regime in order to be more effective.

Theme 3. Prioritisation of economic crime threats;	Individual economic crime threats do receive funding and government profile. However, at a broader level, economic crime threats in Canada are not prioritised or communicated in terms of priorities at the national cross-government level. The National Inherent Risk Assessment (NIRA) for ML is almost 5 years out of date. The extent of threat assessments appears to be low and not provided at a national comprehensive basis. Beyond the 2015 NIRA, there are no publicly stated and regularly reviewed national economic crime threat priorities, which are established and supported by a range of relevant agencies in Canada. The private sector therefore lack clear signals to prioritise limited analytical resources and personnel towards specific crime threats and may fail to build up subject matter expertise and efficiently allocated resources towards threats which may be relatively more important for enforcement agencies. In the absence of any other form of prioritisation signals, it is likely that prioritisation on financial crime threats within major regulated entities is primarily influenced by the topics raised in supervisory enforcement action. The current NIRA led by the Department of Finance, operational priorities through PPP project initiatives and other FINTRAC guidance only partially align and it is not clear what relationship these priorities have to the priorities of law enforcement, Public Safety or the National Coordinating Committee on Organized Crime. In a system with limited resources, both in terms of public and private sector resources, there is no concerted effort to marshal resources towards specific outcomes.
Theme 4. Public-private tactical financial information-sharing;	Canadian public-private tactical financial information sharing does not benefit from a specific enabling legal framework which is designed for purpose. As a result, Canadian public-private financial information-sharing suffers from limitations due legal uncertainty or legal constraints. Most significantly, current Canadian public-private financial information-sharing ‘project initiatives’ have not facilitated the sharing of ‘tactical’ information; i.e. specific names or entities (identifiable information) of relevance to investigations. As such, the impact of public-private information sharing for direct benefit to law enforcement investigation is substantially reduced compared with arrangements in the U.S., the UK, Australia, New Zealand, the Netherlands, Sweden, Ireland, Hong Kong, Malaysia, South Africa and Singapore. FINTRAC is unable to share tactical information related to their STR intelligence back to regulated entities or to request follow up information from regulated entities on the STRs filed. RCMP and law enforcement agencies have a (potential and perceived) lawful basis for tactical information-sharing to regulated entities, however FFIS understands that there is no consensus amongst financial institutions on the extent to which the current legal framework allows for tactical information sharing between financial institutions and RCMP and other law enforcement agencies. Uncertainty around legal risk of public-private financial information-sharing is a principal barrier to the effectiveness of the Canadian AML/ATF regime in Canada.
Theme 5. The extent of public/private co-production of strategic financial intelligence;	Despite their success, the tempo and bandwidth of public-private co-production of strategic intelligence typologies in Canada is low compared to similar foreign jurisdictions. Canadian ‘project initiatives’ take approximately a year to develop and the Canadian approach has historically been restricted in bandwidth to commencing one PPP typology project per year.

Theme 6. Relevance to law enforcement outcomes;	While there have been isolated examples of RCMP-led financial information-sharing, there is no persistent national-level financial information-sharing partnership which is directed by law enforcement operational priorities. Without a strong steer from an operational user of intelligence, the existing Canadian project initiatives have historically struggled to achieve a sense of priorities and to ensure that users of intelligence have acted on the material produced by the project initiatives.
Theme 7. Private-private financial information sharing to detect crime; and	There is no clear legal gateway for regulated entities in Canada to permit the sharing of information with counterpart financial institutions relating to financial crime risks (prior to the determination of suspicion). Canadian regulated entities face privacy law and competition law restrictions which prevent financial crime risk (pre-suspicion) information sharing. The lack of a legal provision in Canada to support private-to-private sector information sharing to determine suspicion of money laundering undermines the detection of economic crime that spans multiple financial institutions.
Theme 8. Mitigating the negative impacts of account closures.	There is no facility or legal gateway in Canada to allow financial institutions to share information related to financial crime investigations post-suspicion. As a result, it is believed to be a regular occurrence that a 'de-marketed' customer who has been exited for financial crime reasons, will re-enter the financial system at an alternative point. In many cases, the financial institution that de-marketed the client will be able to observe the new financial institution which takes receipt of any remaining credit in the account being closed, but will not be able to provide any reference information to the new financial institution on that client. This process results in high-levels of duplication and ultimately does not provide a convincing preventative effect against criminals. However, when a law enforcement agency shares information with an RE in Canada, it may result in an account closure or other action which could undermine a law enforcement investigation. This will negatively affect trust and confidence in law enforcement sharing with REs. Canada does not have a formal account keep open request process.

Theme 1. Data to understand the effectiveness and efficiency of the AML/ATF system

Background:

Most countries have struggled to produce comprehensive data to evidence the effectiveness or efficiency of AML/ATF system in terms of outcomes.

Michael Levi, Peter Reuter and Terence Halliday, in a December 2017 academic study of five jurisdictions' national risk assessments, including Canada, concluded:

> *"Evaluation is a touchstone of contemporary policy making; good policy requires systematic and transparent evaluation. AML is just the kind of broad policy intervention that requires evaluation to improve its design and operation, if not to justify its existence. Despite the publication of national Mutual Evaluation Reports (MERs) and, more recently, National Risk Assessments, the fact is that there has been minimal effort at AML evaluation, at least in the sense in which evaluation is generally understood by public policy and social science researchers, namely how well an intervention does in achieving its goals.*[30]

Despite substantial time and resources within governments being expended in the preparation of National Risk Assessments and ahead of FATF mutual evaluations, no public agency in any of the jurisdictions studied in this paper is responsible for:

- Measuring the cost of the AML/CTF regime for both public and private sectors;
- Measuring what is achieved with that combined expenditure in a comprehensive way; and
- Evaluating to what extent priority AML/CTF objectives have been achieved on a regular basis.

This lack of information on outputs and outcomes associated to the AML/ATF system sits alongside a lack of official estimates on the cost of the system to implement. Available non-government estimates suggest that AML/CTF reporting regimes impose significant costs on regulated entities. In the US, according to a Lexis Nexis industry survey in 2019, US AML compliance costs for financial services firms amount to approximately US$26.4 billion annually.[31] In the UK, the most recent industry estimate indicates that financial crime compliance costs for banking are approximately £5 billion per year.[32] However, data on the private sector cost of AML/CTF obligations is generally absent from official assessments of national AML/CTF system.

[30] Michael Levi, Peter Reuter and Terence Halliday, 'Can the AML System Be Evaluated Without Better Data?', *Crime, Law and Social Change* (Vol. 69, No. 2, 2018), p310.

[31] LEXIS NEXIS Risk Solutions '2019 True Cost Of AML Compliance Study'

[32] British Banking Association, 'Detailed Evidence on the Criminal Finances Bill', November 2016, <https://publications.parliament.uk/pa/cm201617/cmpublic/CriminalFinances/memo/CFB05.pdf>, . This figure has been referenced by the FCA and the Law Commission in their analysis of reporting costs. See Megan Butler, 'A More Effective Approach to Combating Financial Crime', speech given at BBA Financial Crime and Sanctions Conference, delivered 20 September 2016, <https://www.fca.org.uk/news/speeches/more-effective-approach-combatting-financial-crime>, , and Law Commission, 'Anti-Money Laundering: The SARS Regime', <https://www.lawcom.gov.uk/document/anti-money-laundering-the-sars-regime/>,

Effectiveness challenges raised in interview:

**Please note that the following challenges raised in interview, as in all sections, refer to information or an interviewee's understanding as it was conveyed during the interview and may be out of date. Stated individual challenges below provide only a single perspective or opinion, unless otherwise stated. Use of the term "REs" refers to two or more interviewees.*

On outcome data availability…

The available data published by the Canadian government to understand the effectiveness of the AML/ATF system was described by an RE as "very limited".[33]

REs highlighting that there appears to be very little information to understand either the value or the cost of the AML/ATF regime in Canada.

REs referred to the lack of published information about how STRs are used by FINTRAC and by law enforcement agencies.

However, REs did also recognise the efforts on the part of FINTRAC to communicate through email alerts about individual news reports of successful law enforcement action.

On data collection across AML/ATF relevant agencies…

An RE interviewee, an individual with former senior-level experience within a relevant Canadian public agency, highlighted that, in many cases, outcome performance data is not being collected at source. The RE felt that there was a general measurement challenge across agencies and law enforcement agencies typically only produce data based on their internal use requirements.

The same RE highlighted that there appeared to be no public sector data collection strategy for the purposes of informing understanding about the effectiveness of the AML/ATF system as a whole, including the range of agencies who are potential users of FINTRAC disclosures. The RE believed that, outside of FATF evaluations, AML/ATF performance data is not being collected in Canada that covers all relevant agencies.

Multiple interviewees pointed to the relative strength of the FATF evaluation of Canada, as an exercise in drawing out relevant outcomes-focused data from the range of Canadian agencies, compared to the standard available data produced by Canadian agencies on an annual basis for domestic use.

Multiple REs stated that they believed that responding to FATF expectations and pressure ahead of a FATF evaluation was the key driver for performance data collection in Canada.

An interviewee claimed that Canada "doesn't have [AML/ATF regime] targets, and therefore the Government of Canada doesn't know what should be measured."[34] This was felt to be a challenge for Canada as "if Canada doesn't define [what Canada should be achieving], then others define it for Canada."[35]

[33] Interview reference line code - 3082
[34] Interview reference line code - 2039
[35] Interview reference line code - 3722

On current understanding of effectiveness challenges…

An RE stated that the extent to which law enforcement agencies actually act on disclosures from FINTRAC was very low, even for high-profile 'Project initiatives' and that this was Canada's "dirty secret".[36]

There is a widespread perception that the Canadian AML/ATF regime encourages volume of reporting above usefulness.

An interviewee believed that FINTRAC and the most recent regulatory reform package was encouraging more reporting from REs, resulting in more disclosures and more complex disclosures for law enforcement agencies, "creating vast supply of intelligence, but where, ultimately, there is low demand."[37]

An RE described that over-reporting on STRs is incentivised by FINTRAC rather than under-reporting due to the criminal and administrative penalties for under-reporting, but with no penalty for over-reporting.

Without data to understand effectiveness, an RE characterised the most recent reforms to the AML/ATF regulatory regime as focused on "increasing reports to FINTRAC"[38] without regard to the effectiveness or efficiency or intended outcomes of the system as a whole.

Multiple REs indicated a perception that FINTRAC is overloaded, in that they receive more information than they can process in a manner which would be relevant and timely in response to the potential criminality being reported.

With regard to the most recent regulatory amendments, an RE expressed that there was no effort on the part of policy-makers or FINTRAC to understand the anticipated marginal extra benefit of additional reporting being mandated against the cost of producing the additional information and the sustainability of the current approach to AML/ATF regulatory reform in Canada.

One RE described the Department of Finance cost estimates for the 2019 PCMLTFA regulatory updates (i.e. CAD$18,069,097 in costs over a 10-year period in 2018[39]) as a "not robust".[40]

An RE indicated that FINTRAC or the Canadian government should have a view on the effectiveness of the broader eco-system in terms of its performance reporting, including use and impact of disclosures.

REs would like to understand out of the body of the 30m+ transaction reports filed to FINTRAC every year, what proportion have value to users and in relation to what types of activity.

[36] Interview reference line code - 1223
[37] Interview reference line code - 1444
[38] Interview reference line code - 1509
[39] http://gazette.gc.ca/rp-pr/p1/2020/2020-02-15/html/reg1-eng.html
[40] Interview reference line code - 2156

The Canadian context – additional analysis:

In the Levi 2017 study, the Canadian National Inherent Risk Assessment (NIRA) was identified as particularly lacking in data to understand effectiveness. The Canadian NIRA included no estimates of the proceeds of crime (i.e. a macro-level understanding of the scale of the threat) and included 'minimal' enforcement data.[41]

The FINTRAC Annual Report provides information on the total numbers of STRs submitted by regulated entities and cases disclosed by FINTRAC to law enforcement, including breakdown percentages for the recipient agencies, relevant province and the nature of the underlying crime. However, information is not available to adequately determine the impact of that reporting; such as law enforcement investigations opened or existing investigations supported as a result of the FINTRAC disclosures, or prosecutions, assets seized and convictions obtained as a result of the disclosures.

FINTRAC discloses transaction types, and discloses proactively, not only in response to investigations.[42] However, the leading FINTRAC metric available relating to outcomes (beyond activity measures, such as disclosures to law enforcement), is the number of FINTRAC disclosures to contributing to "project-level investigations". In addition, FINTRAC also state that in the 2018-19 annual reporting period they received 318 "disclosure feedback forms" from law enforcement, "90 percent of which indicated that FINTRAC's financial intelligence was actionable", though not whether the reports were 'actioned' or the impact of the intelligence. In 2019-20, this figure for disclosure forms was 254 but "95 percent of which indicated that FINTRAC's financial intelligence was actionable".[43]

Table 5. Information provided by FINTRAC to support evaluation of the AML/ATF system

Performance metric	Performance data from the 2018-19 FINTRAC annual report[44]	Performance data from the 2019-20 FINTRAC annual report[45]
Large Cash Transaction Reports	10,055,099	9,738,058
Electronic Funds Transfer Reports	17,627,947	21,031,401
Suspicious Transaction Reports	235,661	386,102
Cross-Border Currency Reports/Cross-Border Seizure Reports	61,583	53,265
Casino Disbursement Reports	201,145	208,603
FINTRAC disclosures to law enforcement agencies	2,276	2,057
Contribution of FINTRAC disclosures to "project-level investigations"	296	393
Law enforcement investigations opened as a result of FINTRAC disclosures	No data available	No data available
Pre-existing law enforcement investigations supported by FINTRAC disclosures	No data available	No data available
FINTRAC disclosures not resulting in law enforcement action	No data available	No data available
Arrests linked to FINTRAC disclosures	No data available	Limited case studies
Prosecutions supported by FINTRAC disclosures	No data available	No data available

[41] See Table 1 Data Sources and Risk Assessment NRAs of Five OECD Member States in Michael Levi, Peter Reuter and Terence Halliday, 'Can the AML System Be Evaluated Without Better Data?', *Crime, Law and Social Change* (Vol. 69, No. 2, 2018), p323.
[42] https://www.fintrac-canafe.gc.ca/fintrac-canafe/1-eng
[43] https://www.fintrac-canafe.gc.ca/publications/ar/2019/1-eng#s1
[44] FINTRAC Annual Report 2018–19 https://www.fintrac-canafe.gc.ca/publications/ar/2019/1-eng#s1
[45] FINTRAC Annual Report 2018–19 https://www.fintrac-canafe.gc.ca/publications/ar/2019/1-eng#s1

Asset seizure supported by FINTRAC disclosures	No data available	Limited case studies
Convictions supported by FINTRAC disclosures	No data available	No data available

In 2019-20, the latest FINTRAC Annual Report includes a greater amount of information on law enforcement 'outcomes', through case studies, compared to 2019-18.

In the 2019-20 FINTRAC Annual Report 14 case studies of law enforcement action and outcomes are included. Collectively, these case studies indicate a number of arrests, charges, assets, firearms and drugs seized. This is a significant improvement in 'outcome-based' indications, but falls short of a comprehensive understanding of the impact of FINTRAC disclosures.

It is apparent from the development of FINTRAC's Annual Report in 2019-20, that FINTRAC are actively seeking ways to communicate more information about the impact of activity, beyond the disclosure activity statistics. In addition, the 2019-20 FINTRAC Annual Report included a list of qualitative feedback statements about the 'Value of FINTRAC Disclosures' from users of FINTRAC intelligence.

In its 2019-24 strategy, FINTRAC claims it has "renewed its emphasis on results and performance reporting transparency by strengthening indicators and providing clearer definitions of variables reported and tracked over time. This is part of its effort to optimize its effectiveness and efficiency in the delivery of its anti-money laundering and anti-terrorist financing mandate and better align its measurement of performance to government-wide standards."[46]

Table 6. Cumulative quantitative statistics available in the FINTRAC Annual Report 2019-20 related to law enforcement outcomes

Metrics (cumulative from case studies in the Annual Report):	Quantity
Arrests mentioned:	15
Charges mentioned (additional to arrest figures):	72
Firearms seized:	57
Vehicles seized:	56
Seizure in case, accounts and other assets	CAD$82.5m
Kilograms of narcotics	78

It seems unlikely that the 14 case studies in the 2019-20 FINTRAC Annual Report represent the total amount of law enforcement impact associated to FINTRAC reporting, however there are no other law enforcement outcome statistics (as opposed to activity-based or process-based statistics) to refer to beyond those mentioned in the case studies.

Overall, the amount of data available in FINTRAC's annual report is still low compared to similar jurisdictions and insufficient to understand the effectiveness or efficiency of the regime.

FINTRAC produces some additional performance indicators in the FINTRAC submission to the Departmental Results Report[47], which include "Percentage of FINTRAC's financial intelligence disclosures that align with partner investigative priorities" (where FINTRAC consistently scores 100%); "Percentage of feedback from disclosure recipients that indicates that the FINTRAC financial intelligence disclosure was actionable" (where FINTRAC achieved a 97% success rate in 2019–2020); "Percentage of feedback from proactive disclosure recipients that indicates that the independent analysis provided by FINTRAC was actionable" (90% score in 2019-20). While these performance metrics are clearly important for FINTRAC, it is not clear whether

[46] https://www.fintrac-canafe.gc.ca/fintrac-canafe/1-eng
[47] https://www.fintrac-canafe.gc.ca/publications/drr-rrm/2019-2020/drr-rrm-eng

‘actionable’ has a link to intelligence being ‘actioned’. As such, the measures fall short of helping a reader understand the outcomes associated to disclosures.

Despite improvements in 2019-20, the available FINTRAC data published in reference to the effectiveness of the AML/ATF is dominated by the inputs received by industry and disclosures out to law enforcement agencies, monitoring activity rather than outcomes.

It should be noted that this gap in performance data relates to data outside of FINTRAC’s direct responsibility. FINTRAC was created as an administrative FIU, and as such, does not possess the following mandate and related authorities:

i) Investigations of economic crimes
ii) Status and/or results of such investigations
iii) Provide statistics on economic crimes and/or advising RE’s on related crime threats

At a higher-level than FINTRAC, the Department of Finance Canada is responsible for providing the “Secretariat for management and coordination of Canada's AML/ATF Regime”[48] at a a cross-government level.

As part of this leadership role for the Canadian AML/ATF regime, the Department of Finance Canada provides an annual update to Parliament in its Departmental Results Report on the ‘horizontal initiative’ of “Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime”.[49]

Understanding the information available in the Department of Finance Canada Results Report on the AML/ATF regime

The Department of Finance Canada Results Report on the ‘horizontal initiative’ of “Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime” is a wide ranging and annual exercise to bring together performance information of the Canadian AML/ATF regime.

This report is relatively detailed and provides a cross-government[50] review of AML/ATF spending across 16 government programs, and details the expected results against each program, performance indicators, targets and actual results achieved. The 2018-2019 report contains 36 performance indicators and narrative text spanning 7,650 words relating to the effectiveness of the Canadian AML/ATF regime. This is a substantial level of transparency and a coordinated performance monitoring regime, covering agencies and departments across the Canadian government.

However, the overarching performance indicator for the entire ‘horizontal initiative’ is “Level of compliance with international standards and effectiveness in the prevention, detection, deterrence and disruption of money laundering (ML) and terrorist financing (TF).” Despite the wide-ranging record of results presented in the Departmental report, it is still not possible to come to a comprehensive understanding about the effectiveness of the prevention, detection, deterrence and disruption of money laundering and terrorist financing in Canada through this report.

A large number of individual program performance indicators relate to *activity*, such as the number of meetings attended for example, which are likely to have a contribution towards outcomes, but are not – by themselves – instructive in understanding outcomes and overall AML/ATF effectiveness. As FINTRAC is effectively an intermediary in the regime between the public and private sector, its performance indicators do not relate to the disruption outcomes intended for the AML/AFT system. The ‘action arms’ of the AML/ATF regime – the Public Prosecution Service of Canada (PPSC), the Royal Canadian Mounted Police

[48] https://www.canada.ca/en/department-finance/corporate/transparency/plans-performance/departmental-results-report/2019/supplementary-information-tables.html
[49] https://www.canada.ca/en/department-finance/corporate/transparency/plans-performance/departmental-results-report/2019/supplementary-information-tables.html
[50] Department of Justice Canada; Public Prosecution Service of Canada; Financial Transactions and Reports Analysis Centre of Canada; Royal Canadian Mounted Police; Canada Revenue Agency; Canada Border Services Agency.

(RCMP), the Canada Revenue Agency (CRA) and Canada Border Services Agency (CBSA) – do have indicators relating to the overall desired outcomes of the Canadian AML/ATF regime. However, from the entire 2018-19 results report on the AML/ATF regime, in terms of the outcome-based *results* relevant to disruption of economic crime, we learn only that:

i) In fiscal year 2018–19, the PPSC dealt with 6,886 new AML/ATF Regime-related charges: 6,842 were related to the possession of proceeds of crime; 43 were related to money laundering; one was laid under the PCMLTFA. There were no terrorist financing charges.

ii) Over the past fiscal year, FINTRAC received 318 completed disclosure feedback forms with the level of positive feedback from partners exceeding targeted levels. The Centre's contributions were also recognized publicly by several law enforcement agencies as providing valuable assistance to criminal investigations that led to successful disruption of money laundering schemes.

iii) In fiscal year 2018–19, 29% (45 out of 154) of all active tier 1 and tier 2 RCMP projects (including projects in court) had a money laundering component.

iv) From CRA, 24 audits took place and CAD$8.31 million of federal tax was reassessed.

v) CRA conducted 16 audits where a risk of terrorism financing was identified. As a result, three organizations had their charitable status revoked, while four were subject to a compliance agreement to maintain their charitable status, one of which was sanctioned with a penalty.

vi) In fiscal year 2018–19, CBSA has carried out 2,181 seizures for failing to properly declare currency and monetary instruments that meet the reporting threshold of CAD$10,000. The total value of the seized funds was over CAD$35.7 million, of which over CAD$2.7 million was forfeited to the Crown as suspected proceeds of crime and TF.

Wider Public Safety relevant information and provincial law enforcement indicators are not included in this reporting framework.

In summary, despite the array of material produced by the Canadian government with respect of the AML/ATF regime, there is a lack of information to meaningfully understand its effectiveness. Table 7 highlights the limitations of information available in the FINTRAC Annual Report 2019-20 and Department of Finance Results Report for the Canadian AML/ATF regime as a 'horizontal initiative' 2018/19 with respect to AML/ATF prevention; detection and disruption.

Table 7.

Theme	Information available in the FINTRAC Annual Report 2019-20 and Department of Finance Results Report for the Canadian AML/ATF regime as a 'horizontal initiative' 2018/19
Prevention:	The Canadian AML/ATF 'Prevention' objective is ill defined, but largely understood to relate to either (1) the formal financial sanctions regime[51] or (2) the AML/ATF 'preventative measures' taken by private sector REs which result in either a refusal to provide financial services to an entity or to exit an existing account holder (referred to as 'de-marketing' in Canada). There are no performance indicators relating to the formal Canadian economic sanctions regime available in the FINTRAC Annual Report or the Department of Finance Results Report for the Canadian AML/ATF regime as a 'horizontal initiative'[52]

[51] The Canadian economic sanctions regime is constituted by five federal statutes: Part II.1 of the Criminal Code (designations published by Public Safety Canada); United Nations Act; Special Economic Measures Act (SEMA); Freezing Assets of Corrupt Foreign Officials Act; and the Justice for Victims of Corrupt Foreign Officials Act (Sergei Magnitsky Law)

[52] Please note: the Canadian sanctions regime is outside the scope of this report

	The Canadian AML/ATF system is one that involves activity and outcomes across both public and private sectors. However, there are no performance indicators relating to the effectiveness of private sector RE 'preventative measures' activity in the Canadian AML/ATF regime available in the Canadian government performance or accountability material. This is despite the vast majority of total resources in the Canadian AML/ATF system being expended by REs. While there are some statistics available to understand FINTRAC compliance/supervision activity and the number of reports submitted by REs, these do not assist a policy maker to understand how effectively economic crime is being prevented from accessing the Canadian financial system (unless one assumes that compliance with the existing AML/ATF regime will equate to successful 'prevention'). For reasons outlined in "Theme 8" of this report, it is highly doubtful whether high-levels of compliance with the existing AML/ATF regime will result in meaningful preventative restrictions on illicit flows entering the Canadian financial system. Canadian policy makers would benefit from additional information on the scale of account closures or refused accounts by REs, as recorded by the UK JMLIT partnership or the Australian Fintel Alliance for example. Canadian policy-makers may also benefit from law enforcement intelligence analysis relating to whether the priority Canadian organised crime groups have been able to maintain financial services in Canada.
Detection:	While a number of performance indicators relate to 'detection' of ML or TF is some capacity – from publicly available material – policy-makers do not have a clear threat assessment document which describes the adequacy of the national intelligence picture in relation to priority economic crime threats.
Disruption:	Beyond the limited statistics referred to above in the Department of Finance Departmental Results Report for AML/ATF and the FINTRAC Annual Report information described above, it is not possible for a policy-makers to understand what level of disruption of criminal activity the AML/ATF regime is contributing to. Canadian policy-makers would benefit from regular performance information about the number of arrests, the number of prosecutions, convictions, the value of assets restrained and assets ultimately recovered in Canada, relevant to the AML/ATF regime.

Canadian media report on challenging statistics relating to the effectiveness of the overall Canadian regime. A Global News investigation found in February 2019:

> *"that Canada largely fails to effectively prosecute money-laundering cases, with just 321 convictions between 2000-2016. Roughly 809 cases were either stayed, withdrawn or dismissed, over that same time period, resulting in a conviction rate of around 27 per cent. Over the same time in B.C., just 10 people have been found guilty of money laundering since 2002, while Ontario has seen just 186 guilty verdicts since 2006."*[53]

[53] https://globalnews.ca/news/4939801/provinces-canada-fail-to-convict-money-laundering/

Meanwhile, FINTRAC STRs are growing exponentially; increasing 64% from the 2019-20 Annual Report from the previous year and with an average annual growth rate of 37% per year over the previous three years. The volume of case disclosures on to enforcement agencies by FINTRAC is consistently less than 1% of the volume of STR reports received, with the latest Annual Report indicating that disclosures are at approximately 0.5% of STR inputs. Though, it should be noted that a disclosure may contain reference to numerous STRs and potentially other data held by FINTRAC.

While FINTRAC do not offer an assessment of the cost of compliance with the AML/ATF regime in Canada that they supervise, a major 2019 industry survey by Lexis Nexis estimated that US$5.1billion was spent by Canadian financial services firms annually in AML compliance.[54]

The available information above, in a crude measure of impact, may lead us to infer that the AML compliance programme as a whole is delivering over 30 million reports of Canadian financial transactions to FINTRAC in 2019-20 - 386,102 of which are STRs – which (beyond a number of case studies) can only be linked to impact in terms of an (unknown depth of) contribution to 393 "project-level investigations". In addition, from case studies, we can note a contribution of FINTRAC reports towards operations that resulted in 87 individuals charged or arrested; 78 kilograms of narcotics seized; CAD$82.5m of assets seized and another 56 vehicles. While a number of ML charges are mentioned in the case studies, the vast majority of assets referred to are cash, vehicles or property. It is not clear the extent to which the AML/ATF regime is contributing directly to financial disruption, through money frozen in RE financial accounts and recovered for example, in addition to the contribution of more traditional policing seizure of fixed and tangible assets 'on the ground'.

In any case, we can set that outcome against the cost of the system to infer that the average cost to the private sector per single contribution to a project level investigation is approximately US$13million.[55] While this figure does not take into account the impact of the AML system which is unknown to FINTRAC or unreported by FINTRAC, the figure illuminates the current challenge in terms of lack of data about both effectiveness and cost of the current Canadian AML system.

Summary of key challenges in Canada:

- As described above, there is very limited data available to understand the effectiveness of the Canadian AML/ATF system or to guide policy making and supervisory direction to ensure that regulated activity is contributing towards intended outcomes.
- Beyond industry estimates, there is no official estimate for the cost of compliance by the private sector with the Canadian AML/ATF regime. .
- Accordingly, there is no evidence of Canadian authorities seeking to understand the cost-effectiveness of the Canadian AML/ATF regime nor seeking to ensure that private sector resources are being allocated in the most efficient way to support the desired outcomes of the AML/ATF system.
- Where performance monitoring does take place, it does not look at the system as a whole; considering private sector activity, the role of supervision and intelligence development, and law enforcement/criminal justice outcomes collectively, beyond a small number of case studies.
- The limited data that is publicly available indicates very poor returns on the amount of resources spent for the outcomes that are recorded.

Recent developments in Canada:

The Canadian 2019 budget provided funding to the ACE (Anti-money laundering action and co-ordination) Team of CAD$24 million. Indicating Government of Canada recognition of the challenges listed above, FFIS

[54] LEXIS NEXIS Risk Solutions '2019 True Cost Of AML Compliance Study'

[55] Calculated by the leading industry estimate of Canadian AML/ATF compliance spending (the '2019 True Cost Of AML Compliance Study' industry survey by Lexis Nexis indicating that US$5.1billion was spent by Canadian financial services firms annually in AML compliance) divided by the number of project investigations reported by FINTRAC (393 in 2020).

understands that the ACE Fusion Team will be prioritising the development of a performance measurement framework that strengthens reporting of activities and outcomes. The Department of Finance remains the lead Department with responsibility for performance measurement in terms of the AML/ATF regime.

International comparisons:

FINTRAC's performance reporting on outputs and outcomes associated to the AML/ATF reporting framework is limited compared to similar jurisdictions:

Table 8. Comparison of FINTRAC performance data relative to comparable jurisdictions and their respective public-private financial information-sharing partnerships.

\ Country **Performance metric**	Canada	UK FIU[56]	UK JMLIT[57]	Australian Fintel Alliance[58]	Hong Kong FIU[59]	Hong Kong FMLIT[60]
Volume of private sector reporting	✓	✓	✓	✓	✓	✓
FIU disclosures to law enforcement agencies	✓	✓	N/A (all are disclosed)	N/A (all are disclosed)	✓	N/A (all are disclosed)
Contribution of reporting to law enforcement investigations	Very limited	✗	✓	✓	✗	✓
Arrests linked to reporting	✗[61]	✗	✓	✓	✓	✓
Asset seizure linked to reporting	✗[62]	✓	✓	✗	✓	✓

As the table above indicates, relative to the FIU annual reports, respective tactical-level public-private financial information sharing partnerships such as the Australian Fintel Alliance, the UK JMLIT and Hong Kong FMLIT have achieved greater levels of clarity on the contribution of regulated entities to operational results. Canada does not benefit from a tactical-level (entity level) public-private financial information-sharing partnership, which will be discussed further in this report.

The AUSTRAC Corporate Plan 2019-2023 sets out a range of activity based short and medium-term targets and priority evidence categories to measure performance. As part of this plan, AUSTRAC supports a medium term (2020–23) intelligence objectives to explore opportunities to measure ML/TF harm and understand the impact of disruption efforts.[63]

Other recent international developments have also raised the standard of public agencies' performance monitoring frameworks with regard to AML/ATF systems.

The U.S. Bank Secrecy Act "Value Project" organised by the Financial Crimes Enforcement Network (FinCEN, U.S. Treasury) was established in early 2019 and is still underway. It aims to identify what value individual AML policy instruments from the Bank Secrecy Act have for specific stakeholders in terms of outputs, outcomes and costs.

[56] https://www.nationalcrimeagency.gov.uk/who-we-are/publications/390-sars-annual-report-2019/file
[57] https://nationalcrimeagency.gov.uk/what-we-do/national-economic-crime-centre
[58] https://www.austrac.gov.au/sites/default/files/2019-11/Fintel%20Alliance%20Annual%20Report%202018-19.pdf
[59] https://www.jfiu.gov.hk/info/doc/JFIU_Annual_Report_2018.pdf
[60]https://www.gcffc.org/survey-report-five-years-of-growth-in-public-private-financial-information-sharing-to-tackle-crime/
[61] While there is no summary national quantitative data, FINTRAC have increased the number of case studies of law enforcement action and outcomes in the Annual Report
[62] While there is no summary national quantitative data, FINTRAC have increased the number of case studies of law enforcement action and outcomes in the Annual Report
[63] https://www.austrac.gov.au/sites/default/files/2019-08/AUSTRAC_CorporatePlan_2019.pdf

In 2019, the Dutch Ministers of Finance and Justice and Security submitted a "joint action plan for the prevention of money laundering through the Dutch financial system and for tracking and prosecuting criminals and their enablers."[64] This plan set out the Dutch government's commitment to regular evaluations of the AML/ATF policy framework, understanding the effectiveness and shortcomings of the current regime so that "policy is risk-oriented and can be adjusted."[65]

The UK Economic Crime Plan 2019 to 2022[66] commits to improving UK "understanding the threat and performance metrics" as 'Strategic Priority One'. The Plan highlights "A better understanding of the threat plays a key role in enabling the public and private sectors to collectively prioritise the policy reforms and operational activity that deliver the highest impact in combatting economic crime… [and to] measure the impact of our collective actions to tackle economic crime."[67]

The UK has also developed a National Serious and Organised Crime Performance Framework, produced by the Home Office and NCA in conjunction with private stakeholders to identify a quantitative and qualitative approach to understanding the impact of the UK's overseas and domestic response to serious and organised crime. Overall, the UK Economic Crime Plan is accountable against the following 7 Key Performance Questions:

- KPQ 1: How comprehensive is our understanding of economic crime threats and vulnerabilities?
- KPQ 2: How effectively are we pursuing serious and organised economic criminals in the UK, online and overseas?
- KPQ 3: How effectively are we building resilience in the public and private sector against economic crime?
- KPQ 4: How effectively are we supporting those impacted by economic crime?
- KPQ 5: How effectively are we deterring people from involvement in economic crime?
- KPQ 6: How effectively are we developing core capabilities to address emerging economic crime threats?
- KPQ 7: How effectively and efficiently are we managing our resources in countering economic crime?

Opportunities to enhance the Canadian framework:

- Canada can benefit from a more comprehensive understanding of the effectiveness, efficiency and data privacy costs and benefits of the various components of the AML/ATF system;
- Canadian departments can collaborate to elevate performance reporting on the Canadian AML/ATF framework to a national cross-government exercise. FINTRAC's mandate is too limited to publish performance metrics that adequately reflect the inputs, outputs and outcomes to understand 'end-to-end' effectiveness in the AML/ATF system.
- An Economic Crime Disruption Annual Report could usefully be published to include relevant performance data from FINTRAC, law enforcement agencies, the Public Prosecution Service of Canada and, as far as possible, from regulated entities to understand outcomes from the AML/ATF system. Potentially, the ACE Fusion Team may be in a strong position to provide this function.
- In the absence of the above, FINTRAC may be able to extend the coverage of its annual performance monitoring to include greater coverage of outcome indicators from the use of intelligence and to include an official estimate of the cost of the reporting regime on the regulated sector. Such performance data will empower strategic decision making in Canada, and support accountability, to ensure that the AML/ATF system is delivering outcomes effectively and efficiently.

[64] https://www.rijksoverheid.nl/documenten/kamerstukken/2019/06/30/aanbiedingsbrief-plan-van-aanpak-witwassen

[65] https://www.rijksoverheid.nl/documenten/kamerstukken/2019/07/01/onderzoek-informatie-uitwisseling

[66] https://www.gov.uk/government/publications/economic-crime-plan-2019-to-2022/economic-crime-plan-2019-to-2022-accessible-version#strategic-priority-one-understanding-the-threat-and-performance-metrics

[67] https://www.gov.uk/government/publications/economic-crime-plan-2019-to-2022/economic-crime-plan-2019-to-2022-accessible-version#strategic-priority-one-understanding-the-threat-and-performance-metrics

- Improved outcome data relating to effectiveness and efficiency can drive a more effective response to crime in Canada at the policy level and inform changes at the operational level to improve investigations and asset recovery and achieve more efficient use of public and private sector resources within the AML/ATF system;
- In time, Canada can demonstrate a response from the outcomes in the AML/ATF system which is commensurate with the level of national economic crime threats.

Theme 2. A strategic understanding of threats and a strategic approach to addressing economic crime

Background:

In the FATF methodology for evaluating the effectiveness of AML/ATF systems, the first 'immediate outcome' of an AML/ATF system should be that "Money laundering and terrorist financing risks are understood and, where appropriate, actions coordinated domestically to combat money laundering and the financing of terrorism and proliferation."[68]

There are two components to this outcome:

1) Threats are understood; and
2) Coordination takes place at a national cross-government and sub-national level (and potentially including the private sector) to ensure actions respond to threats in a strategic manner

Such national coordination also needs to be flexible to changing underlying market and criminal realities to be relevant and effective.

Substantial and wide-ranging changes have occurred in technology, commerce, crime, digitisation and the nature of financial services since the fundamentals of the regime were established in 1989. FATF itself is engaged in a strategic review of the international standards regime and a number of countries are engaged in activity which is, in effect, re-evaluating the adequacy of current processes in terms of how they fulfil the national AML/ATF objectives and directing relevant policy and operational reforms.

Economic crime strategies, that bring together threat assessments, evaluations of the effectiveness and efficiency of the AML/ATF system and lay out an appropriate policy and operational response, have been developed to guide such reforms.

Effectiveness challenges raised in interview:

With regard to threats being understood…

In terms of understanding specific threats, the Canadian NIRA was described as "quite soft"[69], "neglected"[70] and "out of date".[71]

REs received briefings on threats in individual project initiatives, associated FINTRAC alerts and law enforcement in-person presentations to conferences or working groups.

However, multiple REs believed that there was very limited communication to REs on the nature and scale of economic crime threats facing Canada as a whole.

On RE, outside of the big 6, said, "the most useful thing we could get from FINTRAC would be more detail on threats within Canada".[72]

(Further relevant comments on threat identification are included in sections below; threat prioritisation (theme 3) and strategic intelligence (theme 7) are included in relevant chapters below.)

[68] https://www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%2022%20Feb%202013.pdf
[69] Interview reference line code - 4137
[70] Interview reference line code - 2167
[71] Interview reference line code - 1550
[72] Interview reference line code - 4684

With regard to strategic cross-government coordination to tackle economic crime…

Multiple interviewees believed that there was no apparent national economic crime strategy in place in Canada that links intelligence of the scale of specific economic crime threats with a statement of intent for how the crime threats will be addressed.

Some REs suggested that there was a lack of political will in Canada to drive a strategic approach to address economic crime in Canada. It was noted that the U.S. and the UK had focused on addressing policy and operational shortcomings in their AML/ATF regimes following major terrorist incidents.

An RE expressed a hope that in Canada "We shouldn't wait before something really bad happens to reform."[73]

At a policy level, multiple interviewees indicated that the Government of Canada appears to be led by responding to FATF observations and recommendations, with one RE describing this as a commitment to fulfil perceived FATF requirements "at any costs"[74], rather than by a domestically-driven set of priorities to meaningfully address economic crime in an effective or efficient way.

Over recent months, strategic discussions about reform of the Canadian AML/ATF regime have been perceived to be paused while the implementation details of the current regulatory updates are passed.

With regard to strategic challenges for Canadian AML/ATF information-sharing…

Overall, the following major policy challenges in terms of AML/ATF information sharing effectiveness were raised:

- the lack of capacity in FINTRAC to analyse the 30m + transaction reports they receive each year;
- the limited capacity of law enforcement to take forward proactive disclosures from FINTRAC;
- the poor timeliness of the reporting process, in relation to when the crime takes place and the time it takes for a disclosure to make its way to law enforcement agencies;
- the inability for law enforcement agencies to share with financial institutions information relevant to a case and to receive a timely and relevant response;
- the length of time it takes for law enforcement agencies to receive a response from a production order to REs;
- the inability for FINTRAC to request follow-up information from a RE in relation to a report;
- the inability of financial institutions to share information between each other to identify networks of criminal actors that are spread across multiple institutions; and
- the cost and duplication of risk-displacement caused by a single RE unilaterally de-marketing an account for AML reasons (exiting a risky entity for them only to open up an account elsewhere).

The strategic basis for Canadian information-sharing projects was described as being a "goodwill"[75] type of a regime, based on "passion projects"[76] and lacking a strong governance model. Canadian

[73] Interview reference line code - 3366
[74] Interview reference line code - 2441
[75] Interview reference line code - 1450
[76] Interview reference line code - 2392

approaches to determining activity and driving public/private financial information sharing, being dependent on individuals, inter-personal relationships and good will, was believed to be vulnerable to the ebb and flow of individuals' engagement.

There was believed to be a "huge amount of legal ambiguity"[77] in the expectations to share information to support AML/ATF outcomes.

Major barriers in public-private and private-private information-sharing were believed by REs to be well understood by industry and by relevant civil servants. However, policy reform processes to date were described as "incremental"[78] and "more of the same"[79], without recognising or addressing structural challenges in the regime.

REs raised concern that the underlying assumption of the system appears to be "if more can be reported to FINTRAC, the system will be more effective"[80], which was described as "unconvincing"[81] without recognition of broader challenges relevant to the effectiveness of the regime.

"If there was a real strategy for the next three years, involving financial institutions, around financial crime, then we could close tactical threats, and there could be real prevention."[82], proposed one RE.

(More comments on the strategic coordination of public-private 'project' initiatives are referenced in the section below: theme 7 in relation to strategic intelligence)

With regard to operational cross-government and public-private coordination…

One interviewee described cross-government and public-private operational-level coordination as relatively common and working well within their respective mandates.

Multiple REs noted that Canada appears to run a relatively large number of cross-government and public-private sector committees and working groups, however, these were not felt to contribute to a joined-up strategic national economic framework for prioritising threats and setting out a plan of action for a policy and operational response to those threats.

While there is some activity in process to improve the governance of project-initiatives, several REs raised that projects do not sit within a strategic national approach to tackling economic crime.

Interviewees noted the development of the ACE Fusion initiative and the CIFA initiative which was still in development but potentially offered a forum to improve cross-government and public/private dialogue on economic crime issues.

(More comments on the operational coordination of public-private 'project' initiatives are referenced in the section below: theme 7 in relation to strategic intelligence)

[77] Interview reference line code - 3102
[78] Interview reference line code - 1567
[79] Interview reference line code - 1592
[80] Interview reference line code - 1623
[81] Interview reference line code - 1623
[82] Interview reference line code - 1037

The Canadian context – additional analysis:

The Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada and the FATF evaluation of Canada's strategic approach to understanding and coordinating the national AML/ATF response…

In 2015, the Government of Canada, led by the Department of Finance, produced an Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada (the NIRA) to support the FATF Mutual Evaluation process. Canada achieved a 'substantial' rating in the 2016 4th round FATF Mutual Evaluation in relation to immediate outcome 1, referenced above.

The FATF Mutual Evaluation highlighted the following estimates of the economic crime threat facing Canada:

- An estimate by the Criminal Intelligence Service Canada (CISC) in 2007 that the proceeds of crime generated annually by predicate crimes committed in Canada represent approximately 3-5% of Canada's nominal gross domestic product (GDP), or approximately US$47 billion.
- RCMP estimated in 2011 that the amount of money laundered annually in Canada to be somewhere between US$5 billion and US$15 billion.
- And the Canadian National Inherent Risk Assessment placed profit-generating criminal activity as in the "billions of dollars".

The FATF Mutual Evaluation of Canada found that FINTRAC and OSFI objectives and activities are largely consistent with the ML and TF risks in Canada, as detailed in the NIRA.[83] FATF also highlighted that Canada's AML/ATF 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.

However, the Canadian government's National Inherent Risk Assessment (NIRA) has not been updated since it was prepared for the FATF evaluation.

Canadian cross-government engagement to understand and respond to money laundering threats…

As noted by interviewees, there are many evident strengths relating to the Canadian cross-government approach and budget funding for the fight against economic crime at the operational or working group level.

In addition to the NIRA, threat-based information can be drawn from FINTRAC's various publications (Alerts, Briefs, Guidance and indicators), Public Private Partnerships 'project initiatives' (see section A.6.), FINTRAC presentations at various events (e.g., conferences, workshops), the listing of terrorist entities by Public Safety Canada and other sanctions programs led by Global Affairs Canada. In addition, the Criminal Intelligence Service of Canada publishes an assessment of organised crime threats in Canada.

At a public-level, available to REs, FINTRAC publish a range of strategic intelligence products on their website[84], covering:

Operational briefs

- Risks and indicators for dealers in precious metals and stones
- Indicators of money laundering in financial transactions related to real estate

Operational alerts

- Laundering of proceeds from online child sexual exploitation
- Special Bulletin on COVID-19: Trends in Money Laundering and Fraud

[83] http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-Canada-2016.pdf
[84] https://www.fintrac-canafe.gc.ca/intel/sintel-eng

- Laundering the proceeds of crime through a casino-related underground banking scheme
- Laundering of the proceeds of romance fraud
- Professional money laundering through trade and money services businesses
- Laundering of the proceeds of fentanyl trafficking
- Democratic People's Republic of Korea's use of the international financial system for money laundering/terrorist financing
- Identification of higher risk currency exchange houses in Daesh-accessible territory in Iraq
- Indicators: The laundering of illicit proceeds from human trafficking for sexual exploitation

Assessments

- Terrorist Financing Assessment: 2018

At the strategic level, the Canadian legal framework for AML/ATF is subject to a 5-year review cycle, obliging all relevant stakeholders to engage in cross government policy exercises and respond to Parliamentary scrutiny.

A special joint meeting of federal, provincial and territorial Finance Ministers and Ministers responsible for AML and beneficial ownership was held on June 13, 2019 during which a high-level commitment to combat money laundering and terrorist financing were discussed and agreed.[85]

Financial crime topics have also repeatedly received attention for dedicated funding in recent Canadian budgets. In terms of the current situation in Canada, it appears that 'Money Laundering' as a topic does enjoy significant political/high-level policy engagement as a recipient of new funding.

In the 2019 budget, the following commitments were made by the government of Canada:

- CAD$16.9 million over five years, beginning in 2019–20, and CAD$1.9 million per year ongoing to support the operational capacity of FINTRAC, including with specific intent to expand public-private partnership projects to improve the overall efficiency.
- An additional CAD$2.4 million to FINTRAC over five years, beginning in 2019–20, and CAD$0.5 million per year ongoing to strengthen expertise and capacity.
- The addition of Revenu Québec and the Competition Bureau as disclosure recipients of FINTRAC financial intelligence;
- CAD$24 million to Public Safety Canada over five years to create the Anti-Money Laundering Action, Coordination and Enforcement (ACE) Team to actively coordinate and support inter-agency efforts to counter money laundering in Canada.
- CAD$28.6 million over five years and CAD$10 million ongoing have been allocated for the Canada Border Services Agency (CBSA) to create a Trade Fraud and Trade-Based Money Laundering Centre of Expertise.
- CAD$68.9 million to the RCMP over five years and CAD$20 million per year ongoing for enhanced federal policing capacity, including to fight money laundering.
- The Budget 2019 also raised legislative amendments to strengthen the legal basis to tackle professional money laundered.

Efforts to improve the strategic management of crimes, including the money laundering component, has clearly been a key area of interest for the Canadian government, with dedicated funding and centres of expertise established for Trade Fraud and Trade-Based Money Laundering and funding for FINTRAC to contribute to the National Strategy to Combat Human Trafficking.

[85] https://www.canada.ca/en/department-finance/news/2019/06/joint-statement--federal-provincial-and-territorial-governments-working-together-to-combat-money-laundering-and-terrorist-financing-in-canada.html

Outside of the Budget statements, FINTRAC clearly state their intention to engage in efforts to understand and address system-shortcomings. In the ‘2020–21 Departmental Plan’ FINTRAC commit to “ongoing collaboration with Canada's multi-agency AML/ATF Regime partners […] to identify and address deficiencies, gaps and vulnerabilities. The aim is to dynamically optimize the alignment of information provided by reporting entities with the evolving nature of money laundering and terrorist financing”.[86]

FINTRAC stated in its Departmental Results Report that, in 2019–20, FINTRAC Co-Chaired a new Public Private Collaboration Steering Committee (PPCSC). The main objective of the PPCSC is to improve anti-money laundering effectiveness within existing authorities and will build on existing Regime committees.[87]

FINTRAC also state their intention to “actively participating in the Commission of Inquiry into Money Laundering in British Columbia (“Cullen Commission”) to add value to its information collection and to leverage lessons learned as applicable.”[88]

The following box lays out commitments (pillars and priorities) from the (2019) FINTRAC ‘Strategic Plan 2019–24’[89] relevant to key challenges raised in interview in this FFIS study.

Commitments in the FINTRAC ‘Strategic Plan 2019–24’ relevant to challenges raised in this study:
In 2019, FINTRAC published its ‘Strategic Plan 2019–24’[90], which highlight a number of ambitions which very much reflect the key areas identified in this FFIS study, including:

Priority 2: Ensure transparency through results and performance

- Strengthen our performance measurement framework and regularly report on results
- Proactively engage with, and support various government oversight bodies

Priority 4: Explore and implement innovative solutions

- Leverage our knowledge and expertise to identify future trends and address possible challenges
- Investigate opportunities for private sector engagement and partnerships

Pillar 3: Collaborate to strengthen results, where the narrative lays out FINTRAC ambition for:

- “strategically reach[ing] out to businesses, law enforcement, international and domestic stakeholders and academia to ensure regime-wide value”; and
- “identifying and cultivating purposeful relationships, [that] maximize the value of our contribution and efforts. We will also constructively engage stakeholders to find better ways of doing business both externally, and cross-government.”

Priority 5: Cultivate strategic relationships with key external stakeholders

- Regularly identify, review, and prioritize FINTRAC's relationships with key business and international stakeholders to ensure their alignment with the Centre's compliance, intelligence, and corporate priorities […].
- Play a leadership role in international fora to support the government's broader international efforts to combat money laundering and terrorist activity financing
- Work with external stakeholders to discover new ways of doing business
- Enhance transparency and demonstrate progress with external stakeholders

Priority 6: Strengthen cross-government cooperation

[86] https://www.fintrac-canafe.gc.ca/publications/dp/2020-2021/dp-eng
[87] https://www.fintrac-canafe.gc.ca/publications/drr-rrm/2019-2020/drr-rrm-eng
[88] https://www.fintrac-canafe.gc.ca/publications/dp/2020-2021/dp-eng
[89] https://www.fintrac-canafe.gc.ca/fintrac-canafe/1-eng
[90] https://www.fintrac-canafe.gc.ca/fintrac-canafe/1-eng

- Proactively work with other Canadian government departments/agencies to increase our influence on government policy-making and decision-making on matters related to money laundering and terrorist activity financing
- Work with central agencies in creating more efficient and effective interactions

More broadly, Canada has range of federal level initiatives designed to support coordination and effective action in relation to crime, including:

The National Coordinating Committee on Organized Crime[91]

> *"The National Coordinating Committee (NCC) and its five Regional/Provincial Coordinating Committees (RCCs) work at different levels to a common purpose: Create a link between law enforcement agencies and public policy makers to combat organized crime. The NCC is the primary forum that reviews progress of the National Agenda to Combat Organized Crime."*
>
> *"The NCC is responsible for the identification of national public policy issues, developing national strategies and initiatives to combat organized crime and advising the federal, provincial and territorial Deputy Ministers Steering Committee on Organized Crime on the nature, scope and impact of organized crime. It provides a national forum where the interests and concerns of Canada's law enforcement community can be brought to the attention of people who deal with law, policy and the administration of justice."*

However, there are no recent papers or published material that relate the work of the NCC to money laundering; the closest recent paper being "Patterns in Cannabis Cryptomarkets in Canada in 2018"[92].

The main available strategic guidance document for tackling organised crime in Canada and money laundering and economic crime appears to be the "National Agenda to Combat Organized Crime"[93] which was published in 2006.

The 'National Agenda' paper does provide a strong basis for Federal, Provincial and Territorial (FPT) Government coordination.

The National Agenda identifies four main pillars to be addressed:

- national and regional coordination;
- legislative and regulatory tools;
- research and analysis; and,
- communications and public education.

These pillars assist in meeting the ultimate objectives of:

- preventing and reducing organized crime; and
- preventing and reducing the harms caused by organized crime

Financial Transactions and Reports Analysis Center of Canada (FINTRAC) are members of the NCC, as part of a membership of enforcement and intelligence agencies. The NCC is intended to "facilitate national cooperation

[91] https://www.publicsafety.gc.ca/cnt/cntrng-crm/rgnzd-crm/ntnl-crdntng-cmmtt-en.aspx?wbdisable=true
[92] https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2019-r004/index-en.aspx
[93] https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cmbtng-rgnzd-crm/index-en.aspx

as closer links are established with local agencies and other FPT bodies that are involved in addressing the complexities of organized crime."

An NCC working group on Money Laundering, which is chaired by FINTRAC, is reported as "currently developing ways to improve tracking and feedback on financial intelligence case disclosures made by FINTRAC". However, it is not clear how this group has progressed. The main page has an official 'latest update' of January 2018, but the most recent reference appears to be referring to activity 2008.[94]

In addition to the single reference to the Money Laundering NCC working group, there is a much more prominent set of references to the Integrated Proceeds of Crime Committee (IPOCC). IPOCC was established as an inter-departmental initiative, to "contribute to the disruption, dismantling and incapacitation of targeted organized criminals and crime groups. PSEPC provides policy coordination and regular evaluation of the initiative"[95]

However, this Committee appears to be focused on cash and physical assets, and does not appear to include membership of FINTRAC from available online reference material.

In general, however, the available information on the Canadian strategic approach to addressing organised crime, through Public Safety's online material, appears at least a decade out of date.

The contribution of the AML/ATF regime and particularly private sector REs to disruption, intelligence and prevention goals against organised crime appears to only have a periphery significance in the available strategic documents published by Public Safety. This is despite over CAD$5bn of regulatory mandated spending being expended to identify money laundering.

More recently, the development of the ACE Fusion Team, in particular, appears to have a promising role to respond to current challenges within the Canadian regime with regard to cross-government coordination and, some extent of, strategic direction for the approach to tackle economic crime.

Public Safety also describe a number of recent initiatives to support action on ML threats in dialogue between the federal and provincial levels of government.

Public Safety describe the collaboration at a provincial level including:[96]

> *"with British Columbia, in particular, to address money laundering in the province, including the creation of an ad-hoc working group whose mandate is to enhance communication, information sharing, and alignment amongst relevant operational and policy partners to explore and better address issues and risks related to fraud, money laundering, and tax evasion through real estate in B.C.*
>
> *On January 22, 2020, federal, provincial and territorial (FPT) ministers responsible for justice and public safety concluded a one-day meeting to discuss key priorities of Canadians, which included discussion of money laundering and Ministers reiterated their support for a coordinated approach to better address this problem."*

[94] https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cmbtng-rgnzd-crm/index-en.aspx

[95] https://www.publicsafety.gc.ca/cnt/cntrng-crm/rgnzd-crm/ntgrtd-prcds-crm-en.aspx#:~:text=Integrated%20Proceeds%20of%20Crime%20(IPOC,regular%20evaluation%20of%20the%20initiative.

[96] https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20200621/041/index-en.aspx

Limitations in current cross-government and public-private engagement in coordinating a response to money laundering threats…

The AML/ATF regime involves a broad eco-system of stakeholders, including the FIU (both from an intelligence perspective and as a supervisor), reporting entities in the private sector, law enforcement and other users of financial intelligence, and the range of stakeholders who may have a contribution to make on what crime 'prevention' can be achieved through action by REs.

In terms of the private sector, the Government of Canada uses forums for public/private coordination, such as the Advisory Committee on Money Laundering and Terrorist Financing (ACMLTF)[97] to provide a high-level discussion forum to address emerging issues and provide general advice for Canada's overall anti-money laundering and anti-terrorist financing (AML/ATF) policy.

While the Canadian government has a range of forums to support coordination for efforts to address crime which, in many cases, make reference to the importance of money laundering, there appears to be significant shortcomings with regard to:

- The information made available to REs to understand national threats;
- The existence of a national strategy to address economic crime threats, including through policy and operational actions, covering cross-government agencies and departments and the private sector role; and
- How various Canadian crime disruption and prevention efforts are intended to link with and make full use of the intelligence and disruption opportunities available through the AML/ATF regime.

The only threat assessment made publicly available on the FINTRAC website is the '2018 Terrorist Financing Assessment', which is more focused on a description of hotspots around the world rather than the threat facing Canada and the scale and characteristics of those threats within Canada. FINTRAC produces a range of operational briefs and alerts, which do – in some cases – provide some limited information on the threats themselves, but are generally focused on providing transactional and behavioural indicators to REs.

The author understands that FINTRAC produce a large amount of threat-assessment information which is not available publicly and likely supports a national understanding of threats, available only to government stakeholders. However, from an exhaustive review of material produced by the Canadian government, there is limited evidence that an up-to-date assessment of economic crime threats, based on reporting through the AML/ATF regime, is being integrated into other Canadian strategic approaches to address economic crime.

FINTRAC state in their Departmental Results Report 2019-20 that, through the National Inherent Risk Assessment Working Group, FINTRAC provided support to the Department of Finance Canada in determining which business sectors or industries may need to be assessed for money laundering and terrorism financing risk, and then conducting an assessment of those risks.[98] It appears that FINTRAC have focused on sectoral risk assessments rather that threat assessments of economic crime as a whole facing Canada.

The extent to which the AML/ATF system is integrated into Canadian strategic thinking about crime disruption is far from clear, and most of the publicly material reference available about the extent of cross-government coordination on economic crime issues is out of date.

The extent of a Canadian economic crime strategy in 2020…

Currently, Canada lacks any public documents which identify and set out the planned response to economic crime threats facing the country.

[97] https://www.canada.ca/en/department-finance/programs/committees/advisory-committee-money-laundering-terrorist-financing.html
[98] https://www.fintrac-canafe.gc.ca/publications/drr-rrm/2019-2020/drr-rrm-eng

Even in 2016, FATF recognised that Canada does not have formal 'stand-alone' AML strategy. FATF drew attention to Finance Canada's Annual Report on Plans and Priorities, which supposedly describes the AML/ATF regime's spending plans, priorities and expected results. However, the Departmental Reports for Finance Canada over recent years include only a very high-level reference to commitments relevant to anti-money laundering, with no clear intent as far as expected measurable results relevant to specific threats.[99]

The clearest and most comprehensive articulation of current needs in terms of economic crime policy reform in Canada is the statutory review of PCMLTFA (published in 2018). The review Chapter 2, entitled 'The exchange of information and privacy rights of Canadians', publishes a range of recommendations relevant to the sharing and retention within government; sharing and retention between the government and the private sector; sharing and retention within the private sector; and de-risking.

In the 2019 Federal Budget, the Government of Canada refers to the statutory review, entitled 'Confronting Money Laundering and Terrorist Financing: Moving Canada Forward' as the "roadmap to respond to current and future threats".[100] This indicates that the Government of Canada views this document as the strategic basis for policy reform. However, it should be noted that the review is published by Parliament with recommendations to government, not an articulation of government policy reform or operational strategy. In addition, a majority of the Chapter 2 recommendations relevant to information-sharing have not been taken forward (however, of course this may be due to COVID-19 related disruption.)

If the Government of Canada were to take forward the suite of recommendations outlined in Chapter 2 of the statutory review of 2018, then it would respond to many of the issues highlighted in this FFIS study.

Viewed from this angle, the points outlined in this FFIS study serve to highlight that many challenges remain in the Canadian AML/ATF system, a large proportion of which have been previously identified and are well documented through the statutory review process.

Statutory review of PCMLTFA (2018) recommendations relevant to challenges raised in this FFIS study

Of particular relevance to this FFIS study, the 'Confronting Money Laundering and Terrorist Financing: Moving Canada Forward' statutory review of PCMLTFA (published in 2018)[101] made the following recommendations (truncated):

Recommendation 15 -
That the Government of Canada expands FINTRAC's mandate to allow for:
• an operational model to allow for two-way information sharing system (rather than strictly being an information gathering system);
o FINTRAC should be able to share feedback, best practices and long-term trends, so that reporting entities can properly assist FINTRAC.
• the ability to request more information from specific reporting agencies to clarify reported suspicious activity or to build a stronger case before referring it to law enforcement;

Recommendation 16 -
That the Government of Canada establish a round table partnership with industry leaders who are investing significantly in technology that more efficiently tracks suspicious activities and transactions, so as to promote best industry practices.

Recommendation 17 -
That the Government of Canada take steps to emulate the U.K.'s model of a Joint Money Laundering Intelligence Taskforce in Canada.

Recommendation 18 –

[99] https://www.canada.ca/en/department-finance/corporate/transparency/plans-performance/departmental-plans/2019-2020/report.html
[100] https://www.budget.gc.ca/2019/docs/plan/budget-2019-en.pdf
[101] https://www.ourcommons.ca/Content/Committee/421/FINA/Reports/RP10170742/finarp24/finarp24-e.pdf

That the government of Canada consider tabling legislation that would allow information that is limited to AML/ATF subject matter to be shared between federally regulated financial institutions such as banks and trust companies, provided that FINTRAC is notified upon each occurrence of such sharing.

The need for political and executive engagement in an economic crime strategy…

The statutory review provides a very strong policy basis to address key challenges to the effectiveness of the AML/ATF regime in Canada.

In addition, the special joint meeting of federal, provincial and territorial Finance Ministers and Ministers responsible for AML and beneficial ownership, held on 13 June 2019, produced a high-level commitment to combat money laundering and terrorist financing.[102] However, the statement falls short of recognising the specific shortcomings in the current Canadian AML/ATF regime or making specific policy commitments to address those challenges.

FINTRAC have set out very clearly in their 2019-24 Strategy an intent to support cross-government and public-private collaboration and innovation. However, there is a limit to what FINTRAC can do to address strategic challenges in isolation, outside of wider cross-government and, ultimately, political consideration of what Canada wants to achieve from its AML/ATF regime. Indeed, the potential in Canada to realise a cross-government and public-private collaborative approach to detecting and disrupting economic crime appears to be hamstrung by the legal emphasis on FINTRAC's role as an independent and ‘arm's length’ agency, inhibited in law from both public-private and FIU-to-law enforcement dynamic information-sharing, which was written into the original Canadian AML legislation.

Though more data and research are required (as highlighted in theme 1), in this study, drawing together the various themes identified through the course of the research, the available information we have collected indicates that the Canadian AML/ATF regime…

1. is **not producing substantial operational results**, compared to the scale of economic crime threats, nor designed with a target operating model that could reasonably be expected do so;
2. encourages **massive and continual risk-displacement** in the name of ‘preventative measures’, without a convincing disruptive effect on underlying crime, nor as part of a credible approach to preventing criminal activity;
3. collectively **costs public and private stakeholders many billions** of Canadian dollars to implement annually; and
4. in - terms of privacy – is currently driving **one of the most extensive AML/ATF data collection regimes in the world**, encouraging massive volumes of reporting of Canadian transactions to FINTRAC.

A justification or conceptualisation of the Canadian AML/ATF system sees FINTRAC, as an FIU, as a quasi-guardian of privacy and a gatekeeper for information flow between private and public sectors. For those that support this gatekeeper model, there appears to be a need to explain how it can be made more sustainable, given the current results, costs and ever-increasing data collection footprint associated to the model.

This author notes that, in evidence to the statutory review of PCMLTFA (published in 2018), the Privacy Commissioner of Canada contends that there is “a lack of proportionality in the regime, as disclosures to law enforcement and other investigative agencies made in a given fiscal year represent a very small number when compared with the information received during that same time frame.”[103]

[102] https://www.canada.ca/en/department-finance/news/2019/06/joint-statement--federal-provincial-and-territorial-governments-working-together-to-combat-money-laundering-and-terrorist-financing-in-canada.html
[103] https://www.ourcommons.ca/Content/Committee/421/FINA/Reports/RP10170742/finarp24/finarp24-e.pdf

Many countries, particularly in Europe, achieve a very high standard of protection for privacy rights, while also enabling a more effective AML/ATF public-private and cross-government information-sharing regime. Indeed, given the design features of the Canadian regime, it appears highly plausible that policy reform in Canada could achieve substantial gains across:

- **effectiveness,** in terms of more substantial enforcement, disruption and preventative results;
- **efficiency** in terms of public and private sector resources applied to achieve those results; and
- with **privacy-gains** in terms of a smaller and more targeted overall data collection footprint in Canadian society.

Alternatively, Canada may wish to go 'full swing' behind the conception of FINTRAC as a privacy guardian of data, but go further in terms of data collection to improve the effectiveness, efficiency, timeliness and relevance of the regime by providing FINTRAC with real-time access to all transactions. This approach may follow in the ambitions of the Australian AUSTRAC privacy preserving analytics model currently under development.[104]

Despite the statutory review recommendations, Canada does not benefit from clarity about the future target operating model for how the AML/ATF regime can effectively respond to economic crime threats in Canada, including the role of public and private sectors in balance with the privacy considerations. At the current time, it is unclear whether the various budget commitments in 2019 to agencies will be enough to address the lack of a strategic joined-up approach to both understanding and responding to the economic crime threats in Canada.

Summary of key challenges in Canada:

Publicly available economic crime threat assessments in Canada are scarce and the National Inherent Risk Assessment is almost 5 years out of date.

The current Canadian AML/ATF regime appears unable to demonstrate an effective impact relative to the likely scale of economic crime in Canada, it is very costly to implement and it results in a very high data collection footprint on Canadian society.

Beyond the 2018 statutory review recommendations, the Government of Canada has no published economic crime strategy for policy reform or to set out an end-to-end view of the target operating model for how the range of relevant public agencies and private sector REs should operate and share information in the AML/ATF regime to be more effective.

Such a strategy would ideally benefit from a clear understanding of the effectiveness and efficiency challenges in the Canadian AML/ATF regime, and set out the coordinated and evidenced-based use of policy-reform and operational developments to support intelligence, disruption, prevention and education activities to address the identified national economic crime threats.

Recognising recent developments in Canada:

- The key development to improve the Canadian strategic framework for addressing economic crime appears to be the establishment - and significant multi-year funding in the 2019 Budget - of the ACE Team.[105]
- While still in the 'design phase', the ACE Fusion Team is shaping up to provide operationally-informed contributions to AML/ATF policy making, to help provide a framework for national

[104] See Theme 4 – International Comparisons for more details of the Australian AUSTRAC Alerting Project

[105] https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20200621/041/index-en.aspx

economic crime priorities and to strengthen federal-regional coordination and access to operational support.

- FFIS understand that the ACE Fusion Team's mandate will be to 'look at the AML system as a whole, inclusive of both federal and non-federal partners.' At the policy level, the ACE Fusion Team aims to support or lead on policy, legislative or strategic issues/initiatives to strengthen the effectiveness of ML enforcement efforts.
- However, it is possible that the ACE Fusion Team will be relatively more focused on public-to-public collaboration, rather than public/private information sharing. Also, it is not clear that the ACE Fusion Team has a sufficient mandate to help drive political level engagement in legal reforms in Canada, which may include for example ensuring that the newly proposed privacy law 'Bill C-11'[106] takes account of AML/ATF information-sharing requirements through exemptions.

International comparisons:

In terms of efforts to leverage information sharing to achieve more effective outcomes, a number of jurisdictions are engaged in significant strategic reforms to support legislative changes.

The "EU AML Action Plan 2020" [107] – On 7 May 2020, the European Commission published an action plan for a comprehensive Union policy to prevent money laundering and terrorism financing. The plan built on a number of papers in 2019 that highlighted fragmentation of AML regulations, uneven supervision, limitations in the cooperation among financial intelligence units and inadequate information-sharing across the EU.

The "UK Economic Crime Plan 2019-2022"[108] - The wide ranging and cross-government plan builds from the UK's 7 priority areas for reform which were published in January 2019, covering the need to:

1) develop a better understanding of the threat posed by economic crime and our performance in combatting economic crime;
2) pursue better sharing and usage of information to combat economic crime within and between the public and private sectors across all participants;
3) ensure the powers, procedures and tools of law enforcement, the justice system and the private sector are as effective as possible;
4) strengthen the capabilities of law enforcement, the justice system and private sector to detect, deter and disrupt economic crime;
5) build greater resilience to economic crime by enhancing the management of economic crime risk in the private sector and the risk-based approach to supervision;
6) improve our systems for transparency of ownership of legal entities and legal arrangements; and
7) deliver an ambitious international strategy to enhance security, prosperity and the UK's global influence.

In terms of threat assessments, the UK Economic Crime Plan [109] commits to improving UK "understanding the threat and performance metrics" as 'Strategic Priority One'. The Plan highlights "A better understanding of the threat plays a key role in enabling the public and private sectors to collectively prioritise the policy reforms and operational activity that deliver the highest impact in combatting economic crime… [and to] measure the impact of our collective actions to tackle economic crime."[110]

The UK also committed to adopting a strategic approach to address gaps in the UK evidence base for different types of economic crimes and limitations in the data and statistics collected though the National Risk

[106] https://www.dataprotectionreport.com/2020/11/bill-c-11-canada-proposes-new-data-privacy-legislation/
[107] https://ec.europa.eu/info/publications/200507-anti-money-laundering-terrorism-financing-action-plan_en
[108] https://www.gov.uk/government/publications/economic-crime-plan-2019-to-2022
[109] https://www.gov.uk/government/publications/economic-crime-plan-2019-to-2022/economic-crime-plan-2019-to-2022-accessible-version#strategic-priority-one-understanding-the-threat-and-performance-metrics
[110] https://www.gov.uk/government/publications/economic-crime-plan-2019-to-2022/economic-crime-plan-2019-to-2022-accessible-version#strategic-priority-one-understanding-the-threat-and-performance-metrics

Assessment process, supported by a National Assessments Centre which conducted the first formal public-private economic crime threat assessment in 2019.[111]

In 2020, the U.S. Treasury announced its 'National Illicit Finance Strategy' to both identify key threats and establish "a roadmap to modernize the U.S. counter-illicit finance regime".[112] The Strategy provided the framework for a whole-of-government multi-agency approach and laid out policy and regulatory reforms covering three strategic priorities:

1. Increasing transparency and closing gaps in the U.S. AML/ATF legal framework;
2. Improving the efficiency and effectiveness of the U.S. AML/ATF regulatory and supervisory framework for financial institutions; and
3. Enhancing current AML/ATF operational capabilities.

In 2019, the Dutch Ministers of Finance and Justice and Security submitted a "joint action plan for the prevention of money laundering through the Dutch financial system and for tracking and prosecuting criminals and their enablers" to the Dutch parliament.[113] The 2019 Dutch 'Joint Action Plan', with a suite of over 40[114] specific actions, committed to the regular execution of National Risk Assessments to support policy making and called for cross-government collaboration to be reinforced through the national 'Financial Expertise Centre' to understand threats and share trends across the range of relevant agencies.[115]

The plan set out a strategic intent to support various forms of sharing information, including increasing the effectiveness of joint transaction monitoring by banks by means of a "TM utility". The plan specifically highlights that the value of a transaction monitoring approach will be more effectively realised when participants are able to analyse flows across multiple institutions, rather than to view transaction data only in silos of individual financial institutions. The strategy also supports the development of public-public information sharing by increasing the scope for AML regulators to share information with bodies within the Financial Expertise Centre (FEC) (a partnership between authorities charged with combatting, detecting, and prosecuting money laundering). The plan sees a commitment for funding to support the new framework with EUR 29 million from 2021 onwards.[116]

The broad set of measures proposed in the plan are grouped into three main categories, aimed at

(i) increasing the barriers against criminals channelling illegally obtained income into the financial system;
(ii) increasing the effectiveness of the "gatekeeper" function and how it is supervised, thus excluding the proceeds of crime from the financial system; and
(iii) reinforcing investigation and prosecution, so that criminals can be dealt with even more quickly and effectively.

Importantly, the Dutch Joint Action Plan was accompanied with the publication of additional government research paper reviewing the Dutch legal regime as a whole in the context of the Action Plan, including the assessments of the adequacy of the current Dutch AML/ATF legislation, data protection law (GDPR), competition law and regulation. The study highlights what is currently permissible within the law, what reforms would be required to achieve the ambition of the Action plan, and also highlights the design conditions required to be compliant with data protection and competition law.[117]

These national reform initiatives have, in part, been driven by repeated money laundering failings or scandals; increasing awareness of the scale of the challenges in terms of effectively tackling financial crime; the limited evidence to indicate historic approaches are supporting a meaningful disruptive or deterrent effect against financial crime; and the growing cost of compliance with the system over the previous decade.[118]

[111] https://www.nationalcrimeagency.gov.uk/who-we-are/publications/323-public-private-threat-update-2019-economic-crime/file
[112] https://home.treasury.gov/system/files/136/National-Strategy-to-Counter-Illicit-Financev2.pdf
[113] https://www.rijksoverheid.nl/documenten/kamerstukken/2019/06/30/aanbiedingsbrief-plan-van-aanpak-witwassen
[114] https://www.rijksoverheid.nl/documenten/kamerstukken/2019/06/30/aanbiedingsbrief-plan-van-aanpak-witwassen
[115] https://www.rijksoverheid.nl/documenten/kamerstukken/2019/07/01/onderzoek-informatie-uitwisseling
[116] https://www.nautadutilh.com/en/information-centre/news/new-plan-to-combat-money-laundering
[117] https://www.rijksoverheid.nl/documenten/kamerstukken/2019/07/01/onderzoek-informatie-uitwisseling
[118] https://www.politico.eu/article/the-world-dirty-money-by-the-numbers/

Opportunities to enhance the Canadian framework:

- Economic crime threats in Canada can be assessed at a higher frequency, potentially annually, and contribute to a robust and more regular National Threat Assessment and broader National Risk Assessment (NRA) process.
- Canada can develop a clear strategy for economic crime policy and operational reform, which is founded in current economic crime threat assessments, incorporates the latest learning from the effectiveness of public-private partnership efforts and sets out a vision for the desired operating model for both public-private and private-private financial information sharing in Canada.
- The economic crime strategy can set out clear targets which are commensurate with the assessed economic crime threats and present a credible as a response to those threats.

Theme 3. Prioritisation of economic crime threats

Background:

In some senses, financial institutions are collection assets for a national financial intelligence agency. In more traditional intelligence processes, the collection of intelligence is directed by a set of regularly updated collection priorities, which themselves are based on the needs of end-users of that intelligence.

In financial intelligence, the submission of suspicious reporting is typically not subject to 'prioritisation' outside of each regulated entity's unilateral determination of priorities through the 'risk-based approach'. As such, resources and expertise are not focused in response to the needs of end-users and there can be expected to be a large degree of inefficiency in the servicing of the needs of end-users and fulfilling the objectives of the intelligence system.

Effectiveness challenges raised in interview:

Multiple REs believe that the Canadian Government does not publish clearly defined national economic crime threat priorities.

In terms of sources of information about Canadian economic crime priorities, interviewees mentioned:

- Through FINTRAC alerts and other documentation and press releases;
- Through general media coverage about law enforcement action;
- Through direct participation in Canadian cross-government consultative forums, working groups and thematic operational groups;
- Through RCMP communications, speeches, informal dialogue and through RCMP comments in PPP project initiatives;
- By word of mouth with other public officials;
- Through industry associations and relevant events.
- Through the National Inherent Risk Assessment; and
- Through, or by inference from, the existence of PPP project initiatives.

REs reported a lack of clarity in industry as to who is setting priorities for the national AML/ATF regime in Canada.

REs noted some overlap, but mostly believed that there was a lack of alignment between priorities set in the National Inherent Risk Assessment, Canadian PPP project initiates, stated and informally-communicated law enforcement priorities, FINTRAC alerts and other threats that are in some way communicated to industry.

From the perspective of the PPP project initiatives, REs involved in project initiatives raised uncertainty as to how the project 'priorities' or choices to start a project are made, with an RE stating that this can be heavily influenced by "the enthusiasm of individuals"[119] rather than a national prioritisation and governance process.

In terms of law enforcement priorities, some interviewees believed that RCMP provided annual updates on threats and updates on priorities to specific threat-based working groups, whereas others believed that law enforcement priorities were communicated through informal channels and "who you know".[120]

[119] Interview reference line code - 1913

[120] Interview reference line code - 2262

There was a suggestion that the new CIFA group may be in a position to communicate more clearly about law enforcement priorities, and the balance between federal and regional priorities.

Interviewees offered mixed views as to whether intelligence priorities have any bearing on supervisory/examination interests. An RE, with recent experience, indicated that supervisory interests were procedural and administrative and not engaged in attempting to understand how an RE had contributed to activity that supports intelligence value or project priorities. However, another interviewee did recognise FINTRAC supervisory interest in engagement in project initiatives.

As a result of lack of priorities and a perceived "zero-tolerance, zero-failure"[121] approach to supervision, REs are forced to "shoot everywhere"[122] and reportedly apply the same attention to an STR related to CAD$20 vs CAD$20m.

An RE highlighted "there is a real hunger to work on priorities and action related to something that has impact for Canada, but we don't get clear priorities"[123].

One interviewee stated that "It is not clear that RCMP and FINTRAC have the same priorities."[124].

An RE expressed a view that FINTRAC appear to have an institutional preference to increase volumes of reports, such that they can have a larger network picture in their data-base, and do not wish to communicate priorities to REs, "we will get punished for missing something, so it is very hard to prioritise anything."[125]

A number of interviewees noted that they were aware of much more effective and strategic cross-government collaboration and communication to the private sector on cyber security threats.

[121] Interview reference line code - 1100
[122] Interview reference line code - 2853
[123] Interview reference line code - 2061
[124] Interview reference line code - 1615
[125] Interview reference line code - 4394

The Canadian context – additional analysis:

As stated in the previous section, Canada has no stand-alone economic crime or money laundering strategy.

Within the FATF approach to effectiveness, a country should be guided by a National Risk Assessment of ML and TF threats.

Beyond a general emphasis on professional money laundering of transnational and domestic organised crime, the Canadian NIRA in 2015 highlighted the following ML threats:[126]

Very High Threat Rating

- Capital Markets Fraud
- Mass Marketing Fraud
- Commercial (Trade) Fraud
- Mortgage Fraud
- Corruption and Bribery
- Third-Party Money Laundering
- Counterfeiting and Piracy
- Tobacco Smuggling and Trafficking
- Illicit Drug Trafficking

High Threat Rating

- Currency Counterfeiting
- Illegal Gambling
- Human Smuggling
- Payment Card Fraud
- Human Trafficking
- Pollution Crime
- Identity Theft and Fraud
- Robbery and **Theft**

Medium Threat Rating

- Firearms Smuggling and Trafficking
- Loan Sharking
- Extortion
- Tax Evasion/Tax Fraud

Low Threat Rating

- Wildlife Crime

However, since the NIRA, which is almost five years old, there appears to be no other definitive guidance on priority Canadian economic crime (ML) threats.

In terms of reporting actually being submitted by REs, the top three predicate offences related to FINTRAC's financial intelligence disclosures in 2019–20 were drugs (31%), fraud (30%), and tax evasion (14%).[127]

[126] Public version of the NRA, Department of Finance Canada (2015), Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada, p.22, https://www.canada.ca/en/department-finance/services/publications/assessment-inherent-risks-money-laundering-terrorist-financing.html#_Toc424288854

[127] https://www.fintrac-canafe.gc.ca/publications/ar/2020/1-eng?wbdisable=true

Without a cross-government approach to threat prioritisation, REs must take ‘prioritisation signals’ from a range of sources. In addition to the sources mentioned by interviewees above, it may also possible to infer national economic crime priorities from the following:

- As shared during the inter-departmental and Parliamentary review process during AML/ATF legislative cycles;
- As defined by the National Inherent Risk Assessment Working Group[128]
- As defined by the private sector collaboration with public agencies through project initiatives;
- As observable from law enforcement operational priorities and investigations; and
- As implicit in political priorities or ML scandals that reach public and political attention.

The extent of alignment between the above sources of ‘prioritisation signals’ appears limited.

In any case, beyond extra resources applied to project initiatives, it is unclear to what extent various Canadian prioritisation priorities impact on regulated entities in terms of guiding their allocation of resources, due to the lack of follow-through to any stated financial crime threat priorities and the relevance of those priorities from a supervisory examination perspective.

FINTRAC has taken steps to enhance the transparency of its supervisory inspection process, through the ‘Assessment Manual: The approach and methods used during examination’ updated in November 2020.[129]

A fundamental principle in the FINTRACs approach to supervision is to encourage regulated entities to take a “risk-based approach” to understand how a firm “may be more at risk of being used for money laundering or terrorist activity financing, and on areas where there is a greater risk of not meeting legal requirements (risk of non-compliance).”[130]

The guidance does state that:

> “When determining the risks your business may be exposed to, we rely on our experience, knowledge, training, and professional judgment. **We take into account relevant information from FINTRAC publications and guidance.** We may also take into consideration relevant information taken from publicly available reports and publications issued by well-known credible sources on money laundering and terrorist activity financing.”
>
> Further, that:
>
> *“FINTRAC guidance presents money laundering and terrorist activity financing indicators to help businesses better understand typical risks they may be exposed to, and should watch for, in their day-to-day activities. When we assess the requirement to report suspicious transactions using the methods described in the manual, we may refer to the indicators we provide in the guidance, in addition to the obligation in the PCMLTFA, to support the rationale for suspicion.”*

So, it is clear from FINTRAC’s perspective that FINTRAC guidance and various project related indicator ‘Operational Alerts’ or ‘Briefs’ should contribute to an REs assessment of risk.

[128] Referred to in the FINTRAC Annual Report, but there is limited public information about the priorities being assessed within the Working Group https://www.fintrac-canafe.gc.ca/publications/ar/2019/1-eng#s1

[129] https://www.fintrac-canafe.gc.ca/guidance-directives/exam-examen/cam/cams-eng

[130] https://www.fintrac-canafe.gc.ca/guidance-directives/exam-examen/cam/cam-eng.pdf

At the time of this research[131], these alerts and guidance cover:

- Terrorist Financing
- Risks and indicators for dealers in precious metals and stones
- Money laundering in financial transactions related to real estate
- Laundering of proceeds from online child sexual exploitation
- COVID-19 related Money Laundering and Fraud
- Laundering the proceeds of crime through a casino-related underground banking scheme
- Romance fraud
- ML through trade and money services businesses
- Laundering of the proceeds of fentanyl trafficking
- Democratic People's Republic of Korea's use of the international financial system for money laundering/terrorist financing
- Higher risk currency exchange houses in Daesh-accessible territory in Iraq
- The laundering of illicit proceeds from human trafficking for sexual exploitation

It should be noted that the Canadian NIRA doesn't actually appear on the FINTRAC website[132], nor is there reference to any priorities associated to the National Coordinating Committee on Organized Crime, nor the IPOCC or Money Laundering sub-groups of that committee on the FINTRAC website.

The table below highlights divergence between threat-specific guidance on FINTRAC's website (which have particular importance in FINTRAC's examination process for REs) and the most recent Canadian NIRA.

Table 9. Extent of alignment in economic crime threat prioritisation signals (NIRA to FINTRAC Strategic Intelligence[133])

Priority threats in the Canadian NIRA (ML assessment)	Threats covered in FINTRAC publications (operational alerts and briefs)
Professional money laundering of transnational and domestic organized crime	General alignment
Very High Threat Rating	
Capital Markets Fraud	No clear and specific alignment
Mass Marketing Fraud	No clear and specific alignment
Commercial (Trade) Fraud	Partial alignment through FINTRAC publication 'ML through trade and money services businesses'
Mortgage Fraud	No clear and specific alignment
Corruption and Bribery	No clear and specific alignment
Third-Party Money Laundering	General alignment
Counterfeiting and Piracy	No clear and specific alignment
Tobacco Smuggling and Trafficking	No clear and specific alignment
Illicit Drug Trafficking	Alignment through FINTRAC publication on "fentanyl trafficking", though limited for other narcotics crimes.
High Threat Rating	
Currency Counterfeiting	No clear and specific alignment
Illegal Gambling	Strong alignment through FINTRAC publication: 'Laundering the proceeds of crime through a casino-related underground banking scheme'

[131] FINTRAC website review on 8 December 2020

[132] At time or research

[133] Beyond strategic intelligence, FINTRAC also produce guidance, at a sectoral level, which is intended to cover basic ML indicators which may be used to facilitated a large array of underlying crime types at a high-level. https://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/1-eng

Human Smuggling	No clear and specific alignment (beyond human trafficking)
Payment Card Fraud	No clear and specific alignment
Human Trafficking	Strong alignment
Pollution Crime	No clear and specific alignment
Identity Theft and Fraud	Partial alignment through FINTRAC publication on Romance fraud.
Robbery and Theft	No clear and specific alignment
Medium Threat Rating	
Firearms Smuggling and Trafficking	No clear and specific alignment
Loan Sharking	No clear and specific alignment
Extortion	No clear and specific alignment
Tax Evasion/Tax Fraud	No clear and specific alignment
Low Threat Rating	
Wildlife Crime	A small reference in the 2019-20 FINTRAC Annual Report as a topic of increasing international importance, which FINTRAC has contributed to.

Table 10. Extent of alignment in economic crime threat prioritisation signals (FINTRAC Strategic Intelligence[134] to NIRA alignment)

Priority threats in the Canadian NIRA (ML assessment)	**Threats covered in FINTRAC publications (operational alerts and briefs)**
Alignment as a sectoral risk, though not a national threat topic	Risks and indicators for dealers in precious metals and stones
Alignment as a sectoral risk, though not a national threat topic	Money laundering in financial transactions related to real estate
No clear and specific alignment	Laundering of proceeds from online child sexual exploitation
N/A	COVID-19 related Money Laundering and Fraud
Strong alignment	Laundering the proceeds of crime through a casino-related underground banking scheme
Partial alignment	Romance fraud
Partial alignment	ML through trade and money services businesses
Strong alignment	Laundering of the proceeds of fentanyl trafficking
N/A but strong alignment with TF risk assessment	higher risk currency exchange houses in Daesh-accessible territory in Iraq
Strong alignment	The laundering of illicit proceeds from human trafficking for sexual exploitation
N/A	Terrorist Financing Risk Assessment 2018

In general, national economic crime and financial intelligence threat priorities are poorly defined in Canada.

[134] Beyond strategic intelligence, FINTRAC also produce guidance, at a sectoral basis, which is intended to cover basic ML indicators which may be used to facilitated all a large array of underlying crime types at a high-level. https://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/1-eng

While FINTRAC does refer to the importance of an RE considering FINTRAC publications in an RE's assessment of risk, Canada has yet to attempt to steer RE resources-allocation towards national economic crime threat priorities, outside of project PPP initiatives and associated FINTRAC alerts.

The Canadian AML/ATF regime operates without a sense of national prioritisation, and relies on REs to identify priorities independently and largely in isolation of a broader picture of national priorities.

Part of the reason for this situation is that FINTRAC guidance to REs, outside of project initiatives, is on a sectoral basis with indicators for ML or TF which are intended to cover a large array of crimes.[135] FINTRAC's mandate is to deter, prevent and detect ML and TF, and not the underlying criminal activities. From FINTRAC's perspective, the ML methods and techniques used, and associated indicators, that it publishes are not believed to vary substantially between the threat actors and the source of criminal proceeds. This position stands in some contrast to concept of threat prioritisation and steps that other jurisdictions have taken to prioritise particular threats. Interviews conducted with Canadian REs for this study indicate that private sector perspectives would value a change of mindset that recognises the importance of collectively understanding the individual nature of specific (priority) economic crime threats.

Summary of key challenges in Canada:

- Individual crime threats do receive funding and government 'profile'.
- However, at a broader level economic crime threats in Canada are not prioritised at the national cross-government level or at least not communicated as such.
- Beyond the 2015 NIRA, there are no publicly stated and regularly reviewed national economic crime threat priorities, which are established and supported by a range of relevant agencies in Canada.
- The private sector therefore lack clear signals to prioritise limited analytical resources and personnel towards specific crime threats and may fail to build up subject matter expertise and efficiently allocated resources towards threats which may be relatively more important for enforcement agencies.
- In the absence of any other form of prioritisation signals, it is likely that prioritisation on financial crime threats within major regulated entities is primarily influenced by the topics raised in supervisory enforcement action.
- The current NIRA led by the Department of Finance, operational priorities through PPP project initiatives and other FINTRAC guidance only partially align and it is not clear what relationship these priorities have to the priorities of law enforcement, Public Safety or the National Coordinating Committee on Organized Crime.
- In a system with limited resources, both in terms of law enforcement and private sector resources, there is no concerted effort to marshal resources towards specific outcomes.

Recent developments in Canada:

Specific threats receive particular attention in Canada, such as human trafficking:

- Which has been the subject of the first and longest standing PPP project initiative in Canada;
- Is the subject of a dedicated threat-specific material published by FINTRAC;
- Is addressed in a National Strategy to Combat Human Trafficking, supported by an investment of CAD$57.22 million over five years, starting in 2019-20, with CAD$10.28 million annually thereafter.[136]

[135] https://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/1-eng

[136] https://www.publicsafety.gc.ca/cnt/cntrng-crm/hmn-trffckng/actns-cmbt-hmn-trffckng-en.aspx

In recent examples such as COVID-19 related fraud and Trade-Based Money Laundering (TBML), there are recent examples of cross-government coordination of effort and dedicated funding.

However, again, the most important initiative relevant to the topic of threat prioritisation of economic crime appears to be ACE Fusion. However, of course, it remains to be seen how this initiative will develop and whether Canada will embrace an effort to marshal resources across the AML/ATF regime (public and private) more effectively towards specific threats.

International comparisons

The Netherlands established the 'Financial Expertise Centre' (FEC) as a central national public-public coordinating authority, with oversight of cross-government coordination on financial crime and oversight of all national public-private financial information sharing partnerships. The FEC is a cooperative association of the Netherlands Authority for the Financial Markets (AFM), General Intelligence and Security Service, Tax and Customs Administration, De Nederlandsche Bank (DNB), Fiscal Intelligence and Information Service and Economic Investigation Service, Public Prosecution Service and the Police Force.

The Dutch 2019 'Joint Action Plan' requires the FEC to set crime threat priorities, to conduct research into coordination and prioritisation and encourages cross-agency collaboration and the development of joint projects targeting specific risks, such as prevent abuse by or through foundations, cash (illegal payment), trust sector and investment fraud.[137]

The UK National Economic Crime Centre (NECC) provides an additional model for an integrated approach to national AML/CTF coordination or prioritisation. On October 2018, the UK launched the NECC within the NCA, which includes representation from the UK FIU, City of London Police, Serious Fraud Office, Financial Conduct Authority, Home Office, Crown Prosecution Service and HM Revenue & Customs. The multi-agency centre has responsibility for planning and coordinating the operational responses across agencies, with the stated intent to bring together the UK's capabilities to tackle economic crime more effectively. The NECC has a mandate to define a set of national financial crime priorities, with supervisor and law enforcement support, and FIU and private sector engagement.[138]

The UK committed to adopting a strategic approach to address gaps in the UK evidence base for different types of economic crimes and limitations in the data and statistics collected though the National Risk Assessment process, supported by a National Assessments Centre which conducted the first formal public-private economic crime threat assessment in 2019.[139]

The U.S. Treasury Financial Crimes Enforcement Network (FinCEN) issued an advanced notice of rulemaking (ANPRM) in September 2020 to propose regulatory changes under the Bank Secrecy Act (BSA) in the U.S. The proposed amendments raise the prospect of specific priority national economic crime threats being communicated to financial institutions. The reforms would encourage regulated entities to provide information with a high degree of usefulness to government authorities consistent with both the institution's risk assessment and the risks communicated by relevant government authorities as national AML priorities. Under the proposals FinCEN Director would issue, every two years, a list of national AML priorities.[140]

More generally, in law enforcement-led public-private financial information sharing partnerships such as the UK JMLIT, HK FMLIT, Swedish SAMLIT, NL Serious Crimes Taskforce, the prioritisation process has revolved around law-enforcement investigations and National Risk Assessment priorities.

[137] https://www.rijksoverheid.nl/documenten/kamerstukken/2019/06/30/plan-van-aanpak-witwassen

[138] UK NCA, 'National Economic Crime Centre Launched', press release, October 2018<http://nationalcrimeagency.gov.uk/news/1501-national-economic-crime-centre-launched>, ; UK NCA, 'National Economic Crime Centre announced', press release, 11 December 2017; NCA presentation to the FFIS dialogue roundtable, 12 October 2018.

[139] https://www.nationalcrimeagency.gov.uk/who-we-are/publications/323-public-private-threat-update-2019-economic-crime/file

[140] https://www.fincen.gov/news/news-releases/fincen-seeks-comments-enhancing-effectiveness-anti-money-laundering-programs

In the Australian regime, the Fintel Alliance sets out intelligence priorities, and the range of relevant predicate crimes, against which Fintel Alliance performance is then self-assessed.

Table 11. Australian Fintel Alliance operational priorities.

Fintel Alliance operational priorities	Crimes investigated:
Nationally important campaigns and taskforces	• Australia's most wanted criminals • Serious Organised crime • National drug campaigns • Outlaw Motorcycle gangs • Potential terrorism and human trafficking
Responding to Regional harms	• Foreign corruption and bribery • Foreign PEPs • Visa cancellations • Multi-region drug trafficking and importation
Crimes against the most vulnerable	• Child exploitation material • Child sexual exploitation • Long distance sexual video access • Scams (various)
Exploiting Government Revenues	• Tax fraud and evasion • NDIS fraud • Family Day Care fraud (FDC) • Phoenixing and business rebirthing
Networked & Complex financial crimes	• Money mules and scams • Suspect charitable and not for profit organisations • Complex fraud and money laundering • Credit card fraud and identity theft
Technology and Sophisticated crimes	• Cyber crime • Foreign sourced money laundering • Virtual currency money laundering

The Fintel Alliance, through its dedicated annual report as a public private partnership[141], tracks overtime how specific threat-based projects have contributed to suspicious reporting inputs by REs (broken down both by partnership members and non-members) and tracks recorded law enforcement outcomes relevant to that project.

Opportunities to enhance the Canadian framework:

The cross-government national economic crime strategy (outlined in theme 2) can support public-private collaboration in the development of threat-specific intelligence relating to economic crime, to inform a more regular National Risk Assessment process.

FINTRAC, or another appropriate agency, can publish clear national (and potentially Provincial) economic crime threat priorities which should have relevance to a financial institutions' AML programme design and be recognised by supervisors.

Short of the previous proposal, law enforcement agencies might consider proactive steps to communicate priorities to regulated entities through regular updates.

[141] https://www.austrac.gov.au/about-us/fintel-alliance

FINTRAC could recognise the importance of regulated entities being responsive to law enforcement priority interests and that this should, in part, inform a risk-based approach within regulated entities.

National economic crime threat priorities can be established and reviewed on a regular basis, in line with the economic crime strategy. REs can be made aware of and understand national economic crime threat priorities and reflect those priorities in resource allocation risk-based decisions, incentivised to do so through AML/ATF supervision.

REs could benefit from understanding of the impact that Canada is having in relation to the priority threats, including disruption associated to RE engagement in addressing the threat.

Theme 4. Public-private tactical financial information-sharing

Background:

In Canada, and also around the world, public–private financial information sharing partnerships have, in many cases, developed in the early stages without the benefit of specific enabling legislation. As such, their design has been determined by the availability of (or a new interpretation of) information-sharing gateways in the pre-existing legal framework. This innovative approach to examining legal opportunities, which may have previously been overlooked or unrecognised is a hallmark of early-stage partnerships. However, beyond an early-stage partnership model validation process, the lack of specific enabling legislation for information-sharing partnerships[142], has been reported to raise a number of challenges, including:

- Lack of legal certainty in the full capabilities of the partnership
- Limitations in the financial crime topics addressed by the partnership
- Friction and delay in the information transfer process
- Limitations in private–private sharing
- Limitations in the integration of the FIU in the partnership
- Limitations in the integration of additional law enforcement agencies in the partnership
- Limitations in the ability for partnership information sharing to provide risk management benefits to private sector institutions
- Limitations on intra-public sector sharing of information
- Potential for incoherence or uncertainty between financial crime and data protection legislative priorities

A key objective of policy-makers should be to provide legal clarity for regulated entities and public agencies between the obligations set out under AML/CTF regimes and data protection and anti-competition policy priorities.

In February 2018, FATF Recommendation 2 was amended to clarify the need for compatibility of AML/CTF requirements and data protection: 'Countries should have cooperation and coordination between relevant authorities to ensure the compatibility of AML/CTF requirements with Data Protection and Privacy rules and other similar provisions (for example data security/localisation)'.[143] This mandate from the FATF standards provides an opportunity to update national legislative frameworks with an updated target operating model in mind, and in line with a national strategy for tackling economic crime.

Effectiveness challenges raised in interview:

On FINTRAC to RE sharing…

> Multiple REs recognised FINTRACs efforts to provide feedback on trends and overall challenges with STR reporting in the Major Reporters Forum, and elsewhere.
>
> However, REs highlighted that prior to the FATF evaluation FINTRAC provided feedback to major reporters on institution-by-institution basis on the quality of their STRs and how they might improve. While such feedback may arise in examinations and exit-interviews, REs stated that FINTRAC has stopped providing this level of feedback and that the lack of this feedback is hampering the learning opportunity for REs to improve their STRs.

[142] Maxwell, N (2019) 'Expanding the capability of financial information-sharing partnerships' RUSI Occasional Paper - https://www.future-fis.com/thought-leadership-in-partnership-development.html
[143] FATF, 'Methodology for Assessing Compliance', p. 26.

Interviews also consistently raised issue with FINTRACs inability to request follow up on STRs as undermining an opportunity for REs to provide additional information that may be relevant to investigations and limited feedback opportunities on STRs.

On tactical public-private information sharing (law enforcement and RE sharing)…

Looking at public-private information-sharing more broadly, REs overwhelmingly believe that Canada does not have an effective legal framework to support tactical entity-level sharing between the public sector and private sector relevant to ML and broader economic crime.

REs consistently raised the "lack of safe harbour"[144, 145, 146] for tactical level information-sharing with law enforcement to protect REs from liability from civil legal action by the subjects of the information-shared. An RE described this as the "primary and most significant barrier to effective Canadian AML/ATF information-sharing".[147]

Interviews painted a picture of the current AML information sharing regime whereby CAMLO's face a regulatory risk, that encourages over-reporting to FINTRAC; a financial crime risk, which could be more effectively addressed through dialogue with law enforcement agencies; but simultaneously REs face a privacy liability risk, should non-compulsory information-sharing take place.

Again, multiple banking interviewees noted that more effective public-private information sharing was taking place under the banner of cyber-threat and fraud prevention between the RCMP and banks.

On the need for legal reform…

Multiple interviewees raised the importance of legal reform to support public-private tactical information, beyond national-security information-sharing permitted under the current drafting of PIPEDA.

Collectively, REs described a need to have a safe harbour against liability for such information-sharing, including: civil liability, criminal liability and even commercial loss – in the scenario in which a customer account was either subject to account closure or maintained as a result of law enforcement investigative interests.

Multiple interviewees highlighted that the requirement for legal reform in this area for AML/ATF effectiveness grounds was well rehearsed between industry and the Canadian government, but there had been a consistent failure to bring forward policy proposals to create a legal gateway for such information sharing.

Some interviewees from REs expressed disappointment and fatigue at the lack of progress with the Canadian government on this issue and a fear that the political will to bring forward policy reforms would only come when there was a realisation of the scale of the threat and the systemic failings. One RE referred to a hope that Canada didn't need a "9/11 moment"[148] in order to address the broader legal challenges with the effectiveness of the system.

[144] Interview reference line code - 3450
[145] Interview reference line code - 4350
[146] Interview reference line code - 3393
[147] Interview reference line code - 1867
[148] Interview reference line code - 3371

The lack of a specific enabling piece of legislation for public-private financial information sharing was felt to "put a chill in the regime with respect to information sharing"[149] and the "people are going to err on the side of caution due to privacy risk"[150].

One interviewee criticised the lack of policy reform as "the lack of legal reform is really a failure in will to address the crimes".[151]

On RCMP engagement in exploring forms of tactical information sharing…

There was widespread praise for Project Athena, later reformed as Counter-Illicit Finance Alliance (CIFA) BC, as a significant elevation in the information-sharing between RCMP and the banks – however, essentially, this revolved around RCMP more quickly highlighting the financial activity of banks' own clients to them and there was no additional tactical information shared by RCMP to financial institutions or back to law enforcement.

RCMP was recognised and praised for its "ambition to test the waters"[152] on tactical information-sharing, but a feeling from REs interviewed in this study that there was an insufficient safe harbour for them and therefore an unacceptable litigation risk arising from broader bi-directional tactical information-sharing with RCMP.

The Canadian context – additional analysis:

Canadian public-private financial information sharing partnership arrangements (detailed in an earlier section) have not relied on any dedicated enabling legal basis and, as such, have been largely limited to 'strategic' information sharing, covering insights and indicators relevant to threats in general.

With a global perspective, this is the most basic level of public-private financial information sharing to detect crime.

In Canada, the following types of FINTRAC-to-regulated entities forms of information-sharing are prohibited in Canadian law[153]:

- FINTRAC is not able to request additional information from a bank related to an STR submitted by a bank.
- FINTRAC is not able to share information with a bank on the number of its STRs that have been passed on to law enforcement for investigation.
- FINTRAC is not able to share information with a bank that a STR, related to a specific customer, has been passed on to law enforcement for investigation.

However, RCMP have made clear in the same FFIS 2018 survey that they have previously determined that RCMP believe there is a viable (from RCMP's perspective) legal gateway to exchange tactical information with financial institutions, by authority of the Canadian Criminal Code. However, to date, the adequacy of this legal gateway for information-sharing has not been tested in court and does not enjoy the full support from regulated entities to 'test' the gateway.

[149] Interview reference line code - 4473
[150] Interview reference line code - 3941
[151] Interview reference line code - 1061
[152] Interview reference line code - 1606
[153] FINTRAC confirmed position as submitted in a FFIS survey in 2018, with reference to the PCMLTFA authority for FINTRAC to provide feedback to reporting entities in specific circumstances, as described in Section 58 of the Act

Section 462.47 of the Criminal Code states that "…a person is justified in disclosing to a peace officer … any facts on the basis of which that person reasonably suspects that any property is proceeds of crime or that any person has committed or is about to commit a designated offence."

The Commons Committee study at the time the section was introduced, the third reading in the House of Commons, and the Senate Committee studying the bill, all indicate that it was designed specifically with financial institutions in mind.

Under Section 8(2)(a) of the Privacy Act it states "…personal information under the control of a government institution may be disclosed for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose."

As such, disclosures under this provision need to be discretionary, and decisions should be made on a case-by-case basis. With these caveats in mind, the RCMP reported to FFIS as being comfortable in sharing personal information with financial institutions. In this case, consistent use would either be specific to furthering an investigation, or for the purposes of preventing or suppressing crime generally.

However, following the interview comments in this FFIS study, it appears that a public-private information-sharing partnership based on this legal gateway (i.e. RCMP directed under authority of the Canadian Criminal Code and outside of the purview of FINTRAC) would potentially result in financial institutions 'owning' the legal liability for any future determination that such information sharing went beyond the current law or violated the Canadian Charter of rights.

While different regulated entities may have different legal interpretations of the same legal gateway and different levels of comfort to explore the boundaries of these legal interpretations, it appears that the existing provision in the Criminal Code is insufficient in and of itself to provide a clear legal gateway for public-private information sharing which is law enforcement led (i.e. similar to the UK or the Swedish model of information sharing partnership).

Where tactical level information is released by Canadian public agencies, through media reports, there is some inconsistency as to whether law enforcement agencies release the names of persons charged.[154] This inconsistency limits the ability of REs to identify their exposure to the suspects in question and provide relevant reporting.

The Canadian Government's Fall Economic Statement 2020 (FES)[155] makes commitments to support greater public-private financial information-sharing, though falling short of the ambition of the statutory review and this FFIS study.

Summary of key challenges in Canada:

Canadian public-private tactical financial information sharing does not benefit from a specific enabling legal framework which is designed for purpose. As a result, Canadian public-private financial information-sharing suffers from limitations due legal uncertainty or legal constraints.

Most significantly, current Canadian public-private financial information-sharing 'project' initiatives have not facilitated the sharing of 'tactical' information; i.e. specific names or entities (identifiable information) of relevance to investigations. As such, the impact of public-private information sharing for direct benefit to law

[154] For example, cases in point are below, all in December 2020:
https://toronto.ctvnews.ca/toronto-man-faces-78-charges-after-65-firearms-more-than-18-million-in-illegal-drugs-seized-1.5233289 Name disclosed
https://www.guelphtoday.com/local-news/16-people-charged-in-big-guelph-drug-bust-3176488 Name withheld
https://vancouverisland.ctvnews.ca/30m-fentanyl-bust-carried-out-by-vicpd-b-c-combined-forces-1.5234044 Name withheld

[155] https://www.budget.gc.ca/fes-eea/2020/report-rapport/toc-tdm-en.html

enforcement investigation is substantially reduced compared with counterpart arrangements in the U.S., the UK, Australia, New Zealand, the Netherlands, Sweden, Ireland, Hong Kong, Malaysia, South Africa and Singapore.

FINTRAC is unable to share tactical information related to their STR intelligence back to regulated entities or to request follow up information from regulated entities on the STRs filed. RCMP and law enforcement agencies have a (potential and perceived) lawful basis for tactical information-sharing to regulated entities, however FFIS understands that there is no consensus amongst financial institutions on the extent to which the current legal framework allows for tactical information sharing between financial institutions and RCMP and other law enforcement agencies.

Uncertainty around legal risk of public-private financial information-sharing is a principal barrier to the effectiveness of the Canadian AML/ATF regime in Canada.

Recent developments

Project Athena / CIFA BC

In 2018, the Combined Forces Special Enforcement Unit of British Columbia (CFSEU-BC) engaged with public and private stakeholders to address a money laundering scheme impacting BC casinos. The initiative, named Project Athena, was a collaboration between private sector, law enforcement, FINTRAC and other government and regulatory bodies.

Within the existing legal framework, Project Athena provides a celebrated[156] example of how FINTRAC, RCMP and REs can collaborate, in particular, to focus on a nationally recognised priority crime threat, collaborate across sectors, tie-in the development of a FINTRAC strategic intelligence alert with relevant indicators, but progress - to some extent- action on specific to clients (i.e. some tactical level steer about what REs should be looking at and reporting in response to).

However, this initiative also highlights the limitations of the current regime. In Canada, law enforcement must first prove that an account exists before they can request information from a financial institution, in the form of a production order, on a suspect of interest. In project Athena, in the first instance, RCMP were able to do this through the information that was filed by relevant casinos relevant to bank drafts – which effectively proved the account details of the persons of interest. This process involved RCMP, effectively, providing a middle-man function between suspicion identified by casinos and further data which may be available in financial institutions in a highly manual process.

Project Athena has been reformed, since January 2020, as the Counter-Illicit Finance Alliance (CIFA)-BC. FFIS understands that CIFA is evolving to have both a provincial and a federal perspective, as a centrally coordinated but regionally responsive partnership, with a strong foundation in law enforcement priorities. FFIS understands that CIFA may have a role to draw from operational experience to identify legislative, policy and regulatory change and leverage resources for priority interests.

It remains to be seen how ACE and CIFA will coordinate and the precise division of responsibilities.

International comparisons

Canada is a particular exception in countries with a common-law legal tradition in terms of having no tactical-level public-private information-sharing within their public-private financial information-sharing partnership. The following jurisdictions' partnerships operate tactical information-sharing.

[156] Including multiple positive references to Project Athena in REs interviews as part of this study, a dedicated sanitized explanation of crime typology discovered in the FINTRAC 2019-20 Annual Report, and as part of CIFA-related materials.

- The US FinCEN Exchange
- Joint Intelligence Group (JIG) Ireland
- The UK Joint Money Laundering Intelligence Taskforce (JMLIT)
- The Australian Fintel Alliance
- The Singapore Anti-Money Laundering and Countering the Financing of Terrorism Industry Partnership (ACIP)
- Hong Kong Fraud and Money Laundering Intelligence Taskforce (FMLIT)
- The Netherlands Terrorist Financing Taskforce (NL-TFTF)
- The Netherlands Serious Crime Taskforce (NL-SCTF)
- The Netherlands Fintell Alliance (FA-NL)
- Latvia Cooperation Coordination Group (CCG)
- The Malaysia Financial Intelligence Network (MyFINet)
- South African Anti-Money Laundering Integrated Taskforce (SAMLIT).
- The Swedish Anti-Money Laundering Intelligence Taskforce (SAMLIT)
- New Zealand Financial Crime Prevention Network (NZ-FCPN)

Canada is the only common-law jurisdiction in the FFIS global survey of public private partnerships, published in August 2020, that does not operate a tactical level of information-exchange in its financial information sharing partnership. In terms of partnerships making use of a legal basis specifically for law enforcement agencies to share information with financial institutions (rather than the FIU) the UK Joint Money Laundering Intelligence Taskforce (JMLIT) and Hong Kong Fraud and Money Laundering Intelligence Taskforce (FMLIT) are the most relevant models for consideration.

Internationally, a number of countries faced effectiveness limitations on the public-private financial information sharing owing to the legal gateway that was originally used to set up a 'partnership' forum. Most public-private financial information-sharing partnerships originally made new or creative use of the existing legal regime during the pilot or 'start up' phase of public-private partnerships, and then policy-makers sought to establish a legal regime that was designed for purpose.

The legal basis of the UK Joint Money Laundering Intelligence Taskforce (JMLIT), the Crime and Courts Act 2013, Section 7, provided a pre-existing legal gateway that was initially 'creatively' re-interpreted to support the development of UK JMLIT. Section 7 provides a wide legislative gateway for the UK National Crime Agency (NCA) to share information for the purpose of supporting its functions. As such, the partnership tactical sharing in the UK must be convened by the NCA, which contributed to the design of JMLIT as an in-person Taskforce meeting on NCA premises. However, this legal framework was updated under the 2017 Criminal Finances Act and is also subject to legislative enhancements to enable policy objectives set out in the UK Economic Crime Plan of 2019.

In the Netherlands, the Terrorist Financing Taskforce was founded with authority under a general article in The Netherlands Police Information Act, which requires that three conditions be met before police can share investigative information with third parties in the Netherlands:

- A pressing need.
- Substantial public interest.
- Prevention or investigation of criminal activity.

Following the success of the partnership models in the Netherlands, the Dutch government – in line with the 'Joint Action Plan' is expected to lay new legislation before Q1 2021 specifically to enable public-private and private-private information sharing to support financial crime and terrorist financing investigations.[157]

[157] https://www.rijksoverheid.nl/documenten/kamerstukken/2019/06/30/aanbiedingsbrief-plan-van-aanpak-witwassen

In Australia, the Fintel Alliance was created through a leadership level commitment to public-private information-sharing and to explore how the existing legal regime might support an uplift in the quality of public-private financial information sharing. Within Fintel Alliance, analysts from reporting entities and government agencies other than AUSTRAC are seconded to provide assistance to the AUSTRAC CEO under section 225 (Consultants and persons seconded to AUSTRAC) of the AML/CTF Act. Secondees become 'Entrusted public officials' for the purposes of section 121 (Secrecy – AUSTRAC information and AUSTRAC documents) of the AML/CTF Act. Entrusted public officials may disclose AUSTRAC information in accordance with Part 11 (Secrecy and Access) of the AML/CTF Act. This innovative use of the original 2006 act provision has provided for significant and wide-ranging benefits, however, a number of limitations on the efficacy of the regime have been identified and the legal basis for information-sharing is due to be strengthened in the Anti-Money Laundering and Counter-Terrorism Financing and Other Legislation Amendment Bill, currently before the Australian parliament.[158]

David Watts, David Medine and Louis De Koker,[159] drawing from research expertise in financial services, national security intelligence and data privacy, describe the need for a clear information-sharing legislative framework to support national security and financial crime policy objectives in coherence with civil liberties. They suggest a specific enabling legislation will, in general, require adjustments to public secrecy laws, AML/CTF non-disclosure of STRs laws, and privacy and data protection restrictions, including consideration of:

- The appropriateness of data collection, analysis and processing by regulated entities for crime detection purposes.
- Providing clarity over the functions of FIUs and law enforcement agencies in information sharing with the private sector for intelligence development processes.
- The basis for sharing, including a reasonable belief that such information will be treated securely and confidentially and aid in AML/CTF efforts.
- Clarifying any protections of liability for errors in utilities' data where their reliance was reasonable (in other words, there was no reason to doubt the accuracy of the data).

Looking to future digital and privacy preserving capabilities for public-private information-sharing, the Australian Government 2019 budget awarded funding of AUD$28.4 million over four years for the Fintel Alliance which is to support "establishing an operating platform for collaborative information sharing and intelligence development between partners" and "advancing our analytics capabilities by integrating disparate and distributed data to maximise the alerting capabilities of Fintel Alliance. "[160] The AUSTRAC Corporate Plan sets out a range of commitment in the data and analytics space, including to achieve "integrated enterprise data analytics environment on a consolidated platform"[161]

[158] https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6431

[159] David Watts, David Medine and Louis De Koker, 'Customer Due Diligence and Data Protection: Striking a Balance', 9 August 2018, <https://www.cgap.org/blog/customer-due-diligence-and-data-protection-striking-balance

[160] https://www.austrac.gov.au/sites/default/files/2019-11/Fintel%20Alliance%20Annual%20Report%202018-19.pdf

[161] https://www.austrac.gov.au/sites/default/files/2019-11/Fintel%20Alliance%20Annual%20Report%202018-19.pdf

AUSTRAC's Fintel Alliance Alerting Project (Australia)

The objective of the Alerting Project is to build a platform to identify financial crime crossing the major Australian financial institutions, which can only be identified by connecting the disparate databases held within each organisation. The use of privacy enhancing technologies is a key focus of the project and is being deployed to protect the privacy of data relating to innocent customers (including their personal details, accounts and transactions).

The Alerting Project is intended to deliver: the ability to identify whether there are any financial links between two (or more) suspicious accounts; and the ability to trace suspicious funds as they move between accounts across financial institutions.

The algorithm is designed to flag suspicious networks from domestic retail account and transaction data, while protecting the privacy of all data. No additional customer, account and transaction information will be exposed through the results of the algorithm. Where the transactions meet the criminal typology, AUSTRAC will initiate a follow up process that will be undertaken through formal notice to the relevant REs to identify the specific transactions, accounts and customers of interest.

This project focuses on data relating to domestic retail account transactions. Unlike international fund transfer instructions, domestic transactions are not automatically reported to AUSTRAC under Australian legislation and therefore represent an intelligence gap to the agency and our government partners. This is an active, funded project about to exit the "discovery" phase and enter the "alpha" phase. The project will use a federated architecture. Reporting entities will provide the federated platform with access to the agreed dataset via an API. Initially, it is intended that the project will be tested in a simulated federated architecture using a sample of real data, before the platform is implemented in the real environment. The deployed algorithm is expected to cover more than 100m accounts. The number of transactions will depend, in part, on the temporal range covered by queries - which is undetermined at the time of preparing the case study.

The specific data fields engaged by this project include:

- Transaction date;
- Transaction time;
- Account BSB and number;
- Transaction counterparty account BSB and number;
- Transaction amount; and
- Transaction description.

Further details are available here in the AUSTRAC Fintel Alliance Annual Report:
https://www.austrac.gov.au/about-us/fintel-alliance

A FFIS (September 2020) international mapping exercise of use of privacy preserving analytics to identify financial crime is available here:
https://www.future-fis.com/the-pet-project.html

Opportunities to enhance the Canadian framework:

Under an appropriate strategic national economic crime strategy (see theme 2), the ambition for public-private financial information sharing should be established more clearly. A legislative enabling environment should be created to reflect that ambition, creating a legal basis to achieve the desired capability with regard to:

- The number of regulated entities involved
- The range of regulated sectors involved
- The number of law enforcement agencies/investigators participating
- The range of financial crime threats addressed by the partnership
- The speed in which information can be transferred
- The rate (and volume) of which tactical-level cases and typology-level projects can be processed through the partnership
- The rate, volume and nature of cross-border information sharing connected to partnerships
- The extent of partnership contributions to informing policy or regulatory developments

If there can be greater clarity established around the permissibility for the RCMP to share information with financial institutions, it is possible that a law enforcement-led model of public/private partnership could be used Canada. This could follow the model of UK Joint Money Laundering Intelligence Taskforce, which operates under the legal authority entrusted to the National Crime Agency to share information.

The RCMP and other agencies can explore means to provide greater clarity over the current legal permissibility of law enforcement to bank information sharing, optimising use of the current framework. Public entities and major reporters may consider establishing a pilot information-sharing model, founded on the legal gateway to share both strategic and tactical information between the RCMP and regulated entities.

However, given the feedback of financial sector stakeholders, it is more likely that a new legal provision which provides a specific enabling clause for the public-private financial information-sharing will be required to support law enforcement-led information-sharing, either through reforms to the AML law or the privacy regime. The author notes that on 17 November 2020, the Canadian Minister of Innovation, Science and Industry, tabled proposed legislation in Parliament that aims to overhaul Canada's data privacy law: *"Bill C-11, entitled An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Act"*.[162]

It is understood by the author that the new Bill aims to emulated some aspects of the data protection rights regime established under GDPR. GDPR is the privacy legal framework for many jurisdictions that support tactical-level public-private AML/ATF information-sharing. Intrinsic in FATF Recommendation 2 is a requirement to ensure that countries establish compatibility of AML/CTF requirements and data protection. Canadian policy-makers have an opportunity to fulfil this mandate from FATF to ensure that the new privacy law adequately reflect policy-intent with regard to the AML/ATF regime and associated information sharing requirements.

Looking to the future, rather than simply emulating other countries innovations of five years ago, Canada may wish to establish a more direct, real-time and digital relationship between the FIU and transactions of major reporters, in a privacy preserving manner (as described in theme 2) and in line with the Australian intent raised above through the 'Alerting Project'.

[162] https://www.dataprotectionreport.com/2020/11/bill-c-11-canada-proposes-new-data-privacy-legislation/

Outside of legal reform, FINTRAC may be able to support greater public-private financial information sharing by providing more direct feedback on the quality and relevance of STR reporting to regulated entities.

Canadian public agencies should consider whether a facility could be established that discloses the names of charged individuals on a real-time and confidential basis to RE designed persons, allowing REs to investigate and report back to FINTRAC and LE with additional transaction and counterparties.

Theme 5. The extent of public/private co-production of strategic financial intelligence

Background:

From an international perspective, typology co-development within financial information-sharing partnerships has been a major focus for early partnership efforts. The development and distribution of typology knowledge products is the principal way that partnerships provide benefits to members and non-members in terms of heightened understanding of risk. In some models, typology co-development groups have provided an initial gateway for non-banking stakeholders, as well as NGO and academic perspectives to be involved in financial information-sharing partnerships.

Strategic co-development of intelligence has been cited as a major benefit for private sector members in public-private financial information-sharing partnerships in independent research, FATF evaluations and in national government summary reports.

Partnerships around the world have developed strategic alerts have produced strategic intelligence from topics as diverse as: terrorist financing; tax evasion; drug trafficking; fraud; "Laundromat" schemes; corruption; human trafficking; virtual assets; casinos, real estate and high-value goods; misuse of legal persons (shell companies and trusts); trade-based money laundering; wildlife and environmental crime; money laundering in capital markets; and illegal mining. Canadian initiatives could leverage from this existing body of knowledge from partnerships around the world to accelerate the rate and extent of production of typology/strategic intelligence products.

Quantitative indicators only provide a partial indication of the benefit of enhanced risk understanding in the private sector, however, some quantitative data is available relating to the impact of strategic intelligence co-development. In the UK, trade-based money laundering (TBML) was identified as a challenging financial threat to detect and was designated as a priority area for JMLIT Expert Working Group analysis and typology co-development. JMLIT TBML typologies have been credited by the NCA with supporting a 20-fold increase over a three-year period in relevant suspicious reporting, from eight reports in the first quarter of 2015 to 163 reports in the first quarter of 2018.[163] In Australia, according the Fintel Alliance, since the establishment of the partnership and its work on child exploitation crimes, there has been a 945% increase in suspicious reporting on those crimes.[164]

Effectiveness challenges raised in interview:

In terms of how public/private co-production of strategic financial intelligence (typologies/alerts) can be improved in Canada, interviewees referred to:

> The timeliness and tempo of project initiatives and ultimate publication of risk indicators could be improved, with indicators currently taking up to a year to be formally published.
>
> The time lag in project deliberations has the effect of limiting value to REs outside of the working groups and was felt by some interviewees to lead to displacement of risk from the members of a PPP working group to non-members outside of the project initiative. One interviewee described this as "it becomes about good information for who is around the table and everyone else is last to know."[165]
>
> Some REs, outside of the big 6, apparently struggle to understand how to best operationalise or ingest the typology products.

[163] UK National Crime Agency (NCA) data presented at the FFIS 2018 Conference of Partnerships, 22 June 2018.
[164] https://www.austrac.gov.au/sites/default/files/2020-11/Fintel%20Performance%20Report%202020.pdf
[165] Interview reference line code - 4652

Questions were raised in interview about a lack of information around what impact project initiatives have had from a law enforcement perspective and whether the allocation of resources was providing commensurate value.

Multiple interviewees raised that to be valuable, strategic intelligence should be built on tactical insight.

REs referred to the limits of what can be done with typologies, outside of tactical information, and raised fentanyl as an example where harmful behaviour is very difficult to distinguish from innocent behaviour absent tactical guidance from public agencies.

REs referred to the current project initiatives, in general, being dominated by the banking sector, rather than being cross-sectoral.

Project initiatives being published as risk indicators in Operational Alerts, through FINTRAC, were criticised as being in some instances very broad and leading to sets of rules that would catch a very large proportion of a customer base.

Moving forward, REs talked about the need to expand the scale of data and improve the use of advanced analytical techniques to identify behaviour and associations that a human would not be able to identify through machine learning. However, to achieve this development in typologies, tactical insights from the public sector would be required to instruct such models.

There was a call for a time-limit to put on PPP project initiatives, as one RE described the problem as follows: "You don't want to be the bank that says 'no' to an important topic, but these projects don't end. Everything is additive. There is a prioritisation problem."[166]

Another RE perspective questioned whether projects were identifying the predicate offence or money laundering. As an example, Project Shadow focused on uncovering the Child Exploitation Material (CEM). However, in this case it is very difficult to identify ML/proceeds of crime and if they are using legitimate funds to buy CEM material, there is no proceeds of crime. Therefore, there may be a challenge as to whether an STR can be filed under PCMLTFA.

REs referred to the value of FINTRAC's work and alerts on COVID-19 during 2020, which included thematic feedback on the implications of COVID-19 for reporting trends.

In terms of how far detailed typologies can be circulated with the regulated community, it was recognised that there is a challenge that indicators "may teach criminals of how to evade detection"[167].

The Canadian context – additional analysis:

As outlined earlier in this report, Canadian public-private financial information sharing efforts have revolved around strategic information sharing 'project initiatives'.

These project initiatives have been credited with a number of successes.

[166] Interview reference line code - 1450

[167] Interview reference line code - 1398

The Canadian typology co-development initiative 'Project Protect' was launched in January 2016 and focused on developing and distributing risk indicators of human trafficking. FINTRAC data indicates that the public–private typology development project resulted in a four-fold increase in the number of human trafficking Suspicious Transaction Reports after the first year of the project. In terms of quality indicators, these reports saw a five-fold increase in the disclosures by the Canadian FIU of actionable intelligence to law enforcement agencies, indicating both measurable quantity and quality improvements as a result of the typology co-development initiative.[168]

The existing Canadian project initiatives are detailed in an earlier section of this report.

FINTRAC, from a supervision perspective, appears to encourage the use of partnership typology products to support compliance education processes, ensuring that there is a connection between the supervisory examination process and the extent to which relevant regulated entities have ingested the typologies in their risk-based approach. FINTRAC, through its Assessment Manual and other guidance provided on its website, already requires its reporting entities to take a risk-based approach and assess the ML/TF risks it faces based on various FINTRAC publications and other similar documents published domestically and internationally.

Key challenges in Canada:

Despite their success, the tempo and bandwidth of public-private co-production of strategic intelligence typologies in Canada is low compared to similar foreign jurisdictions.

Project initiatives take approximately a year to develop and the Canadian approach has historically been restricted in bandwidth to commencing one typology project per year.

International comparisons

As the leading partnership in this aspect, the UK JMLIT is only matched in the rate of production of strategic intelligence products by the German AFCA partnership and stands out in the sheer volume of products produced; being responsible for 49 'JMLIT Alert' reports between its establishment in April 2015 and June 2020.

Table 12.
Rate of co-production of strategic typology products within financial information-sharing partnerships.

🇬🇧	🇭🇰	🇩🇪	EUROPOL	🇦🇺
JMLIT	**FMLIT**	**AFCA**	**EFIPPP**	
10 typology products per year	4 typology products per year	10 typology products per year	5 typology products per year	6 typology products per year

In the U.S. 2020 National Illicit Finance Strategy highlighted the importance of producing alerts and advisories that reach beyond the largest financial institutions to include, small banks, money transmitters, and broker-

[168] The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), 'FINTRAC Tactical Intelligence: Project PROTECT', <https://beta.theglobeandmail.com/files/editorial/News/0219-nw-na-trafficking/PROJECT-PROTECT.pdf>

dealers, as well as other sectors that have an important role with respect of being gatekeepers or otherwise having valuable information or insights into risks. As an example, the strategy highlights “targeted advisories to the shipping, insurance, and aviation industry to assist them in identifying potential sanctions evasion activity” and how “Treasury has also engaged with key participants in the real estate market about sale and purchase trends and illicit finance risks identified in the real estate in the national risk assessments and other Treasury advisories”.[169]

While typology products have been linked to increased reporting from regulated entities, AML/CTF supervisors - outside of Singapore - have not yet formally recognised partnership typology products as having value as supervisory guidance or educational value for compliance purposes. From a regulatory-risk perspective, a regulated entity must ensure that they are using a set of rules and scenarios which will be satisfactory for their risk appetite and their supervisory examiners. However, generally, partnership typology products are not benefiting from supervisory recognition to the extent that they can provide an authoritative basis for revising model rules.

In contrast, in Singapore, ACIP typology products have been actively leveraged to inform and enhance the quality of compliance in regulated entities outside of partnerships.[170] As one of the few partnerships designed and led from a supervisory perspective, the Singapore ACIP specifically set out to highlight red flags, typologies and set out industry best practices for the identification and mitigation of risks that would have standing as a compliance education tool. The partnership does not enable tactical information-sharing, but partnership typologies have supported training sessions for regulated entities, been incorporated into broader training provided by the banking association and now form part of a university compliance elective module.

Opportunities to enhance the Canadian framework:

Canadian public and private stakeholders should increase the ambition for the rate and extent of development of strategic intelligence typology products. As resources allow, this partnership forum may consider how to enhance:

- The rate of production of typology products;
- The number of financial crime threats covered;
- The number of regulated sectors and entities participating in the knowledge exchange process;
- The number of localised typology products to reflect the unique characteristics of certain regions, or certain criminal networks;
- The responsiveness and timeliness of the development of the knowledge products;

This effort could leverage the increasing library of strategic intelligence products produced in other jurisdictions and re-evaluate them in the Canadian context, thereby building on previous analytic efforts rather than duplicating international effort.

FINTRAC might seek to support the ‘industrialisation’ of typology papers and embed them into the supervisory processes.

To complement human analyst generated typologies FINTRAC could support the digitisation and sharing of typologies as data models, developed through machine learning techniques, that can be integrated and overlayed onto digital systems.

[169] https://home.treasury.gov/system/files/136/National-Strategy-to-Counter-Illicit-Financev2.pdf

[170] See Association of Banks in Singapore, ‘Industry Guidelines’, <https://www.abs.org.sg/industry-guidelines/aml-cft-industry-partnership>

Theme 6. Relevance to law enforcement outcomes

Background:

"Money Laundering threats are detected and disrupted, and criminals are sanctioned and deprived of illicit proceeds." – Financial Action Taskforce (FATF) Intermediate Outcome 3 within an effective system to combat money laundering and terrorist financing.[171]

Ultimately, the AML/ATF regime is intended to provide a regulatory framework for private sector entities to file reports of suspicious activity or transactions and take 'preventative measures' designed to be of value to law enforcement investigations, criminal justice outcomes and crime prevention more broadly.[172]

However, a major challenge in the implementation of the FATF framework has been relatively low levels of observable impact on economic crime generally. Part of the challenge is very significant disconnect between what is reported by REs and what is used by law enforcement agencies. The FFIS research programme previously reported that interviews conducted with past and present FIU heads indicated that over 80% of suspicious activity or transaction reports were believed to be of no operational value to active law enforcement investigations.[173] Europol, using a different methodology identified that only 10% of suspicious transaction reports across Europol member countries are investigated further after the initial report is made.[174]

Law enforcement agencies, in every jurisdiction, have limited resources and capacity to take action in response to reports of criminality and must prioritise their activity. In the experience of the FFIS programme - reflecting on a common theme from over 50 events worldwide in three years that provided a chatham house-rule level of discussion between senior law enforcement officers, FIU figures, policy makers and private sector participants - law enforcement agencies can often have a low appetite for being presented with cases from other agencies which do not already correspond to their priorities.

Considering the intelligence cycle more broadly[175], senior decision makers through to operational analysts consider the needs of operational arms, or other customers of intelligence, to direct intelligence collection; not the other way around.

If disruption of criminality through law enforcement action is a principal objective of the AML/ATF regime, then law enforcement priorities and an orientation towards law enforcement information requirements, will likely need to have a central role in determining intelligence collection requirements through the AML/ATF regime.

In terms of public-private financial information-sharing partnership efforts, a number of partnerships around the world are directly led by law enforcement agencies, which has the advantage of ensuring a stronger link between partnership projects and law enforcement appetite for progressing the intelligence through to an investigation.

[171] http://www.fatf-gafi.org/publications/mutualevaluations/documents/effectiveness.html
[172] http://www.fatf-gafi.org/publications/mutualevaluations/documents/effectiveness.html
[173] RUSI Occasional Paper, 'The Role of Financial Information-Sharing Partnerships in the Disruption of Crime', Oct 2017, Nick Maxwell and David Artingstall
[174] Europol, 'From Suspicion to action - Converting financial intelligence into greater operational impact', September 2017
[175] https://www.canada.ca/en/security-intelligence-service/corporate/publications/2019-public-report/the-intelligence-cycle.html or https://www.intelligencecareers.gov/icintelligence.html

Effectiveness challenges raised in interview:

Multiple interviewees raised the importance of law enforcement investigative priorities and for FINTRAC and REs to align to those priorities.

REs generally believe that the current AML/ATF reporting framework is characterised by a drive towards volume for FINTRAC in the hope that enough information will be collected such that it will provide a useful source of data for law enforcement agencies.

Multiple REs believe this approach generally does not provide timely reporting relevant to live cases for law enforcement agencies, and it does not provide law enforcement with a basis to take timely action in response to 'crimes in progress' identified by REs. "The money has left long before law enforcement gets to see the intelligence through FINTRAC", explained one RE.[176]

Law enforcement agencies can make requests from FINTRAC for information in response to a specific case need, however this process has again been referred to as "often too slow"[177], by those with direct experience.

The intelligence cycle in the Canadian AML/ATF regime is "built backwards"[178], based on volume reporting which is disconnected to law enforcement interests, creating "a vast database of historic transactions which no longer reflect reality".[179]

A number of REs believed law enforcement agencies could be more active in communicating their needs to REs, particularly to communities of small and mid-tier organisations who are "not at the table"[180] of the various working groups and projects.

Production orders appear to be the main contact point on tactical information with law enforcement agencies in Canada. "When you receive a production order, there is a clear mandate about we can provide and what we should provide."[181]

REs highlighted that sometimes information requests through production orders can be written in a way which misses the key value that the REs can provide, or information which REs believe is relevant to support the investigation. It was noted that, where inter-personal relationships are strong, law enforcement teams can benefit from guidance from the REs as to "what might be useful to ask for"[182], though this type of advice to law enforcement was a difficult balance for REs and exposed them to privacy risks.

However, REs raised concerns with timeliness of the process as a whole in that it takes 30 days for law enforcement to receive the result of a production order, and that law enforcement agencies must have already confirmed that a relevant account exists prior to preparing and submitting the production order. This length of time is believed to be "completely inadequate to keep pace with money laundering activity."[183]

[176] Interview reference line code - 2715
[177] Interview reference line code - 4463
[178] Interview reference line code - 1382
[179] Interview reference line code - 3355
[180] Interview reference line code - 1365
[181] Interview reference line code - 2159
[182] Interview reference line code - 1283
[183] Interview reference line code - 4491

> “All it takes is for the bad guys to send the money around a few accounts to stop law enforcement finding it. Send the money outside of Canada and bring it back, just once, and this would add a few months to an investigation”[184], claimed one RE.
>
> “We’re a dinosaur compared to money launderers. We only catch the idiots.”[185] explained another RE, referring to the Canadian AML/ATF system as a whole.
>
> In terms of current public-private partnership initiatives, one RE described recent PPP project initiatives as producing “filing effectiveness”[186] but there was some doubt as to what extent project initiatives have aligned to law enforcement interests or to what extent reporting has been taken forward to support law enforcement outcomes.
>
> An RE highlighted that “a number of years ago”[187], there were stronger direct links with law enforcement teams, but the practice of sharing regular information direct with law enforcement had been stopped to due privacy liability risk concerns.
>
> Other REs did highlight RCMP communications, the value of law enforcement engagement in working groups and projects, and pointed to regular RCMP engagement in the Major Reporters Forum.
>
> REs noted that feedback across provinces and at the federal level was fragmented and very dependent on an individual officer and that officer’s experience and confidence with engaging REs.
>
> The ACE Fusion and CIFA initiatives were noted in terms of their promise to support a more effective model of collaboration and orientation towards law enforcement needs, but uncertainty was expressed in interview as to what both initiatives would ultimately focus on.

The Canadian context – additional analysis:

In its ‘Strategic Plan 2019–24’, FINTRAC emphasises its principal financial intelligence role as “support[ing] Canada's broader policing, national security and foreign policy priorities, including in relation to the links between money laundering and criminal activity, and the resourcing of terrorist groups.”[188]

In addition, the 2019-20 FINTRAC Annual Report included a list of statements about the ‘Value of FINTRAC Disclosures’ from users of FINTRAC intelligence, showing a very positive response from a wide range of law enforcement agencies.[189]

However, looking from a more strategic perspective, the Canadian AML/ATF regime, viewed as part of an intelligence cycle framework, does appear to ‘built backwards’ with regard to the role of law enforcement operational needs.

In the Canadian AML/ATF system, REs determine what they file and do not have tactical information about criminality from law enforcement or intelligence agencies which assists them to prioritise. REs therefore ‘collect’ and report with limited awareness of collection requirements of end-users of the information.

[184] Interview reference line code - 2218
[185] Interview reference line code - 1777
[186] Interview reference line code - 2228
[187] Interview reference line code - 2775
[188] https://www.fintrac-canafe.gc.ca/fintrac-canafe/1-eng
[189] https://www.fintrac-canafe.gc.ca/publications/ar/2020/1-eng#s1

FINTRAC, as the government agencies tasked with collecting reports and forming intelligence disclosures, is not permitted to provide any feedback to REs on filed reports and (as outlined in theme 3) does not provide a clear sense of priorities for 'collection' to REs.

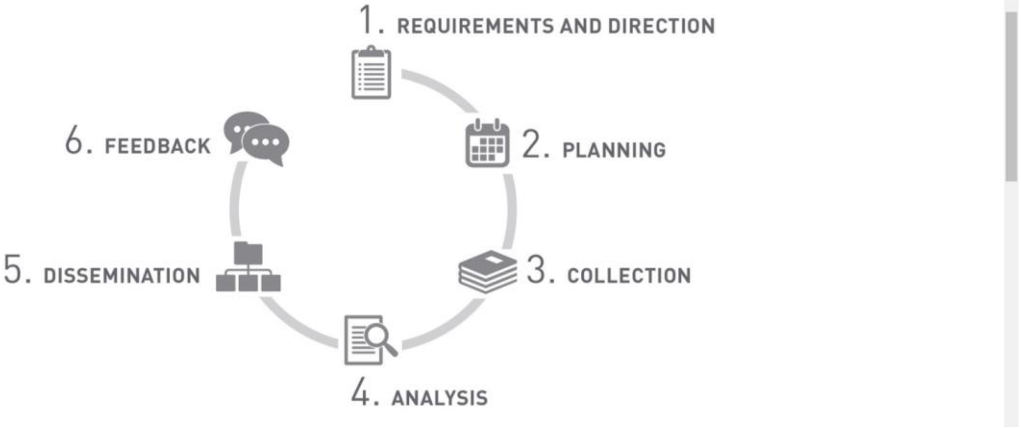
Therefore, in a framework that was originally conceived as one that protects Canadian's privacy, FINTRAC has a perverse incentive to collect as much reporting as possible, in the hope that there will be useful information for law enforcement. The vast majority of the reported information to FINTRAC will likely relate to the innocent behaviour of Canadians. FINTRAC operates one of the most aggressive collection regimes of financial transaction data in the world, securing one of largest volumes of RE reporting among FIUs worldwide and far eclipsing the United States by 10million reports per year.[190]

End-user law enforcement agencies of the intelligence are, as yet, unable to communicate tactical level insights through to REs in any formalised way. End-users can make production order requests of REs, but with a 30-day period for a response. End users can also make requests from FINTRAC for information in response to a specific case need, a however there are concerns that this process does not achieve a timely response. However, that would be relevant to crime-in-progress financial behaviour and ultimately relies on FINTRAC finding relevant historic data, rather than real-time information from REs.

There is very limited evidence that the Canadian AML/ATF regime is oriented around law enforcement outcomes in any systemic way, or that AML/ATF information produced in a manner or a process that could be relevant to disrupting ML crimes 'in progress'.

Unlike, the U.S., Australia or the UK, law enforcement agencies don't have direct access to the filing database at FINTRAC. Instead, FINTRAC takes time to work reporting into case disclosures, to provide a package of intelligence. Law enforcement are generally not able to see individual STRs. As a result, feedback opportunities to contributing REs as to what individual elements of information are useful to law enforcement is not possible.

Fig. Canadian Government description of The Intelligence Cycle[191]



[190] https://www.fintrac-canafe.gc.ca/publications/ar/2020/1-eng and https://www.fincen.gov/what-bsa-data#:~:text=In%20fiscal%20year%202019%2C%20more,other%20financial%20crimes%2C%20and%20terrorism.

[191] https://www.canada.ca/en/security-intelligence-service/corporate/publications/2019-public-report/the-intelligence-cycle.html

Table 13. Intelligence stage and Canadian AML regime challenges:

Requirements and direction	End-users of AML intelligence are at least two-steps removed from collection. End-users can request voluntary information records from the historic database of transactions that is held by FINTRAC, though this process may take time.
Planning	There is no direction of intelligence collection, and therefore no planning in an intelligence sense.
Collection	30,000+ REs form their own view of collection requirements. In the absence of a collection direction, volume reporting appears to be a strategic goal of the system.
Analysis	FINTRAC analyses STR reporting and produced intelligence material.
Dissemination	FINTRAC disseminates disclosures to law enforcement on a proactive or reactive basis.
Feedback	There is no tactical-level feedback to REs from either end-users or FINTRAC

Key challenges in Canada:

- While there have been isolated examples of RCMP-led financial information-sharing, there is no persistent national-level financial information-sharing partnership which is directed by law enforcement operational priorities.
- Without a strong steer from an operational user of intelligence, the existing Canadian project initiatives have historically struggled to achieve a sense of priorities and to ensure that users of intelligence have acted on the material produced by the project initiatives.

International comparisons:

Around the world, public-private financial information sharing partnerships vary in how they are constituted and which public-agency takes the lead.

A number of partnerships are directly led by law enforcement agencies: including the UK Joint Money Laundering Intelligence Taskforce (JMLIT); Hong Kong Fraud and Money Laundering Intelligence Taskforce (FMLIT); The Netherlands Terrorist Financing Taskforce (NL-TFTF); The Netherlands Serious Crime Taskforce (NL-SCTF); The Swedish Anti-Money Laundering Intelligence Taskforce (SAMLIT); The Europol Financial Intelligence Public Private Partnership (EFIPPP).

Law enforcement-led partnerships tend to achieve significant results in terms of criminal justice indicators of impact, due in a large part because the 'customer' of the intelligence and the relevance of the information-exchange to an ongoing investigation is clearly established. The quantitative indicators of impact for the UK and Hong Kong public-private financial information sharing is set out below:

Table 14. Quantitative indicators of impact of public–private financial information sharing partnerships

		Quantitative indicators of impact	Time period
🇬🇧	**JMLIT**	750 cases[192]; £56m in asset seizure or restraint; 210 arrests; over 5,000 suspect accounts linked to money laundering activity identified by JMLIT members that were not previously known to law enforcement (leading to closures of 3400 accounts by financial institutions); and 49 Alerts (strategic intelligence products) produced.	February 2015 to June 2020
🇭🇰	**FMLIT**	108 cases have been presented to FMLIT, leading to the identification of 8,162 accounts, 379 persons and 513 companies relevant to investigations (previously unknown to police). $646.8 million HKD of assets have been frozen, restrained or confiscated; $105.6 million HKD of loss to fraud has been actively prevented; 250 persons have been arrested; and 16 prosecution cases have been achieved as a result of FMLIT information sharing.	May 2017 to May 2020

[192] Referring to 'Section 7s' of the UK Crime and Courts Act 2013.

For Financial Intelligence Unit-led partnerships, there can sometimes be a disconnect between the intelligence collection process and law enforcement interests.

However, the U.S. FinCEN Exchange model is entirely directed around a law enforcement customer, with variable RE membership on a case-by-case basis, at the determination of FinCEN. Participation in FinCEN Exchange meetings is by invitation only, as determined by FinCEN and relevant law enforcement agencies specific to the case at hand.

The U.S. 314(a) PATRIOT Act gateway allows for direct queries of RE with regard to tactical information. Traditionally, FinCEN forwards requests from law enforcement under 314(a), following a quality review, through secure communications to more than 39,000 points of contact at more than 16,000 financial institutions. The requests contain names of relevant individuals or businesses with pertinent identifying information. The institutions are required to query their records and respond with matches within two weeks. Section 314(a) requests are credited by FinCEN with significant intelligence gains.[193]

Opportunities to enhance the Canadian framework:

As appropriate to the Canadian broader economic crime strategy (theme 2), Canada can achieve a legal framework which provides for the desired level of information-sharing between REs in response to law enforcement requests and live investigations.

The legal provisions for public-private financial information sharing achieve the strategic target operating model, developed through consultation and articulated in a policy and operational economic crime reform strategy.

Law enforcement investigative interests, as part of the delivery of the economic crime strategy for disruption, are the principal orientation for AML/ATF activity which is intended to achieve or support ‘disruption’.

‘Prevention’ functions of the AML/ATF regime are also geared around broader crime prevention strategies.

[193] The latest FinCEN 314(a) Fact Sheet, dated Sept 2017, states that, on average, for every 314(a) request: ten new suspicious accounts are identified; 47 new suspicious transactions are identified; and ten follow-up initiatives are taken by law enforcement agencies with financial institutions. The Fact Sheet also indicates that no less than 95% of 314(a) requests have contributed to arrests or indictments. However, it should be noted that 314(a) requests are tightly focused and arise only out of significant law enforcement investigations.

Theme 7. Private-private financial information sharing to detect crime

Background:

Professional money launderers are known to open and manage multiple accounts, across multiple financial institutions.[194] However, the traditional approach to identifying financial crime through national anti-money laundering reporting systems is based on individual financial institutions observing their own business data in isolation from other financial institutions. As such, analysis to identify suspicious activity is taking place on fragmented financial data, with only partial visibility of potential criminal networks.

Effectiveness challenges raised in interview:

In Canada, due to the concentration of the banking sector, some REs believe there is an opportunity to support a much more effective, system-wide, transaction monitoring process by allowing the largest financial institutions to collaborate in transaction monitoring and allow for information-sharing in the detection of ML (i.e. pre-suspicion information sharing).

Multiple interviewees believe that the special carve out for fraud related (pre-suspicion) information-sharing within PIPEDA should be expanded to ML and broader economic crime detection and prevention.
"We have done a lot of thinking about what legislation we need to do this"[195], an RE explained in reference to private-private pre-suspicion AML information sharing. Banks are understood to have drafted proposed legislation, with versions for either PIPEDA or PCMLTFA reform, which would provide a suitable gateway for pre-suspicion information sharing.

Some REs referred to the need to hardwire obligations to share and collaborate between REs into the regulatory system, to ensure that REs collaborated to identify economic crime spanning multiple institutions. Again, this time in reference to private-private information-sharing, REs referred to the superiority of the Canadian approach for tackling fraud and cyber threats, when compared to ML.

REs referred to the international trend of financial institutions achieving greater coordination between or amalgamating their AML, fraud and cyber risk teams to provide "a more holistic understanding of risk"[196]. However, the very different treatment of fraud within Canadian law does not facilitate this approach in Canada.

REs referred to private/private sharing as providing an opportunity to more convincingly respond to the scale of economic crime facing Canada, with public/private financial information sharing more relevant to threats known to law enforcement. In complement, private/private sharing is felt to be able to operate at scale and be relatively more effective at identifying previously unknown risks and to support more consistent actions to 'prevent' access to the financial system of illicit funds.

REs referred to the very high levels of trust and confidence between the CAMLOs of the big 6 banks, supported by regular dialogue on sector-wide issues. However, the same forums for regular dialogue were not believed to be in place for Schedule II banks.

[194] FATF, 'Professional Money Laundering', 2018. <http://www.fatf-gafi.org/publications/methodsandtrends/documents/professional-money-laundering.html>
[195] Interview reference line code - 2970
[196] Interview reference line code - 1919

The Canadian context – additional analysis:

PIPEDA exemptions set out where private-private economic pre-suspicion information-sharing can take place. Such sharing is permissible for fraud prevention, but not for the prevention of money laundering.

Under the provisions of PIPEDA, a bank may share limited information with another bank without client consent for the purposes of "investigating a breach of an agreement or a contravention of the laws of Canada or a province that has been, is being or is about to be committed" or "detecting or suppressing fraud or of preventing fraud that is likely to be committed"[197].

The first case suggests that there is knowledge of a crime that has, is, or is going to take place. In contrast, under the PCMLTFA/R, the threshold for reporting to FINTRAC only requires that the reporting entity has "reasonable grounds to suspect". The implication of the higher PIPEDA threshold (which implies "knowledge") is generally read to preclude the AML investigative unit at one bank from sharing information with another bank.

The second case is limited to fraud and does not include the actual offense of money laundering or any other predicate offense from which the proceeds of crime could be derived. This limitation further restricts the circumstances under which the AML investigative unit of one bank generally believes that it can share information with another bank.

Both of these cases reduce the effectiveness of the Canadian regime by limiting the ability of banks to share information on those customers for which they have submitted STRs or have decided to terminate their relationships.

As a result, under the existing PIPEDA provision, it is understood that there is an ability to share information between financial institutions related to fraud, but a similar exemption is not provided for (the arguably more serious) offences related to money laundering and terrorist financing.

Key challenges in Canada:

There is no clear legal gateway for regulated entities in Canada to permit the sharing of information with counterpart financial institutions relating to financial crime risks (in this section we are concerned with sharing prior to the determination of suspicion).

Canadian regulated entities face privacy law and competition law restrictions which prevent financial crime risk (pre-suspicion) information sharing.

The lack of a legal provision in Canada to support private-to-private sector information sharing to determine suspicion of money laundering undermines the detection of economic crime that spans multiple financial institutions. As a result, criminal networks can easily establish themselves in alternative financial institutions should an account ever be closed at any given financial institution.

[197] https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

International comparisons

Legal frameworks in the UK[198], US and the Netherlands provide specific gateways for private–private information sharing.

In the US, there has been considerable progress and innovation in the use of existing legal provisions for private–private sharing under the provisions of the U.S. PATRIOT Act. The PATRIOT Act, section 314(b), created a voluntary programme that enables pre-SAR sharing and gives legal authority for financial institutions to share information with one another for purposes of identifying, and, where appropriate, reporting activities that may involve possible terrorist activity or money laundering.[199] The number of institutions engaged in the 314(b) process has nearly doubled between 2014 and 2018.[200]

In 2015, a group of major banks in the US initiated a partnership to better exploit the legal provision of 314(b) and develop a more effective network intelligence picture of financial crime threats across participating entities. The private–private partnership supports co-location of analysts and real-time exchange of information. The partnership has reportedly worked on a large number of major cases, covering human trafficking, corruption, narcotics trafficking, trade-based money laundering, proliferation and sanctions evasion. Members report the benefits to include a more holistic view of criminal networks and supporting arrests, convictions, asset seizures and forfeiture, though no public performance statistics are available for the partnership.[201]

More broadly, FinCEN states[202] that Section 314(b) of the PATRIOT Act supports financial institutions in:

- Gathering additional information on customers or transactions potentially related to money laundering or terrorist financing, including previously unknown accounts, activities, and/or associated entities or individuals.
- Shedding more light upon overall financial trails, especially if they are complex and appear to be layered amongst numerous financial institutions, entities, and jurisdictions.
- Building a more comprehensive and accurate picture of a customer's activities where potential money laundering or terrorist financing is suspected, allowing for more precise decision-making in due diligence and transaction monitoring.
- Alerting other participating financial institutions to customers whose suspicious activities it may not have been previously aware.
- Facilitating the filing of more comprehensive SARs than would otherwise be filed in the absence of 314(b) information sharing.
- Identifying and aiding in the detection of money laundering and terrorist financing methods and schemes.

FinCEN also highlight the importance of growing diversity across sectors in the use of 314(b) information sharing; including by broker-dealers and the insurance sector.[203]

[198] The UK has a stated policy goal to support joint disclosures of suspicious activity reports from multiple regulated entities, through private–private sharing. The UK Circular 007/2018 on the Criminal Finances Act 'sharing information within the regulated sector' is an example of legal and policy guidance clarifying the intent to support joint disclosure reporting of suspicions from multiple regulated entities. See Home Office, 'Home Office Circular: Criminal Finances Act 2017', <https://www.gov.uk/government/publications/circular-0072018-criminal-finances-act-sharing-information-within-the-regulated-sector>,

[199] For more details on the USA PATRIOT Act, see David Carlisle, 'Targeting Security Threats Using Financial Intelligence: The US Experience in Public–Private Information Sharing Since 9/11', *RUSI Occasional Papers* (April 2016).

[200] *Wall Street Journal*, 'In the Name of Security, Banks Share Information', 20 June 2018.

[201] *Wall Street Journal,* 'In the Name of Security, Banks Share Information'.

[202] https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf

[203] https://www.fincen.gov/sites/default/files/shared/sar_tti_23.pdf

In the Netherlands, Transaction Monitoring NL (TMNL) is being explored as a platform for a new approach to transaction monitoring by the banking association and Deloitte. The Netherlands has a policy mandate for the national regulator to support KYC and TM functions as a utility for regulated entities and TMNL is being established by the five largest banks in the Netherlands as a Joint Venture. The objective is to provide a platform to collect and analyse all the members' transaction information and apply typologies and algorithms to the combined data.

Opportunities to enhance the Canadian framework:

Policy makers could consider expanding the information-sharing legal provisions beyond PIPEDA to also allow for private-private sharing relevant to investigations relating to money laundering offenses, terrorist financing offenses, and any other predicate offense included in the PCMTLFA/R.

PCMLTFA/R may also be updated to broaden its scope for information sharing (e.g. to share information that an STR has been filed on a particular customer) and include "safe-harbour" protections similar to those in section 314(b) of the USA Patriot Act, which permit information to be shared between banks for AML/ATF investigative purposes. Additionally, the scope to share information could be expanded to include the fact that a bank has chosen to exit a customer to limit risk displacement.

The Office of the Privacy Commissioner may consider developing additional guidance relating to pre-suspicion information sharing.

Theme 8. Mitigation of the negative impacts of account closures.

Background:

Professional money launderers are known to open and manage multiple accounts, on the assumption that individual accounts may be shut down, as a means to maintain the resilience of their money-laundering activities.[204] However when regulated entities are prohibited from sharing financial crime risk information on specific customers or the details of accounts closed with other regulated entities, this allows criminals who may have been subject to account closure to open up new accounts with different financial institutions. The newly targeted regulated entity must commence independent due diligence and AML investigations again. Account closures give effect to each financial institutions' efforts to protect their own institution from financial crime risk. They are rational actions from the perspective of individual institutions and, indeed, are encouraged by AML supervisors as part of 'preventative measures'.

Some level of risk displacement is also inevitable as a consequence of law enforcement pressure on criminal networks in any form. However, there is very limited evidence to indicate that risk-displacement is making an effective contribution to addressing financial crime threats overall and there is no compelling theoretical basis for it to provide such an outcome. Risk-displacement remains an entrenched characteristic of many AML/ATF regimes around the world, as the principal outcome following the determination of suspicious activity by a regulated entity, but with very limited evidence of the systemic value of such activity.

There are two major risk-displacement effects that we cover below:

1. The potential that the closure of an account will undermine an ongoing law enforcement investigation;
2. The challenge posed by an 'exited' risky customer simply opening up a new account in an alternative RE to continue illicit activity.

To address the first risk-displacement effect, jurisdictions have been developing 'keep open' procedures, such that law enforcement interests in an account being maintained for investigative purposes may supersede normal regulatory pressure to close accounts linked to suspicions of crime.

Effectiveness challenges raised in interview:

Interviewees raised the following points in response to questions relating to the extent of risk-displacement to another part of the Canadian AML/ATF regime when any given financial institution closes an account on the basis of suspicion of money laundering:

- "It's huge."[205]
- "We're just moving the risk around."[206]
- "It is very prevalent and it happens daily."[207]
- "The system is all about kicking the can down the street."[208]
- "This happens in almost a 100% of cases following a demarketing decision"[209]
- "It is a chain that never stops."[210]
- "At best, we are marginally increasing the complexity of their operation."[211]

[204] FATF, 'Professional Money Laundering', 2018. <http://www.fatf-gafi.org/publications/methodsandtrends/documents/professional-money-laundering.html>, accessed 29 December 2018.
[205] Interview reference line code - 4468
[206] Interview reference line code - 4513
[207] Interview reference line code - 3460
[208] Interview reference line code - 4129
[209] Interview reference line code - 4191
[210] Interview reference line code - 3471
[211] Interview reference line code - 3153

- "It is probably not providing value to the system to de-market, but it is necessary to comply with regulations"[212]
- "It is obvious that banks are being played. Clients are going to the next bank."[213]
- "The risky customers just go to the credit unions and smaller financial institutions."[214]

REs highlighted that money launderers will have multiple accounts in multiple financial institutions, so an account closure will not, by itself, result in a significant disruption to their operations.

However, an RE described that it would be wrong to think, just because as bank has accepted a de-marketed account, it means that the client is a "genuinely bad person"[215]. This is because "De-marketing can happen for a range of reasons: yes, egregious activity, but also it could just be that it costs too much to monitor a particular type of activity. Different banks have different levels of maturity, one bank may not be technically advanced enough to bank that type of business."[216]

In terms of the adequacy of law enforcement processes in Canada to request for accounts to be kept open by a financial institution to support law enforcement/financial intelligence interests, interviewees highlighted:

Some REs suggested that requests were relatively rare, once in 3 or 4 years.

Some REs indicated that the process was not clear for how to handle the requests, and there was no established guidance from FINTRAC. However, other REs reported a high degree of confidence that FINTRAC would accept the requirement to keep an account open after a law enforcement request should the issue be raised in a supervisory examination.

An RE highlighted that keep open requests can be very complicated from a risk perspective, and if there is an international component, then supervisors in the relevant jurisdictions may not have regard to any law enforcement request and take punitive action against the RE for keeping the account open.

One challenge raised is that there is no legal mandate to adhere to a keep open letter.
A further challenge, is that an RE described an expectation that FINTRAC would expect routine STR filing on a case of that sort and that after multiple STR filings at some point there would be overwhelming pressure from a risk perspective in the bank to de-market.

One perspective shared, by an interviewee with both law enforcement and private sector experience, claimed "many times when a bank know that law enforcement are interested in the account, then they close the account."[217]

REs highlighted that information on accounts closed due to fraud-risk is shared between banks, but not for ML de-marketing.

[212] Interview reference line code - 1873
[213] Interview reference line code - 2604
[214] Interview reference line code - 1473
[215] Interview reference line code - 3714
[216]Interview reference line code - 3715
[217] Interview reference line code - 1552

> An interviewee believed that the continual churn of de-marketing contributes to a 'learning' process for criminal networks about the triggers and circumstances that led to being 'de-marketed', thus enhancing their knowledge and capacity to evade such detection in the future.[218]

Key challenges in Canada:

- There is no facility or legal gateway in Canada to allow financial institutions to share information related to financial crime investigations post-suspicion.
- As a result, it is believed to be a regular occurrence that a 'de-marketed' customer who has been exited for financial crime reasons, will re-enter the financial system at an alternative point.
- In many cases, the financial institution exited the client will be able to observe the new financial institution which takes receipt of any remaining credit in the account being closed, but will not be able to provide any reference information to the new financial institution on that client.
- This process results in high-levels of duplication and ultimately does not provide a convincing preventative effect against criminals.
- Canada does not have a formal account keep open request process, however some REs do have a high confidence in Canada that FINTRAC would support and RE that complied with a keep open request.
- However, when a law enforcement agency shares information with an RE in Canada, it may result in an account closure or other action which could undermine a law enforcement investigation. This will negatively affect trust and confidence in law enforcement sharing with REs.

International comparisons:

The available data indicates that private sector partnership participants do make account closure decisions as a result of financial information-sharing partnerships. For example, over five years, JMLIT information sharing has resulted in 3,400 customers being subject to account closure.[219] In these cases, any individuals that are committed to laundering proceeds of their crimes will likely continue to attempt to launder money by alternative means and institutions, which are either complicit or vulnerable enough, until they are successful. There is also a possibility that accounts being closed by partnership members may inadvertently increase the knowledge base of criminal networks by effectively 'tipping off' the suspect as to what trigger or behaviour led to an account closure.

The US FinCEN has guidance on keep open procedures dating from 2007, which states that law enforcement agency requests to maintain an account should be in a written form, and the requirement should last no longer than six months and be recorded by the financial institution for five years. Keep open letters should be issued by a supervisory agent or by an attorney within the respective US attorney or state prosecutor's office. In the US, if a regulated entity is made aware through a FinCEN Exchange Briefing that an account is under investigation, then 'FinCEN recommends that the financial institution notify law enforcement before making any decision regarding the status of the account'. However, the FinCEN guidance confirms that keep open letters are essentially voluntary requests, stating: 'Ultimately, the decision to maintain or close an account should be made by a financial institution in accordance with its own standards and guidelines'. It remains possible that current US keep open letters also do not protect regulated entities from all supervisory, criminal or reputational risks in maintaining an account suspected of links to financial crime or terrorist activity.[220]

In Australia, since 2017, AUSTRAC does support a 'keep open' procedure through "Chapter 75" which 'specifies that the AUSTRAC CEO may exempt reporting entities from particular sections of the AML/CTF Act where a requesting officer of an eligible agency reasonably believes that providing a designated service to a customer would assist the investigation of a serious offence.'

[218] Interview reference line code - 3815

[219] Maxwell, N (2020) Future of Financial Intelligence Sharing (FFIS) research programme 'Five years of growth in public–private financial information-sharing partnerships to tackle crime'.

[220] US Treasury FinCEN, 'FIN-2007-G002: Subject: Requests by Law Enforcement for REs to Maintain Accounts', 13 June 2007.

In the Netherlands, there are strict laws that, in general, prevent a financial institution from closing an individual's account and thereby denying the individual a right to financial services. As such, upon determination of suspicion, banking clients in the Netherlands are typically moved to 'limited service accounts', which provide only basic banking services, and the regulated entity continues to report to the national financial intelligence unit as appropriate.

UK and US legal frameworks include private–private post-suspicion information-sharing legal gateways, however the evidence available to analyse their impact is so far limited.

In 2020, there is some indication that the risk of undermining a law enforcement investigation through account closures is significantly reducing engagement in the UK JMLIT partnership.

The Netherlands 'Joint Action Plan'[221] sets out an ambition to remove existing legal barriers to inter-bank data sharing of 'black listing' information related to risky entities and provide a review of the legal basis for such a mechanism in the context of GDPR data privacy obligations and providing opportunities for redress and correction for individuals to challenges their designation on such a list.[222]

In the context of the UK Economic Crime Plan,[223] a specific cross-government and industry working group has been developing a UK model for 'post-suspicion' AML/CFT information-sharing, similar to the confirmed fraud information-sharing platform in the UK, to avoid risk displacement when customers are exited by REs.

Opportunities to enhance the Canadian framework:

Canadian 'keep open' processes could be formally established and benefit from clear guidelines (to both REs and law enforcement agencies), including clarity over roles and responsibilities for the account and expectations in terms of the duration of the request.

The requirement to abide by a 'keep open' request could be given a high priority from a supervisory perspective, such an incident of an RE still closing an account despite a 'keep open request' is rare or non-occurring. As a result, law enforcement would be able to achieve a high level of confidence that an account will not be closed outside of a coordinated disruptive plan of action and the AML/ATF system removes a perverse incentive to undermine law enforcement investigations.

It is possible that a Canadian 'keep open' request regime will require a statutory underpinning to protect REs from civil liability (i.e. litigation by victims of the criminality in question, based on harm caused by not closing the account related to the criminality)

Canada could establish a legal gateway to share ML information post-suspicion, through an appropriate governance model with an opportunity for redress for innocent parties. The post-suspicion ML framework could support preventative outcomes for ML risks comparable to that available for fraud and cyber threat sharing (see box below 'Further reading on cyber security learning in the field of public-private partnerships…').

AML/ATF 'preventative measures' in Canada can be encouraged to be effective at a sector or system wide level, not just a firm-level (which may otherwise incentivise risk-displacement and harm to other REs).

REs could benefit from cost savings in terms of reduced duplication in AML activity to repeatedly identify risk relating to the same entity, (which may potentially be provided through a centralised utility with statutory underpinning) and effectiveness gains.

[221] https://www.rijksoverheid.nl/documenten/kamerstukken/2019/06/30/aanbiedingsbrief-plan-van-aanpak-witwassen
[222] https://www.rijksoverheid.nl/documenten/kamerstukken/2019/07/01/onderzoek-informatie-uitwisseling
[223] https://www.gov.uk/government/publications/economic-crime-plan-2019-to-2022

Further reading on cyber security learning in the field of public-private partnerships…

For more information on cyber security public private partnerships, please see "Countering the Cyber Threats Against Financial Institutions in Canada: A Qualitative Study of a Private and Public Partnership Approach to Critical Infrastructure Protection".[224] The study provides 19 recommendations for practices and 11 recommendations for future studies and contains a detailed literature review covering relevant developments in PPP initiatives, highlights legal and organisational barriers, examines Public Safety's role and explores the role of technology.

[224] Pomerleau, Pierre-Luc (2019) "Countering the Cyber Threats Against Financial Institutions in Canada: A Qualitative Study of a Private and Public Partnership Approach to Critical Infrastructure Protection" Northcentral University, Graduate Faculty of the School of Business and Technology Management, Dissertation

Supplementary Information:

Reproduction of public sector responses to RUSI FFIS survey on AML/ATF information sharing permissibility in Canada (May 2018)

The following represents the public sector responses to RUSI FFIS survey on AML/ATF information sharing permissibility in Canada (completed in May 2018).

SURVEY RESULTS

Information sharing from a Canadian bank to a Canadian government agency

In the normal course of its dealings with **FINTRAC**, is a bank:

a. Able to share (as part of its STR submission) information on **a transaction that it deems suspicious** relating to a customer's activities **in the specific branch/ office location** where the transaction occurred?

Public Sector Entity Response:

Yes

b. In its STR submission, able to share information on **all of the other transactions** (relating to the customer's activities over an appropriate "lookback" period) **in that specific branch/office location** that it deems suspicious?

Public Sector Entity Response:

Yes

c. In its STR submission, **required to** share information on **all of the other transactions** (relating to the customer's activities over an appropriate "lookback" period) in that particular branch/office location **regardless of whether or not the bank deems these to be suspicious**?

Public Sector Entity Response:

If you are a reporting entity in section 5 of the PCMLTFA, you have to send a suspicious transaction report to FINTRAC whenever there are reasonable grounds to suspect that a transaction or an attempted transaction is related to the commission or the attempted commission of a money laundering or terrorist financing offence.

An assessment of suspicion should be based on a reasonable evaluation of relevant factors, including the knowledge of the customer's business, financial history, background and behaviour. It could be the consideration of many factors. All circumstances surrounding a transaction should be reviewed.

Your suspicion about there being a relation to a money laundering or a terrorist financing offence may be as a result of more than one transaction. In this case, you should include all the transactions that contributed to your suspicion in the same report. Transactions that happened or were attempted at a different branch or office locations must be reported in separate reports.

“There are established mechanisms for legislative and regulatory interpretations, and therefore responses to [this question] are not available.”

d. In its STR submission, able to share information **on all of the other transactions** (relating to the customer’s activities over an appropriate “lookback” period) **in all of the branches/office locations in the country** that the bank deems to be suspicious?

Public Sector Entity Response:

Your suspicion about there being a relation to a money laundering or a terrorist financing offence may be the result of more than one transaction. In this case, include all the transactions that contributed to your suspicion in the same report. Transactions that happened or were attempted at different branch or office locations must be reported in separate reports.

“There are established mechanisms for legislative and regulatory interpretations, and therefore responses to [this question] are not available.”

e. In its STR submission, **required to** share information **on all of the other transactions** (relating to the customer’s activities over an appropriate “look back” period) in all of the branches/office locations in the country **regardless of whether or not the bank deems these to be suspicious**?

Public Sector Entity Response:

See responses to 3(c) & 3(d).

“There are established mechanisms for legislative and regulatory interpretations, and therefore responses to [this question] are not available.”

f. In its STR submission, able to share information on **all of the other transactions** (relating to the customer’s activities over an appropriate “look back” period) **in all of the branches/office locations (of its foreign affiliates) in other countries** that the bank deems to be suspicious?

Public Sector Entity Response:

If you are a financial entity and you have foreign subsidiaries or foreign branches, the suspicious transaction reporting requirement does not apply to their operations outside Canada.

“There are established mechanisms for legislative and regulatory interpretations, and therefore responses to [this question] are not available.”

g. Are there formal mechanisms in place to allow a bank to share the in-house intelligence (e.g. a new criminal scam that it is seeing in its branches) with FINTRAC and/or the RCMP and other law enforcement agencies?

Public Sector Entity Response:

Yes

With respect to question 3 (g), a formal mechanism is in place to allow a bank to share in-house intelligence with FINTRAC (i.e., through the Voluntary Information Record process), but no formal mechanism is in place for sharing this information with RCMP.

h. Expected by FINTRAC to file a STR for every unusual transaction for which there is not sufficient information for the bank to fully discount it as not suspicious? (i.e. in such a situation, is a bank expected to file a "defensive" STR submission?)

Public Sector Entity Response:

See response to 3(c). "There are established mechanisms for legislative and regulatory interpretations, and therefore responses to [this question] are not available."

i. Expected by FINTRAC to classify a customer as "high risk" after the bank has submitted one (or more) STRs on their activities?

Public Sector Entity Response:

The PCMLTFA requires that you develop a risk-based approach, which means that you must conduct a risk assessment for each client in order to determine the level of risk they pose of committing a money-laundering or terrorist financing offence. You need to determine a risk level for each client in order to determine how often you must conduct your ongoing monitoring. For high-risk clients and business relationships, you will be required to conduct more frequent monitoring of your business relationship and take enhanced measures to ascertain the identification and keep this client information up to date.

In addition, you must reassess the level of risk associated with your client's transactions and activities as part of your obligations. This is done to ensure that the transactions and activities align with what you know about your client. In turn this will help you detect suspicious transactions that may need to be reported to FINTRAC.

STRs on file should elevate the risk of the client or business relationship.

"There are established mechanisms for legislative and regulatory interpretations, and therefore responses to [this question] are not available."

j. Expected by FINTRAC to exit a customer after the bank has submitted one (or more) STRs on their activities?

Public Entity Response:

Section H of the STR provides an opportunity to describe what action, if any, was taken by you, as a result of filing a suspicious transaction report.

"There are established mechanisms for legislative and regulatory interpretations, and therefore responses to [this question] are not available."

k. Able to formally transfer a member(s) of its staff to FINTRAC to support the agency's analytical work?

Public Entity Response:

With respect to question 3 (k), this has not been done to date but could be considered if the secondee were to work within the intelligence sector at FINTRAC.

ADDITIONAL COMMENTS ON SECTION 3 (FINTRAC)

Comments of Public Sector Entities:

There are established mechanisms for legislative and regulatory interpretations, and therefore responses to questions 3(c) to 3(f) and 3(h) to 3(j) above are not available.

The following provides further background on the legislative frameworks relevant to questions in this section.

The *Canadian Charter of Rights and Freedoms* guarantees the right to be secure from unreasonable searches and seizures. Parliament is, however, permitted to authorize reasonable searches and seizures in furtherance of legitimate public concerns, with reasonableness being assessed contextually by reference to objective notions of reasonable expectations of privacy. Respecting this fundamental right, the Canadian AML/ATF Regime is designed to deter criminals and terrorist financiers from using financial institutions and other entities for their criminal purposes and to provide appropriate tools to law enforcement to combat money laundering and terrorist financing, while also respecting the privacy rights of individuals and minimizing the compliance burden on reporting entities.

As set out in Canada's *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA), Financial Transactions and Reports Analysis Centre (FINTRAC) was created as a stand-alone agency, separate from police, whose function is to receive reports from reporting entities, to analyze these reports and other information and, subsequently, to disclose financial intelligence to police. FINTRAC does not have any investigative authority with respect to money laundering, and therefore does not have the authority to compel reporting entities to provide information that is not reported.[225]

FINTRAC is an intermediary, created to ensure and safeguard the privacy provisions of citizens, so that there is vetting of information and that only high level information will be submitted to police. Regarding Suspicious Transactions Reports (STRs), the *Proceeds of Crime (Money Laundering) and Terrorist Financing Suspicious Transaction Reporting Regulations* prescribe:

- the entities that are subject to Part 1 of the Act;
- the information that must be in a suspicious transaction report and a terrorist property report;
- the time limits and the format of the reports; and
- the 'designated information' which FINTRAC can disclose.

FINTRAC provides guidance to reporting entities on their transaction reporting requirements: see http://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/1-eng.asp Also, there are mechanisms for reporting entities to seek clarifications from FINTRAC on specific questions relating to legislative and regulatory requirements.

The following excerpts from the Guidance further explain when an STR must be filed and what information must be included:

When to File an STR

[225] However, similar to frameworks in other geographical locations, Canadian law enforcement has the capability to gather additional information through separate methods such as production orders or subpoenas.

The requirement for you to report a suspicious transaction applies if you have reasonable grounds to suspect. “Reasonable grounds to suspect” is determined by what is reasonable in your circumstances, including normal business practices and systems within your industry. This applies not only when the financial transaction has been completed, but also when it has been attempted. There is no monetary threshold for making a report on a suspicious transaction. A suspicious transaction may involve several factors that may on their own seem insignificant, but together may raise suspicion that the transaction is related to the commission or attempted commission of a money laundering offence, a terrorist activity financing offence, or both. The context in which the transaction occurs or is attempted is a significant factor in assessing suspicion. This will vary from business to business, and from one client to another. An assessment of suspicion should be based on a reasonable evaluation of relevant factors, including the knowledge of the customer's business, financial history, background and behaviour. All circumstances surrounding a transaction should be reviewed.

In the normal course of its dealings with **the RCMP or other law enforcement agencies**, and the absence of a judicial warrant or production order, is a bank:

l. Able to share information on **a transaction that it deems suspicious** relating to a customer’s activities **in a particular branch/office location**?

Public Sector Entity Response:

Yes

m. Able to share information on **all of the other transactions** (relating to the customer’s activities) **in that particular branch/office location** that the bank deems suspicious?

Public Sector Entity Response:

Yes

n. Able to share information **on all of the other transactions** (relating to the customer’s activities) **in all of the branches/office locations in the country** that the bank deems to be suspicious?

Public Sector Entity Response:

Yes

o. Able to share information on **all of the other transactions** (relating to the customer’s activities) **in all of the branches/office locations (of its foreign affiliates) in other countries** that the bank deems to be suspicious?

Public Sector Entity Response:

Will depend on the legal framework of the jurisdiction of the branch or subsidiary.

p. Able to formally transfer a member(s) of its staff into a law enforcement taskforce to support its investigative work?

Public Sector Entity Response:

No

ADDITIONAL COMMENTS ON SECTION 3 (RCMP AND OTHER LAW ENFORCEMENT AGENCIES)

Comments of Public Sector Entities:

Regarding 3(p), there are currently no agreements or MOUs in place that would allow the RCMP to formally second bank staff into a taskforce to support an investigation.

The following provides further background on legislative frameworks relevant to questions in this section.

Section 462.47 of the Criminal Code states that "…a person is justified in disclosing to a peace officer … any facts on the basis of which that person reasonably suspects that any property is proceeds of crime or that any person has committed or is about to commit a designated offence."

It is the view of the RCMP that this provision provides protection to the banks in order to share. Reading material from the Commons Committee study at the time the section was introduced, the third reading in the House of Commons, and the Senate Committee studying the bill, indicates that it was designed specifically with financial institutions in mind.

Information sharing from a Canadian government agency to a Canadian bank

In the normal course of its daily operations, can ***FINTRAC***:

a. Share information with a bank on the general quality of the STRs (especially Section G narratives) that it has received from that bank over a certain period of time (e.g. the past year)?

Public Sector Entity Response:

Yes

b. Request additional information related to an STR submitted by a bank?

Public Sector Entity Response:

No

c. Share information on emerging trends in criminal activity that FINTRAC is seeing?

Public Sector Entity Response:

Yes

d. Share information on the types of STRs that the banks are most frequently submitting to FINTRAC (e.g. increased reporting of tax evasion)?

Public Sector Entity Response:

Yes

e. Share information on the values of the STRs that banks are submitting to FINTRAC (e.g. the percentage of these STRs which have a dollar value of more than $1 million)?

Public Sector Entity Response:

Yes

f. Share information on the values of the case disclosures that FINTRAC submits to the RCMP and other law enforcement agencies (e.g. the number of case disclosures that FINTRAC receives, which have a dollar value of more than $1 million)?

Public Sector Entity Response:

Yes

g. Share information with a bank on the number its STRs that have been passed on to law enforcement for investigation?

Public Sector Entity Response:

No

h. Share information with a bank that a STR related to a specific customer, has been passed on to law enforcement for investigation?

Public Sector Entity Response:

No

ADDITIONAL COMMENTS ON SECTION 4 (FINTRAC)

Public Sector Entities Response:

With respect to 4(b), FINTRAC is able to ask for “missing information from mandatory fields” but not “additional info” since this will be considered “going back to reporting entities”.

4. With respect to 4(d),4(e) and 4(f), authorities would be open to discuss what types of STR feedback could be considered most useful. It is important to note that an STR with a higher dollar value would is not necessarily be of more or less importance than an STR with a lower dollar amount.

In addition, the following provides further background on the legislative framework relevant to questions in this section.

The PCMLTFA permits FINTRAC to provide feedback to reporting entities in specific circumstances, as described in Section 58 of the Act:

Feedback, Research and Public Education
Section 58 (1) states that the Centre may

(a) inform persons and entities that have provided a report under section 7, 7.1 or 9, or a report referred to in section 9.1, about measures that have been taken with respect to reports under those sections;

(b) conduct research into trends and developments in the area of money laundering and the financing of terrorist activities and improved ways of detecting, preventing and deterring money laundering and the financing of terrorist activities; and

(c) undertake measures to inform the public, persons and entities referred to in section 5, authorities engaged in the investigation and prosecution of money laundering offences and terrorist activity financing offences, and others, with respect to

(i) their obligations under this Act,

(ii) the nature and extent of money laundering inside and outside Canada,

(ii.1) the nature and extent of the financing of terrorist activities inside and outside Canada,

(iii) measures that have been or might be taken to detect, prevent and deter money laundering and the financing of terrorist activities inside and outside Canada, and the effectiveness of those measures.

Limitation Restrictions

(2) The Centre shall not disclose under subsection (1) any information that would directly or indirectly identify an individual who provided a report or information to the Centre, or a person or an entity about whom a report or information was provided.

In the normal course of its daily operations, can ***the RCMP and other law enforcement agencies***:

i. Share tactical information with a bank on emerging trends in criminal activity that the RCMP and other law enforcement agencies are seeing?

Public Sector Entity Response:

Yes

j. Request additional information related to an STR submitted by a bank (without a judicial warrant or production order)?

Public Sector Entity Response:

No

k. Share information with the banks on the minimum dollar value of a criminal case currently required to justify a criminal investigation (e.g. $1 million)?

Public Sector Entity Response:

This question is not applicable as the RCMP does not prioritize cases on a dollar value basis. A number of criteria are used to prioritize cases which the RCMP is able to share with financial institutions.

l. Share information with the banks (which is not in the public domain) about particular individuals or entities that are currently under investigation?

Public Sector Entity Response:

Yes

ADDITIONAL COMMENTS ON SECTION 4 (RCMP AND OTHER LAW ENFORCEMENT AGENCIES)

Public Sector Entities Response:

The following provides additional background on legal frameworks relevant for these questions.

Under Section 8(2)(a) of the *Privacy Act* it states "…personal information under the control of a government institution may be disclosed for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose."

Disclosures under this provision need to be discretionary, and decisions should be made on a case-by-case basis. With these caveats in mind, the RCMP feels comfortable in sharing personal information with financial institutions as the consistent use can either be specific to furthering an investigation, or for the purposes of preventing or suppressing crime generally.