Part V
Financial Institutions

Financial institutions may be the first entities that come to mind when considering money laundering risks. Most people and companies rely on banks and other financial institutions to handle many of their financial transactions. Financial institutions offer a broad range of financial services, from savings and loans to investments and financing complex corporate transactions. It is not hard to conclude that most money launderers seek to pass their illicit funds through a financial institution at some point, and this results in significant money laundering vulnerabilities.

This Part addresses three kinds of financial institutions. Chapter 20 discusses banks and credit unions – key institutions of interest to money launderers. Chapter 21 addresses money services businesses, which are essentially an alternative to traditional banking and face well-known money laundering vulnerabilities. Finally, in Chapter 22, I examine white-label automated teller machines.

Chapter 20
Banks and Credit Unions

It has long been recognized that banks, credit unions, and other financial institutions face significant money laundering vulnerabilities. As gatekeepers to the financial system, these institutions face inherent risks of being abused by money launderers seeking to introduce illicit funds into their bank accounts and thereby cloak their ill-gotten gains with a façade of legitimacy. Bad actors may also seek to use financial institutions to transfer funds, including abroad and to legal entities such as corporations or trusts.

When the Financial Action Task Force first introduced its 40 recommendations in 1990, the recommendations focused largely on financial institutions (see Chapter 6). Although the recommendations have since expanded to include certain non-financial businesses and professions (including accountants, casinos, real estate professionals, and lawyers), they still have a particular focus on financial institutions. This is understandable given the significant risks arising in this sector and the opportunities that financial institutions have to observe suspicious behaviour. Indeed, in the 2019–20 fiscal year, the five major Canadian banks — the Royal Bank of Canada (RBC), Bank of Montreal (BMO), Canadian Imperial Bank of Commerce (CIBC), Bank of Nova Scotia (Scotiabank) and TD Canada Trust (TD) – were responsible for over 90 percent of all reports received by the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC).[1]

In this chapter, I begin by setting out some jurisdictional and other limitations applicable to my discussion of this sector. Under the *Constitution Act, 1867*, banks are federally regulated entities. As a provincial commissioner, I cannot make recommendations to the federal government or federal institutions. As I explain below, this limitation means

1 Exhibit 1021, Overview Report: Miscellaneous Documents, Appendix 15, FINTRAC Report to the Minister of Finance on Compliance and Related Activities (September 30, 2020), p 10.

that my discussion of banks is somewhat general. I then discuss the legal and regulatory framework applicable to banks and credit unions, including their obligations under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, SC 2000, c 17 (*PCMLTFA*), and regulation undertaken by the British Columbia Financial Services Authority (BCFSA) and the Office of the Superintendent of Financial Institutions (OSFI). I then turn to money laundering risks affecting financial institutions and anti–money laundering measures currently in place at those institutions. I end this chapter with a discussion of the importance of information-sharing initiatives involving financial institutions.

Constitutional and Other Limitations

Under the Canadian Constitution, the federal Parliament has jurisdiction over banks.[2] As the Supreme Court of Canada has explained, the purpose of putting banks under federal jurisdiction was

> to create an orderly and uniform financial system, subject to exclusive federal jurisdiction and control in contrast to a regionalized banking system which in "[t]he years preceding the Canadian Confederation [was] characterized in the United States by 'a chaotic era of wild-cat state banking.'" [References omitted.][3]

Although banks are subject to federal jurisdiction, the provinces regulate non-bank provincially incorporated financial institutions.[4] These include credit unions (and the roughly equivalent *caisses populaires* operating predominantly in Quebec), trust and loan companies, co-operatives, insurance companies, pension plans, and treasury branches.[5]

The evidence before me focused on banks and credit unions, the primary financial institutions that accept deposits, facilitate transfers, and conduct other activities attractive to money launderers. Credit unions are co-operative organizations: they are owned by their members, and the members are depositors. Their activities essentially consist of taking deposits from their members and lending money out in retail or residential-type lending, primarily mortgages. Some credit unions have subsidiaries offering services such as wealth management and insurance.[6]

As banks are federally regulated institutions, jurisdictional issues prevented the Commission from exploring the effectiveness of the major banks' anti–money

2 *Constitution Act, 1867*, ss 91(15) ("Banking, Incorporation of Banks, and the Issue of Paper Money") and 91(16) ("Savings Banks").

3 *Canadian Western Bank v Alberta*, 2007 SCC 22 at para 83.

4 MH Ogilvie, *Bank and Customer Law in Canada*, 2nd ed (Toronto: Irwin Law, 2013), pp 1–2, 9, 12–14.

5 There is no specific provision in the *Constitution Act, 1867*, referring to provincial financial institutions. However, the courts have interpreted section 91(15) as referring strictly to "banks" – a name that only federally chartered banks can use — and Parliament has never asserted jurisdiction over *all* financial institutions. As a result, other financial institutions have been permitted to offer "banking" services so long as they do not call themselves "banks": MH Ogilvie, *Bank and Customer Law in Canada*, pp 32–33.

6 Evidence of C. Elgar, Transcript, January 15, 2021, pp 17–18.

laundering efforts in great detail. I was pleased to hear evidence from the chief anti–money laundering officers at RBC, Scotiabank, and HSBC, who testified on their own behalf as well as on behalf of the "big five" national banks (RBC, TD, CIBC, BMO, and Scotiabank). Their testimony was heard in a rare *in camera* (non-public) hearing as a result of Ruling 24. In that ruling, I explained:

> [7] In essence the evidence sought to be heard *in camera* consists of a panel of witnesses from each of the Bank of Nova Scotia, the Royal Bank of Canada and HSBC. As I understand it, these witnesses will be testifying about money laundering typologies as well as countermeasures utilized by "the most sophisticated and largest financial institutions in the country." Commission counsel submits the evidence will be highly sensitive and will describe typologies and methods of money laundering in detail "including new and cutting-edge techniques." The evidence will also detail what the banks are doing in response and the measures they are taking to identify, prevent and address money laundering risks and activity.
>
> ...
>
> [22] The prospect of proceeding *in camera* in a public inquiry is, in general, undesirable. In the present circumstances the issues being addressed by the evidence – the methods being used by criminals to launder money through Canada's major financial institutions and the measures taken to detect and prevent them – are important ones.
>
> ...
>
> [24] In my view it would imperil the administration of justice if the evidence were to be made publicly available ... Evidence illustrating well-developed methods of laundering money may provide information useful for criminals seeking to launder proceeds of crime through financial institutions that are not as well-equipped to detect or resist them as are Canada's major banks. Even more importantly, publicizing advanced strategies and methods used by the banks to detect and deter money launderers are likely to undermine the success of those strategies by providing notice to those who are being, or are otherwise likely to be targeted.

I also noted that there was no practical way of ameliorating the risks short of an *in camera* hearing. The evidence would be of significant benefit to the Commission, and it may not have been heard in the absence of an *in camera* hearing.[7] I did not take the decision lightly, however. The public has an interest in hearing how money laundering affects important economic institutions such as banks and knowing how they respond to money laundering risks. Further, the effect of an *in camera* hearing is that the evidence can be referred to in only a very general way in this Report.[8]

7 Ruling 24, Application for *In Camera* Hearing, issued January 15, 2021, para 25.

8 Ibid, para 26.

On balance, I determined that it was appropriate to hear the evidence *in camera*, with all participants but one permitted to be present.[9] My discussion of the *in camera* hearing is therefore high level and does not reveal any specific information obtained from the panel.

All of this being said, given the similarities between services offered by banks and credit unions, many of the money laundering risks and vulnerabilities are very similar, if not the same. Further, both federal and provincial financial institutions are subject to the *PCMLTFA*. Therefore, while there are limitations on what I can recommend with respect to banks, this chapter will examine the risks inherent to both banks and credit unions, but my recommendations will be confined to provincial institutions.

Legal and Regulatory Framework

Banks and credit unions are highly regulated entities, subject to both the *PCMLTFA* and regulation by provincial and federal regulatory bodies. I review these schemes in turn.

The *PCMLTFA*

The *PCMLTFA* applies to various financial institutions, which are listed in sections 5(a) to (h.1) of that statute. These include, but are not limited to, banks (including some foreign banks), credit unions and *caisses populaires*, life insurance companies, trust and loan companies, securities dealers, and domestic and foreign money services businesses. I discuss money services businesses, whose obligations differ slightly from the other institutions I have just listed, in Chapter 21.

Financial institutions have a variety of obligations under the *PCMLTFA*. First, they must implement a compliance program, which has six aspects. Institutions must:

- appoint a compliance officer responsible for implementing the program;
- develop and apply written compliance policies and procedures that are kept up to date and, in the case of an entity, are approved by a senior officer;
- conduct a risk assessment of the business to assess and document the risk of a money laundering offence or a terrorist activity financing offence occurring in the course of the business's activities;
- develop and maintain a written, ongoing compliance training program for employees, agents, mandataries, or other authorized persons;
- institute and document a plan for the ongoing compliance training program and deliver the training; and

9 Ibid, para 28.

- institute and document a plan for a review (at least every two years) of the compliance program for the purpose of testing its effectiveness.[10]

In line with the first requirement, banks and credit unions appoint a "chief anti–money laundering officer" (often referred to as a "CAMLO").

Financial institutions have a variety of client identification and verification requirements. They must verify a client's identity in various situations, including when they:

- receive $10,000 or more in cash;[11]
- receive virtual currency in an amount equivalent to $10,000 or more;[12]
- issue or redeem money orders, traveller's cheques, or other similar negotiable instruments of $3,000 or more;[13]
- initiate and remit electronic funds transfers of $1,000 or more;[14]
- transfer and remit virtual currency in an amount equivalent to $1,000 or more;[15]
- conduct foreign currency exchanges of $3,000 or more;[16]
- conduct exchanges of virtual currency for funds, funds for virtual currency, or one virtual currency for another in an amount equivalent to $1,000 or more;[17] and
- open bank accounts or credit card accounts for clients.[18]

Financial institutions must keep records with respect to the above situations.[19] In line with how the *PCMLTFA* applies to all reporting entities, these verification measures need not be done when the client is a public body, financial institution, or a very large corporation or trust.[20] Financial institutions must also take reasonable measures to verify the identity of every person or entity that conducts or attempts to conduct a suspicious transaction before filing a suspicious transaction report.[21] They are also required to obtain beneficial ownership information when verifying the identity of an entity and to

10 *PCMLTFA*, s 9.6(1); *Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations*, SOR/2002-184 [*PCMLTF Regulations*], s 156(1).

11 *PCMLTF Regulations*, ss 84(a), 105(7)(a), 109(4)(a), 112(3)(a), 126.

12 Ibid, ss 84(b), 105(7)(a), 109(4)(a), 112(3)(a), 129.

13 Ibid, ss 86(a)(iii)(A) and 105(7)(a).

14 Ibid, ss 86(a)(iii)(B) and (F) and 105(7)(a).

15 Ibid, ss 86(a)(iii)(D) and (F) and 105(7)(a).

16 Ibid, ss 86(a)(iii)(C) and 105(7)(a).

17 Ibid, ss 86(a)(iii)(E) and 105(7)(a).

18 Ibid, ss 86(a), (b), and (c); 87; 105(7)(b) and (d); 109(4)(c) and (d); 112(3)(c) and (d).

19 Ibid, ss 10–14.

20 Ibid, ss 10, 11, 84(a), 84(b), 154(2)(m), (n), (o).

21 *PCMLTFA*, s 7; *PCMLTF Regulations*, ss 85(1), 105(7)(c), 109(4)(b) and 112(3)(b).

take reasonable measures to confirm the accuracy of that information,[22] as well as take reasonable measures to determine if a third party is involved in a transaction.[23] They also have a number of obligations with respect to politically exposed persons.[24]

The *PCMLTFA* imposes a number of reporting obligations on financial institutions. They must report, to FINTRAC:

- the receipt of $10,000 or more in cash in a single transaction[25] from a person or entity;[26]
- the initiation, at the request of a person or entity, of an international electronic funds transfer of $10,000 or more in a single transaction;[27]
- the receipt of an international electronic funds transfer of $10,000 or more in a single transaction;[28]
- the receipt of an amount of $10,000 or more in virtual currency in a single transaction;[29] and
- every financial transaction for which there are reasonable grounds to suspect that the transaction is related to the commission or suspected commission of a money laundering or terrorist financing offence.[30]

Financial institutions also have obligations to monitor their business relationships[31] with their clients. They must implement a process to review all the information obtained about a client in order to detect suspicious transactions, keep information up to date, re-assess the level of risk associated with the client's transactions and activities, and determine whether the client's transactions and activities are consistent with the information obtained about them and their risk assessment.[32] This monitoring must be done periodically based on the institution's risk assessment of the client, and enhanced monitoring is necessary for high-risk clients.[33] The institution must keep a number of records relating to this ongoing monitoring.[34]

22 *PCMLTF Regulations*, s 138.

23 Ibid, ss 134(1) and 135(1).

24 Ibid, s 116.

25 A "single transaction" includes two or more transactions conducted in a 24-hour period if they are conducted by or on behalf of the same person or entity or for the same beneficiary: ibid, ss 126–129.

26 Ibid, s 7(1)(a).

27 Ibid, s 7(1)(b).

28 Ibid, s 7(1)(c).

29 Ibid, s 7(1)(d).

30 *PCMLTFA*, s 7.

31 Financial institutions enter a business relationship with a client when they open an account for the client or, if the client does not have an account, the second time within a five-year period that the client engages in a financial transaction for which the institution is required to verify their identity (with some exceptions): *PCMLTF Regulations*, ss 4.1(a), (b); 154(1)(a) to (d); 154(2)(a) to (l) and (p).

32 *PCMLTF Regulations*, s 123.1.

33 Ibid, ss 123.1, 157(b)(ii).

34 Ibid, s 146(1).

Finally, the *PCMLTFA* creates a "travel rule." When engaged in electronic funds or virtual currency transfers, financial institutions must include specified information relating to the originator (the person or entity who requested a transfer) and beneficiary (the person or entity that received it).[35] They must also take reasonable measures to ensure that any transfers received include this information.[36] They are also required to develop and apply written risk-based policies and procedures for determining whether to suspend or reject transfers in the event that the transfer does not include the required information and for any follow-up measures they should take.[37]

FATF Recommendations

A number of the Financial Action Task Force's recommendations relate to financial institutions. Recommendation 10 sets out client due diligence measures, which include: verifying the identity of clients; identifying beneficial owners and taking reasonable steps to verify their identity; understanding and obtaining information about the purpose and intended nature of the business relationship; and conducting ongoing due diligence of the business relationship and scrutiny of transactions.[38] Recommendation 11 sets out record-keeping requirements. Recommendation 12 relates to politically exposed persons.[39] Additional requirements for banks engaged in cross-border correspondent banking are set out in Recommendation 13, and the travel rule referred to above is discussed in Recommendation 16.[40] The obligations to implement programs for anti–money laundering and counterterrorist financing, to report suspicious transactions to the financial intelligence unit, and to ensure adequate regulation and supervision of financial institutions are set out in Recommendations 18, 20, and 26, respectively.[41]

The Financial Action Task Force also published its *Guidance for a Risk-Based Approach: The Banking Sector* in 2014.[42] The report provides detailed guidance on how the recommendations relating to financial institutions should be implemented, including how they should implement a risk-based approach, how to conduct risk assessments, how to mitigate risks effectively, and the internal mechanisms that should be in place. It also provides guidance for supervisors and regulators.

35 *PCMLTFA*, s 9.5(a); *PCMLTF Regulations*, ss 124(3) and 124.1(1)(a).

36 *PCMLTFA*, s 9.5(b); *PCMLTF Regulations*, 124.1(b).

37 *PCMLTF Regulations*, ss 124(4) and 124.1(2).

38 Exhibit 4, Overview Report: Financial Action Task Force, Appendix E, FATF, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations* (Paris: FATF, 2019), pp 12–13.

39 Ibid, pp 13–14.

40 Ibid, pp 14–15. Recommendation 16 states that financial institutions should obtain accurate originator and beneficiary information on wire transfers and ensure that the information remains with the wire transfer throughout the payment chain. Financial institutions should also monitor wire transfers for the purpose of detecting transfers that lack the required originator and/or beneficiary information and take appropriate measures: Ibid, p 15.

41 Ibid, pp 16–17, 20.

42 Exhibit 4, Overview Report: Financial Action Task Force, Appendix JJ, FATF, *Guidance for a Risk-Based Approach: The Banking Sector* (Paris: FATF, 2014).

Regulation by BCFSA

Provincial financial institutions are regulated by the British Columbia Financial Services Authority.[43] BCFSA is empowered by the *Financial Services Authority Act*, SBC 2019, c 14, and administers several statutes.[44] The core business areas for which it has responsibility are: mortgage brokers; credit unions; insurance and trust companies; pensions; and Credit Union Deposit Insurance (the statutory corporation that guarantees deposits and non-equity shares of credit unions).[45]

BCFSA is the successor to the Financial Institutions Commission, which was more commonly known as FICOM. BCFSA became a Crown corporation on November 1, 2019. Its role and mandate are basically the same as FICOM: to ensure safety and soundness in the financial system. However, FICOM was not a Crown corporation. Christopher Elgar, vice-president and deputy superintendent of financial institutions, prudential supervision, at BCFSA, testified that the shift from FICOM being part of "core government" to BCFSA being a Crown corporation means that BCFSA has more transparency and latitude. For example, it now controls its own operating budget.[46] He expects that BCFSA's status as a Crown corporation will help address staffing challenges that FICOM experienced in the past. Indeed, in the 18 months prior to his testimony, BCFSA had stabilized its vacancy rate from around 30 percent to 7 or 8 percent.[47]

There are 40 credit unions in BC and two "central credit unions": Stabilization Central and Central 1. Central unions are co-operatives *for* the co-operatives; they are owned by credit unions and provide support and services to credit unions, such as treasury services, education, and payment and settlement services.[48] An advantage of this approach is that centrals can assist smaller credit unions that do not have the scale or scope to manage all services themselves. Indeed, centrals provide some anti–money laundering services, including program development, education, and screening for wire transfers. Mr. Elgar estimated that 26 of the 40 credit unions in BC use Central 1's anti–money laundering services program.[49]

BCFSA has five priorities set out in its provincial government mandate letter: risk-based supervision and consumer protection; engaging with industry; regulatory governance and legislation; deposit insurance; and anti–money laundering. This last priority involves working collaboratively with government to improve the effectiveness of the anti–money laundering regime. It was added to the mandate letter for the 2021 fiscal year.[50] I elaborate on BCFSA's anti–money laundering activities below.

43 Evidence of C. Elgar, Transcript, January 15, 2021, p 49.

44 Ibid, pp 8–9.

45 Ibid, p 6; BCFSA, "Credit Union Deposit Insurance," online: https://www.bcfsa.ca/public-resources/credit-union-deposit-insurance.

46 Ibid, pp 5, 9–10.

47 Ibid, pp 84–85; Exhibit 423, BCFSA 2020/21 – 2022/23 Service Plan (February 2020), p 6.

48 Evidence of C. Elgar, Transcript, January 15, 2021, pp 18–19.

49 Ibid, pp 19–20.

50 Ibid, pp 6–8.

Prudential Risk Regulation

BCFSA is a prudential risk regulator. Prudential risks are "those that can reduce the adequacy of [an entity's] financial resources, and as a result may adversely affect confidence in the financial system or prejudice customers." Some of the main types of prudential risks are credit, market, liquidity, operational, insurance, and group risk.[51] BCFSA accordingly supervises and regulates provincial financial institutions to ensure they are in sound financial condition and are complying with their governing laws and supervisory standards.[52] It uses a "risk-based supervisory framework to identify imprudent or unsafe business practices" and aims to identify issues or problems early on and to take corrective actions when necessary.[53]

A guiding principle for BCFSA's regulation is proportionality. This means that it considers the size of different financial institutions and adjusts its expectations accordingly. Some credit unions in BC have thousands of employees and many branches; others have a single branch and just a few employees. As a result, although BCFSA's expectations around certain core functions of governance and risk management will be the same for all institutions, the application will vary depending on the scope and scale of the institution.[54]

BCFSA and OSFI (the regulator of federal financial institutions, discussed below) take very similar approaches to their regulation. Both are prudential risk regulators and have virtually identical supervisory frameworks. They both apply a risk-based approach and consider proportionality.[55]

Anti–Money Laundering Regulation

BCFSA continues to develop its anti–money laundering regulation. Its 2020/21 to 2022/23 service plan indicates that one of its objectives is to work collaboratively with the Government of British Columbia to improve the provincial anti–money laundering regime.[56] To strengthen its role within the current regime, BCFSA will:

- amplify its focus on anti–money laundering controls in its supervisory assessment of financial institutions;
- increase scrutiny of mortgage broker applications and activities for potential money laundering risks;
- continue to report suspected money laundering activities to relevant federal partners; and

51 UK Financial Conduct Authority, FCA Handbook, section PRU 1.4, "Prudential Risk Management and Associated Systems And Controls," online: https://www.handbook.fca.org.uk/handbook/PRU/1/4.html?date=2006-08-30.

52 BCFSA, "Mandate and Values," online: https://www.bcfsa.ca/about-us/what-we-do/mandate-and-values.

53 Ibid.

54 Evidence of C. Elgar, Transcript, January 15, 2021, p 16.

55 Ibid, p 21.

56 Exhibit 423, BCFSA 2020/21 – 2022/23 Service Plan (February 2020), objective 5.1.

- increase interactions with anti–money laundering partners on a bilateral and multilateral basis.[57]

No single body or group at BCFSA deals with anti–money laundering.[58] Rather, it is part of BCFSA's assessment of regulatory compliance and operational risk, which is the same approach that was taken by FICOM.[59] Anti–money laundering and counterterrorist financing are considered in the context of whether an institution has an effective risk management program that is commensurate with its profile. BCFSA considers whether the institution: has anti–money laundering policies in place; provides reports to the board; ensures the independence of its chief anti–money laundering officer; and has policies and processes in place (for example, know-your-client checklists and suspicious transaction reporting mechanisms) to ensure that obligations under the *PCMLTFA* are being met.[60]

BCFSA's "risk matrix," which represents the approaches and methodology it uses to examine provincial financial institutions, now has an explicit line relating to anti–money laundering. This was added at the beginning of 2020, and BCFSA plans to update its supervisory framework on its website to reflect a focus on anti–money laundering as well.[61] The matrix results in a "composite risk rating," which in turn determines what kinds of intervention by BCFSA are necessary and the level of intensity of its ongoing monitoring.[62] This rating may lead to an increase in Credit Union Deposit Insurance premiums as well as increased oversight and review by BCFSA; credit unions are therefore incentivized to maintain a good composite credit risk rating.[63]

BCFSA refers to and uses a guideline produced by OSFI called "Guideline B-8: Deterring and Detecting Money Laundering and Terrorist Financing."[64] As I note below, this guideline was rescinded in July 2021 following changes to the anti–money laundering regulation undertaken by OSFI and FINTRAC. BCFSA has not issued its own anti–money laundering guidance. Mr. Elgar testified that if BCFSA receives clear direction on its anti–money laundering mandate, it may develop its own guidance; in the interim, however, it will continue to rely on Guideline B-8.[65]

57 Ibid, objective 5.1(b). The "AML partners" in the last bullet essentially refers to FINTRAC, as BCFSA has not worked with law enforcement: Evidence of C. Elgar, Transcript, January 15, 2021, p 90.

58 Evidence of C. Elgar, Transcript, January 15, 2021, pp 12–13.

59 Ibid, pp 29–30; Exhibit 417, FICOM Letter from Frank Chong to All Provincially Regulated Financial Institutions (May 5, 2016).

60 Evidence of C. Elgar, Transcript, January 15, 2021, pp 35–36, 38–39.

61 Ibid, pp 42–43.

62 Ibid, pp 40–41, 45–46.

63 Ibid, pp 105–106.

64 Exhibit 416, OSFI Guideline B-8, "Deterring and Detecting Money Laundering and Terrorist Financing" (December 2008). An archived version of the guideline can be found online at https://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/b8.aspx.

65 Evidence of C. Elgar, Transcript, January 15, 2021, pp 26–27.

Some key factors identified in Guideline B-8 for a financial institution's compliance program are as follows:

- Is there senior manager oversight of an anti–money laundering program and institution? When has an anti–money laundering report last been provided to senior management?
- Have they identified a chief anti–money laundering officer (CAMLO) responsible for implementation of the anti–money laundering / counterterrorist financing program? Is the CAMLO independent?
- Does the institution do a risk assessment of inherent money laundering / terrorist financing risks? Consider clients, products, geographic location of activities, and other relevant factors (including account transaction risk factors).
- Does the institution keep up-to-date anti–money laundering /counterterrorist financing policies? Are there know-your-client checklists and programs to verify source of funds, client identity, etc.?
- Does the institution have a written ongoing training program?
- Is there adequate self-assessment of controls?
- Is there adequate effectiveness testing?[66]

Although not everything in Guideline B-8 is applicable to credit unions, significant parts are.[67] BCFSA (and previously FICOM) also encourages all provincial financial institutions to refer to FINTRAC's risk-based guide in addition to Guideline B-8.[68]

While I appreciate that much of the content of Guideline B-8 is applicable to credit unions, I am of the view that BCFSA should develop its own guidance focused specifically on credit unions. This would ensure that credit unions are aware of BCFSA's specific expectations of them. Further, as Guideline B-8 has technically been repealed by OSFI, it strikes me that it would be useful for BCFSA to develop its own version that it can continue to update as necessary.

Recommendation 45: I recommend that the British Columbia Financial Services Authority develop anti–money laundering guidance for credit unions.

66 Exhibit 416, OSFI Guideline B-8, "Deterring and Detecting Money Laundering and Terrorist Financing" (December 2008), pp 7–8; Evidence of C. Elgar, January 15, 2021, pp 35–36.

67 Evidence of C. Elgar, Transcript, January 15, 2021, pp 25–26.

68 Ibid, p 30.

Mr. Elgar emphasized that BCFSA is making efforts to modernize and become more efficient and effective. He cited the increased focus on anti–money laundering as demonstrated by its inclusion in the risk matrix, the ongoing efforts to update the supervisory framework, and the discussion of anti–money laundering objectives in the service plan. He further noted that BCFSA is working to increase engagement and awareness of the industry about its anti–money laundering activities and expectations.[69] Members of BCFSA are in the process of obtaining the certified anti–money laundering specialist designation, and BCFSA is seeking out candidates with anti–money laundering experience when it hires.[70] When asked how the explicit focus on anti–money laundering will change BCFSA's approach, Mr. Elgar explained:

> I think it's going to have a couple of important changes. One, it's going to reinforce BCFSA's view for credit unions or insurance companies, [and] trust companies, that [anti–money laundering] is important. It is part now that we're signalling it as a line item of centralized activities. Our expectations are becoming elevated with the institutions, and it's part of our overall mandate where we're looking to engage with industry and our external stakeholders so there are no surprises. We are communicating through a number of different tools, advisories and in particular on guidelines what are our expectations as BCFSA continues to evolve, become much more modern and effective in its supervision of the financial services industry in British Columbia, [and] largely to ensure the safety and soundness. And again it comes back to the consistency to what the government's overall objectives are … a sustainable financial services economy in British Columbia. [Anti–money laundering] is one component and we just elevated that to a point where it's not getting buried anywhere in the inherent risks of operational risk.[71]

BCFSA also has a new rule-making power under the *Financial Institutions Act*, RSBC 1996, c 141. This power enables it to make rules that have the same legal force as an act or regulation. When asked whether BCFSA intends to introduce rules focused on anti–money laundering, Mr. Elgar testified that that would depend on whether BCFSA has a clear anti–money laundering mandate.[72]

Although BCFSA has taken steps toward making anti–money laundering a priority in its regulation, it appears that the organization is waiting for an explicit mandate from the Province before taking further steps, such as developing guidance and rules. Given the clear importance of BCFSA engaging in anti–money laundering regulation, I am of the view that an explicit mandate in this regard would be useful. I therefore recommend that BCFSA be given a clear anti–money laundering mandate.

69 Ibid, pp 42–44, 47–48, 80–81.

70 Ibid, pp 85–86, 88–89.

71 Ibid, pp 44–45.

72 Ibid, pp 81–82.

Recommendation 46: I recommend that the Province provide the British Columbia Financial Services Authority with a clear, enduring anti–money laundering mandate.

In Chapter 21, I recommend that money services businesses in British Columbia be regulated by BCFSA. Given the size of that industry and the significant workload that this expanded mandate will entail, BCFSA will require sufficient resources and support to take on this added responsibility. This is particularly important given that BCFSA has, in the last few years, already undergone significant organizational changes. The Province should therefore provide BCFSA with sufficient resources to create or staff a group focused on anti–money laundering. The group should also be responsible for liaising with law enforcement, public-private partnerships, and other government stakeholders.

Recommendation 47: I recommend that the Province provide sufficient resources to the British Columbia Financial Services Authority (BCFSA) to create or staff an anti–money laundering group. This group should serve as a contact point for BCFSA with law enforcement, public-private partnerships, and other government stakeholders.

Collaboration with FINTRAC

BCFSA collaborates with FINTRAC through a memorandum of understanding.[73] That agreement states that BCFSA will share the following with FINTRAC:

- the name of each institution that it plans to review for compliance with Part I of the *PCMLTFA*;
- a copy of the notes it uses to assess that compliance;
- the results of its review;
- a copy of correspondence between it and the institution regarding any compliance deficiencies;
- a description of any actions (plus the results of those steps) that BCFSA asks the institution to take to rectify deficiencies; and
- a description of progress by the institution in taking those corrective actions.[74]

73 Exhibit 419, Memorandum of Understanding between the Financial Transactions and Reports Analysis Centre of Canada and the Financial Institutions Commission (January 9, 2005). This memorandum of understanding was entered into by FICOM but has been taken over by BCFSA and is still in full effect: ibid, p 5; Evidence of C. Elgar, Transcript, January 15, 2021, p 51.

74 Exhibit 419, Memorandum of Understanding between the Financial Transactions and Reports Analysis Centre of Canada and the Financial Institutions Commission (January 9, 2005), p 2.

Mr. Elgar added that BCFSA sometimes shares statistical information as well.[75] It also provides FINTRAC with its observations relating to the institution's policies and education programs and whether these are updated and working effectively.[76] Meanwhile, FINTRAC agrees to share the following information with BCFSA:

- compliance-related information, including risk assessment information that BCFSA may use in determining which institution to review for compliance with Part I of the *PCMLTFA*;
- the result of FINTRAC's compliance actions with respect to an institution; and
- a copy of correspondence between FINTRAC and the institution regarding compliance deficiencies.[77]

Mr. Elgar explained that BCFSA uses that information when considering whether an institution has addressed a deficiency and has a mitigation plan to meet it.[78] He described the relationship between BCFSA and FINTRAC as collaborative and noted that the industry is aware that they work together.[79]

FINTRAC provides reports to BCFSA on matters such as the number of compliance examinations of credit unions it conducts, the deficiencies it observes, and the numbers of suspicious transaction reports filed.[80] Mr. Elgar explained that although it is useful for BCFSA to know the number of suspicious transaction reports filed, from a prudential point of view, BCFSA's focus is not so much on the number of reports filed but, rather, ensuring that the financial institution has the tools in place to report large and suspicious transactions.[81]

FINTRAC conducted 14 examinations of BC-based credit unions in 2017–18 and nine examinations in 2019–20.[82] In 2015–16, nearly 89 percent of credit unions examined in BC were partially deficient in terms of their policies and procedures. This fell to 67 percent in 2016–17 and 14 percent in 2017–18.[83] BCFSA conducted 22 prudential reviews in 2019–20 and has seen an improvement and greater awareness among credit unions of the importance of maintaining rigorous governance and risk management in all areas of risk.[84]

75 Evidence of C. Elgar, Transcript, January 15, 2021, p 52.

76 Ibid, p 50.

77 Exhibit 419, Memorandum of Understanding between the Financial Transactions and Reports Analysis Centre of Canada and the Financial Institutions Commission (January 9, 2005), p 2.

78 Evidence of C. Elgar, Transcript, January 15, 2021, pp 49–50, 52–53, 57, 77–78.

79 Ibid, p 50.

80 For an example of a report presented by FINTRAC to FICOM for the 2017–18 year, see Exhibit 420, FINTRAC, Reporting Statistics Updates: Fiscal Year 2017–2018, Presented to FICOM.

81 Evidence of C. Elgar, Transcript, January 15, 2021, p 61.

82 Exhibit 420, FINTRAC, Reporting Statistics Updates: Fiscal Year 2017–2018, Presented to FICOM, slide 3; Exhibit 421, FINTRAC Report on Compliance Examinations of Credit Unions in 2019/2020, p 1; Evidence of C. Elgar, Transcript, January 15, 2021, pp 74–76.

83 Exhibit 420, FINTRAC, Reporting Statistics Updates: Fiscal Year 2017–2018, Presented to FICOM, slide 12.

84 Evidence of C. Elgar, Transcript, January 15, 2021, pp 63–64.

Regulation by OSFI

The Office of the Superintendent of Financial Institutions regulates and supervises over 400 federally regulated institutions and 1,200 pension plans. In a similar way to BCFSA, it seeks to ensure that these institutions are in sound financial condition and are complying with relevant laws. The federal institutions it regulates include all banks, as well as federally incorporated or registered trusts and loan companies, insurance companies, co-operative credit associations, fraternal benefit societies, and private pension plans. It considers matters such as the institution's financial condition, material risk, and quality of its governance, risk management, and compliance.[85]

Following a consultation with industry and discussions with FINTRAC around eliminating duplication and redundancy, OSFI rescinded Guideline B-8 on July 26, 2021.[86] This change appears to be in response to findings by the Financial Action Task Force's 2016 mutual evaluation of Canada, which noted duplication in efforts between FINTRAC and OSFI and a need to coordinate resources and expertise more effectively.[87]

Money Laundering Risks Facing Financial Institutions

As I noted at the beginning of this chapter, the money laundering risks facing financial institutions are in many ways common sense. Financial institutions are gatekeepers to the financial system, and money whose source is or appears to be a financial institution receives a veneer of legitimacy. It can easily be assumed that the goal of many money launderers is to have their funds pass through a financial institution at some stage.

Canada's 2015 national risk assessment noted that banks hold over 60 percent of the financial sector's assets, and the six largest domestic banks (BMO, Scotiabank, CIBC, RBC, TD, and National Bank) hold 93 percent of those assets.[88] As of November 2014, credit unions and *caisses populaires* held over $320 billion in assets.[89] The assessment rated domestic banks as having a "very high" vulnerability rating, while credit unions, *caisses populaires*, and foreign bank branches and subsidiaries were rated "high."[90] FINTRAC has similarly identified banks, credit unions, *caisses populaires*, and money services businesses as high risk.[91]

85 Office of the Superintendent of Financial Institutions, "About Us," online: https://www.osfi-bsif.gc.ca/Eng/osfi-bsif/Pages/default.aspx.

86 Office of the Superintendent of Financial Institutions, "OSFI's Activities on Anti–Money Laundering/Anti-Terrorist Financing (AML/ATF) Supervision" (May 17, 2021), online: https://www.osfi-bsif.gc.ca/Eng/fi-if/in-ai/Pages/aml-let.aspx.

87 Exhibit 4, Overview Report: Financial Action Task Force, Appendix N, FATF, *Anti–Money Laundering and Counter-Terrorist Financing Measures – Canada, Fourth Round Mutual Evaluation Report* (Paris: FATF, 2016), pp 4, 7, 90, 94.

88 Exhibit 3, Overview Report: Documents Created by Canada, Appendix B, Department of Finance, *Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada 2015* (Ottawa: 2015), p 34.

89 Ibid, p 35.

90 Ibid, p 32.

91 Exhibit 4, Overview Report: Financial Action Task Force, Appendix N, FATF, *Anti–Money Laundering and Counter-Terrorist Financing Measures – Canada, Fourth Round Mutual Evaluation Report* (Paris: FATF, 2016), p 90.

Domestic banks were rated the most vulnerable, primarily due to the size of the six largest ones. The national risk assessment explained that those banks have very significant transaction volumes, asset holdings, and scope of operations (both domestic and international). They offer a large number of vulnerable products and services to a large client base, including a significant number of high-risk clients and businesses. Services can be provided both face-to-face and remotely, thereby varying the degree of anonymity and complexity. Further, there were opportunities to use third parties and gatekeepers, including accountants and lawyers, to undertake transactions.[92]

Similar concerns were raised for credit unions, *caisses populaires*, foreign bank branches and subsidiaries, and trust and loan companies. The assessment also noted that some credit unions and *caisses populaires* operate in more remote Canadian locations that may attract high crime and corruption activities, as well as transient workers sending remittances to countries that may have high money laundering or terrorist financing risks.[93]

The national risk assessment identified a number of activities undertaken by deposit-taking financial institutions that are vulnerable to the placement and layering stages of money laundering, including the use of personal and business domestic accounts; domestic and international wire transfers; currency exchanges; and monetary instruments such as bank drafts, money orders, and cheques. The main money laundering techniques used to exploit these products and services were said to include the following:

- Structuring of cash deposits or withdrawals and smurfing (multiple deposits of cash by various individuals and low-value monetary instruments purchased from various banks and [money services businesses]);
- Rapid movement of funds between personal and/or business deposit accounts within the same financial institution or across multiple financial institutions;
- Use of nominees (individuals and businesses);
- Large deposits of cash and monetary instruments followed by the purchase of bank drafts or [electronic funds transfers] to foreign individuals;
- Exchanges of foreign currencies for Canadian currency and vice versa;
- Refining (i.e., converting large cash amounts from smaller to larger bills); and
- Non-face-to-face deposits (i.e., night deposits, armoured cars).[94]

92 Exhibit 3, Overview Report: Documents Created by Canada, Appendix B, Department of Finance, *Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada 2015* (Ottawa: 2015), p 37.

93 Ibid, pp 37–38.

94 Ibid, p 44.

The Financial Action Task Force's *Guidance for a Risk-Based Approach: The Banking Sector* similarly identifies a number of financial products and services associated with money laundering and terrorist financing risks. First, certain retail banking activities – providing accounts, loans, and savings products – pose risks insofar as they involve the provision of services to cash-intensive businesses, a large volume of transactions, high-value transactions, and diverse services.[95] Second, providing wealth management services may entail risks due to a culture of confidentiality, difficulty in identifying beneficial owners, concealment through the use of offshore trusts, banking secrecy, complexity of financial services and products, politically exposed persons, high-value transactions, and involvement of multiple jurisdictions.[96] Third, investment banking services may be misused for layering and integration and can raise risks due to the transfer of assets between parties in exchange for cash or other assets and because of the global nature of markets.[97] Finally, correspondent banking services may involve high-value transactions, limited information about the remitter or source of funds, and possible involvement of politically exposed persons.[98]

The Financial Action Task Force's 2016 mutual evaluation of Canada concluded that financial institutions have a "good understanding of their risks and obligations, and generally apply adequate mitigating measures."[99] While noting a number of positive aspects of financial institutions' anti–money laundering programs, the evaluation noted some deficiencies relating to the identification of politically exposed persons and beneficial owners.[100] Some smaller financial institutions also displayed a weaker understanding of money laundering and terrorist financing measures, had weaker record-keeping measures, and regarded anti–money laundering and counterterrorist financing measures as a burden.[101] A "priority action" was to ensure that financial institutions comply with beneficial ownership requirements.[102]

In the 2018–19 and 2019–20 fiscal years, FINTRAC conducted 92 compliance examinations of financial entities across Canada.[103] FINTRAC's report to the Minister of Finance on the 2019–20 fiscal year notes that examinations of banks require significantly more resources in terms of hours dedicated by regional compliance officers than other sectors.[104] Further, FINTRAC and OSFI were in the process of streamlining the

95 Ibid, pp 17–18.

96 Ibid.

97 Ibid.

98 Ibid.

99 Exhibit 4, Overview Report: Financial Action Task Force, Appendix N, FATF, *Anti–Money Laundering and Counter-Terrorist Financing Measures – Canada, Fourth Round Mutual Evaluation Report* (Paris: FATF, 2016), pp 4, 7, 78.

100 Ibid, pp 7, 78–79, 83.

101 Ibid, pp 79, 83.

102 Ibid, p 9.

103 Exhibit 629, FINTRAC Report to the Minister of Finance on Compliance and Related Activities (September 30, 2019), p 17; Exhibit 1021, Overview Report: Miscellaneous Documents, Appendix 15, FINTRAC Report to the Minister of Finance on Compliance and Related Activities (September 30, 2020), p 16.

104 Exhibit 1021, Overview Report: Miscellaneous Documents, Appendix 15, FINTRAC Report to the Minister of Finance on Compliance and Related Activities (September 30, 2020), p 15.

supervision of the banking sector's anti–money laundering and counterterrorist financing compliance, with FINTRAC set to become the sole federal regulator in this regard on April 1, 2021.[105] FINTRAC's examinations often identify a lack of awareness or consistent application of anti–money laundering and counterterrorist financing policies, procedures, and training within bank operations.[106] However, the 2019–20 examinations found that financial institutions are investing significant resources into their anti–money laundering and counterterrorist financing programs.[107]

Anti–Money Laundering Measures in Banks and Credit Unions

Banks and credit unions recognize the risks inherent in their work and dedicate significant resources to their anti–money laundering programs. In what follows, I discuss those programs and key challenges faced by financial institutions.

Compliance Programs at Credit Unions

I heard evidence from the chief anti–money laundering officers at three BC credit unions: Erin Tolfo of Coast Capital Savings, Ezekiel Chhoa of BlueShore Financial, and Lindzee Herring of First West Credit Union. Chief anti–money laundering officers are responsible for overseeing the anti–money laundering programs at financial institutions. They report to the board of directors and other senior management. As Ms. Tolfo put it, they act as "a checkpoint and a challenge point in order to ensure that the right steps are taken to test the controls that we have in place, and to make sure that training and information is cascaded throughout the organization."[108]

The anti–money laundering teams at the three institutions are set up differently. However, they all essentially involve an independent team looking for specific alerts and escalating issues as necessary.[109] According to the BC credit union witnesses, credit unions recognize their role in helping to support the national and international fight against money laundering and devote considerable efforts to fulfilling their obligations under the *PCMLTFA*. They indicate that credit unions take care to identify transactions meeting the reporting thresholds and report to FINTRAC, as well as law enforcement, where appropriate.[110] This is described as an "enterprise-wide effort" to ensure that staff at different levels are able to identify suspicious behaviour and ensure that the institution's obligations are fulfilled,[111] although much of the reporting

105 Ibid, p 18.

106 Ibid.

107 Ibid, p 19.

108 Evidence of E. Tolfo, Transcript, January 19, 2021, pp 11–12.

109 Ibid, p 13; Evidence of E. Chhoa, Transcript, January 19, 2021, pp 13–14; Evidence of L. Herring, Transcript, January 19, 2021, p 15.

110 Evidence of E. Tolfo, Transcript, January 19, 2021, pp 7–9.

111 Ibid, pp 8–9.

required under the *PCMLTFA* is done through automated systems.[112] Credit unions also leverage FINTRAC guidance as well as information from industry associations and other financial institutions in order to stay current on key changes and information.[113]

Due to the relative size of some credit unions and other financial institutions, a number of credit unions face challenges in implementing anti–money laundering programs. Certain fixed costs must be borne by a financial institution regardless of its size, such as the cost of anti–money laundering software.[114] Further, smaller credit unions may be unable to have staff dedicated solely to anti–money laundering activities; rather, staff tend to "wear a number of different hats," unlike larger institutions that can afford to have potentially hundreds of staff members dedicated to anti–money laundering alone.[115] Indeed, at some credit unions, the chief anti–money laundering officer is also the privacy officer, which can pose challenges. As Mr. Chhoa explained:

> [W]hen I wear a privacy hat, there are times when … I simply cannot share a piece of information even though from a money laundering perspective I may say "hey, I want to share that," but from a privacy perspective, you just cannot. And so it is a delicate balance and it's something [for which] I think increased clarity in legislation would be very helpful for the credit union system.[116]

Credit unions may also have difficulty training junior staff to focus on anti–money laundering because they need to seek out individuals who have the breadth of knowledge and experience allowing them to handle not only anti–money laundering but other responsibilities.[117]

Other difficulties arise in terms of access to anti–money laundering services. For example, larger financial institutions can avail themselves of offshore services, while smaller ones may be unable to do so.[118] In this regard, the services provided by Central 1 are very helpful for smaller credit unions. However, "even though the smaller credit unions have outsourced the activity, they cannot outsource the responsibility … the responsibility still rests on a very small credit union to ensure compliance regardless of who performs the activity."[119] Conversely, one potential advantage for credit unions is that they tend to be more "deeply rooted in [their] communities" than bigger banks, allowing for the kind of "personal connection with their frontline" staff that a bigger bank may not have.[120]

112 Evidence of E. Chhoa, Transcript, January 19, 2021, p 31.

113 Ibid, p 10.

114 Ibid, p 37.

115 Ibid.

116 Ibid, p 30. Sometimes there may be a simple solution, such as asking a client for consent, but not always: ibid, pp 46–47.

117 Ibid, p 38.

118 Ibid, pp 37–38.

119 Ibid, pp 38–39.

120 Evidence of L. Herring, Transcript, January 19, 2021, p 40.

Collaboration between credit unions and FINTRAC is largely one way, in the sense that credit unions report to FINTRAC but do not receive follow-up on those reports. However, FINTRAC does provide feedback through compliance exams and dialogue with industry.[121] Credit unions may also find out about reports they have filed if an investigation is started and a production order is sought.[122] Credit unions have a designated western Canada contact at FINTRAC for general questions.[123] They also have a dedicated RCMP email address where they can forward suspicious transaction reports directly; however, there is no dedicated person at the RCMP to whom they can provide concerns, which, it should be noted, is unlike the situation with respect to fraud.[124] Indeed, most of the interactions between credit unions and law enforcement relate to fraud rather than money laundering. Mr. Chhoa explained:

> [M]oney laundering … is a very difficult crime to prove … [W]e are not law enforcement … our job is primarily reporting the data and ensuring that the data gets into the hands of the people who are in a position to investigate. So … we don't communicate with law enforcement saying "hey, look, we believe there's money laundering," because … quite frankly, most of the time it's "suspicion" versus "we truly believe there is a crime here."[125]

Ms. Herring testified that credit unions are "passionate about information sharing." They share information with law enforcement, the International Association of Financial Crime Investigators, the Bank Crime Prevention and Investigation Framework, and the Credit Union Office of Crime Prevention and Investigation.[126] She explained:

> [T]hese are actually mechanisms for us to communicate between investigators, between credit union to credit union, and it's in a formal way to actually provide disclosures … [Y]ou have to have evidence, you have to have reasonableness to disclose information, but it is a process and it is something that between banks and credit unions can be a challenge as well. But definitely the avenues are there to be used. I think they're under-utilized. They do not specifically state "just for fraud"; they do say "financial crime." However, they have been primarily used for fraud. So there are some channels and mechanisms in place for financial institutions to do better.[127]

Ms. Herring continued that it would be useful from her perspective for credit unions to be able to avail themselves of a "safe harbour" provision.[128] As I elaborate later in this chapter, such a provision would essentially create an exception under relevant privacy

121 Evidence of E. Chhoa, Transcript, January 19, 2021, pp 33–35; Evidence of L. Herring, Transcript, January 19, 2021, p 36.

122 Evidence of E. Chhoa, Transcript, January 19, 2021, p 19.

123 Evidence of L. Herring, Transcript, January 19, 2021, p 36.

124 Evidence of E. Tolfo and E. Chhoa, Transcript, January 29, 2021, p 19; Evidence of L. Herring, Transcript, January 19, 2021, pp 20–21.

125 Evidence of E. Chhoa, Transcript, January 19, 2021, pp 21–22.

126 Evidence of L. Herring, Transcript, January 19, 2021, pp 24–25.

127 Ibid, p 25.

128 Ibid, pp 25–26.

legislation, enabling institutions to share information relating to money laundering with one another without fear of civil liability arising from the potential for intrusions on personal privacy.

The panellists identified some areas that are seen as higher risk for credit unions to engage in. Each credit union and financial institution conducts its own assessment of risk against its capabilities to meet its regulatory requirements. Some evolving business areas and risks can therefore be seen as challenging to have as clients. For example, money services businesses have minimal regulation and are complex because they essentially embed one financial institution with another – conducting their own transactions, but relying on credit unions to process them – which raises the question of which institution is responsible for what obligation.[129] Similarly, cash-based businesses are inherently high risk. This does not mean that financial institutions will not do business with them; rather, they will apply increased scrutiny, which in turn requires more resources and increases the regulatory burden.[130] The risk profile of certain businesses may also change: for example, the cannabis industry has gone from being illicit to regulated, which allows financial institutions to place some reliance on government infrastructure and regulation when determining their risk tolerance.[131]

Compliance Programs at Banks

As I explained above, I heard from the chief anti–money laundering officers at HSBC, Scotiabank, and RBC in an *in camera* hearing. Broadly speaking, they discussed the anti–money laundering programs at their banks, risks they have observed, and other topics. In this section I set out some general observations from that panel, without revealing any of the details that were protected by the *in camera* nature of the testimony. I have relied on the witnesses' testimony from the *in camera* panel, along with one sealed exhibit, Exhibit 457, a detailed submission made by the banks to outline a typical Canadian bank's anti–money laundering and counterterrorist financing program.

Large banks in this country invest a great deal into their anti–money laundering programs. The witnesses on the banks' CAMLO panel described having robust anti–money laundering programs and practices; ensuring their teams are educated about the risks; and being committed to revisiting their anti–money laundering programs to address new risks and typologies. Their programs involve various client identification mechanisms and methods for the ongoing monitoring of business relationships. They also have good systems in place for investigating suspicious activity and an awareness of the guidance they obtain from FINTRAC, the Financial Action Task Force, and others. They are involved in public-private partnerships (discussed further below) and find them useful.

129 Evidence of E. Chhoa, Transcript, January 19, 2021, p 44.

130 Evidence of E. Tolfo, Transcript, January 19, 2021, pp 42–43.

131 Ibid, pp 41–42.

There are critics who are sharply critical of how banks address money laundering activity, both abroad and in Canada. Given the constraints on this Inquiry process, as well as the federal nature of much of the banking domain, I do not purport to settle those controversies. I can say, based on the evidence I have received, of a general character as noted above, that I have no strong reason to doubt that the large national banks understand their role and responsibility in the anti–money laundering regime.

Information Sharing

The need for strong information-sharing pathways was a theme that permeated the Commission's hearings. I address this subject in detail in Chapter 7, including the differences between the sharing of *tactical* information (which relates to specific individuals or entities) and of *strategic* information (which focuses on typologies and general indicators of suspicion).[132] In that chapter, I also discuss concerns that have been raised by participants, witnesses, and others about the propriety and constitutionality of sharing specific tactical information, as well as the need for clear frameworks governing information-sharing arrangements. My focus in this section is on information sharing as it affects financial institutions – their ability to share information with government bodies and with each other.

Public-Private Partnerships

Public-private information-sharing partnerships are arrangements that allow public and private entities to share information relating to the discovery and detection of money laundering, terrorist financing, and broader economic crime.[133] As Nicholas Maxwell, a leading expert on public-private information-sharing partnerships, explained, the Financial Action Task Force considers effective information sharing to be the "cornerstone" of a well-functioning anti–money laundering framework.[134] The framework set out by the Financial Action Task Force

> really puts the private sector as the leading edge of the detection of money laundering. [I]t's up to the private sector to spot suspicions of money laundering and terrorist financing within their business [and] client base and to report that through to public agencies through to a dedicated financial intelligence unit.[135]

Because the regime also places emphasis on prevention, another goal of information sharing is to prevent illicit flows from accessing the financial system.[136]

132 Evidence of N. Maxwell, Transcript, January 14, 2021, pp 7–10; Exhibit 411, Nicholas Maxwell, Future of Financial Intelligence Sharing Briefing Paper – Canada in Context (January 4, 2021, updated December 11, 2021), p 18.

133 Evidence of N. Maxwell, Transcript, January 14, 2021, pp 6–7.

134 Ibid, pp 12–13.

135 Ibid, p 13.

136 Ibid, pp 13–14.

As I expand in Chapter 7, experts generally support increased collaboration between the public and private sector. Mr. Maxwell testified that there had been significant growth in the use of public-private partnerships in the five years preceding his testimony.[137] He concludes in a report prepared for the Commission that Canada has made insufficient use of public-private financial information sharing to detect money laundering.[138] However, while public-private information-sharing arrangements are common in other countries, they have posed difficulties in Canada. This is due in part to legal uncertainties and constraints, as participants have concerns about what information can properly be shared in light of Canadian privacy legislation and constitutional requirements.[139]

Project Athena is an example of a partnership that was in large part successful. It also illustrates, however, that lack of engagement by members of a partnership can slow its progress and even lessen its effectiveness. I describe Project Athena in detail in Chapter 39 and address some concerns about the propriety of the information-sharing arrangement it used in Chapter 7. Here, however, my focus is on the involvement of financial institutions in the initiative. In what follows, I describe the participation of the six major financial institutions and some lessons learned about ensuring future public-private partnerships are successful. In particular, the story of Project Athena offers two main lessons for financial institutions:

- they must be engaged, responsive, and open to creative solutions; and
- they must be represented by individuals who have the authority to implement such solutions in a timely manner.

A precursor to the Counter-Illicit Finance Alliance of British Columbia, Project Athena was a public-private partnership between the Combined Forces Special Enforcement Unit (CFSEU, a policing unit), financial institutions, the BC Lottery Corporation, and other stakeholders. Following Peter German's interim recommendation that gaming service providers complete a source-of-funds declaration whenever they received cash deposits or bearer bonds in excess of $10,000,[140] it became more difficult to launder cash through casinos. As a result, criminals turned to other methods, including bank drafts. CFSEU had concerns about the anonymity and transferability of bank drafts. Most were anonymous in the sense that they did not include the name of the purchaser or the account number from which the funds were sourced. The concern was that the absence of this information made it easier for bank drafts to be given to casino patrons who were not themselves the account holders, which could further a money laundering scheme.[141]

137 Ibid, p 7.

138 Exhibit 411, Nicholas Maxwell, Future of Financial Intelligence Sharing Briefing Paper – Canada in Context (January 4, 2021, updated December 11, 2021), p 9.

139 Evidence of N. Maxwell, Transcript, January 14, 2021, pp 30–31.

140 Exhibit 832, Peter M. German, *Dirty Money: An Independent Review of Money Laundering in Lower Mainland Casinos Conducted for the Attorney General of British Columbia* (March 31, 2018), p 244.

141 Evidence of B. Robinson, Transcript, April 14, 2021, pp 32–35, 48–49.

In March and April 2018, CFSEU analyzed all the bank drafts received at BC casinos in January and February of that year. It contacted the financial institutions that issued those bank drafts to determine whether the person presenting the draft at the casino held an account with that financial institution. That analysis revealed that most casino patrons did have an account at the issuing financial institution; however, it also disclosed a number of discrepancies in the source-of-funds declarations completed by casino patrons when they made buy-ins at BC casinos.[142]

In May 2018, CFSEU convened a meeting with financial institutions (including HSBC, BMO, Scotiabank, RBC, TD, and CIBC), the BC Lottery Corporation, and the provincial Gaming Policy and Enforcement Branch to convey its concerns about the use of bank drafts. One of the solutions proposed at that meeting was to put the purchaser's name on the front of the bank draft in order to reduce anonymity.[143] Reporting entities were also asked to include the words "Project Athena" on certain suspicious transaction reports made to FINTRAC to streamline the process.[144]

During an October 2018 meeting, participants discussed the exchange of *tactical* information relating to the exploitation of bank drafts (that is, information about specific customers and drafts). A process was developed by which tactical information could be shared between the BC Lottery Corporation, CFSEU, financial institutions, and FINTRAC. Part of this process involved CFSEU analyzing information it received from the BC Lottery Corporation about the suspicious use of bank drafts at BC casinos and seeking information from financial institutions as to whether the individual in possession of the bank draft held an account with their institution.[145]

I discuss the benefits of this information-sharing system further in Chapter 39. One notable benefit was the fact that all parties were able to streamline their processes and focus on transactions that were truly suspicious. It also allowed reporting entities to flag reports in a way that ensured that FINTRAC could bring them to the attention of the proper law enforcement agency – when the threshold for disclosure was met under the *PCMLTFA*.

Even before the October 2018 meeting, CFSEU had begun to provide tactical information to financial institutions. A report sent by then-Sergeant Melanie Paddon of CFSEU to TD on August 14, 2018, is illustrative. It sets out the following information for the month of June 2018:

- the total number of bank drafts purchased from all financial institutions that were tendered at BC casinos that month;
- the number of those bank drafts that were issued by TD;

142 Ibid, pp 44–46, 50; Exhibit 839, Project Athena and CIFA-BC Presentation, slide 10.

143 Evidence of B. Robinson, Transcript, April 14, 2021, pp 51–52; Exhibit 840, Project Athena Stakeholders Meeting October 24, 2018, slide 9.

144 Evidence of B. Robinson, Transcript, April 14, 2021, pp 51–52, 161–62.

145 Ibid, p 56.

- the number of patrons who tendered three or more bank drafts from all financial institutions at BC casinos, and of those patrons, the number using drafts from multiple banks; and
- the number of patrons who bought in at BC casinos with bank drafts purchased from TD, and a list of patrons identified as using drafts from multiple banks or with a high volume of bank drafts solely from TD.[146]

TD, along with the other participating financial institutions, received this information from CFSEU on a monthly basis. From the email correspondence, it appears that TD began receiving these monthly updates in June 2018 and continued to do so until June 2019 (providing information that, in total, covered a period from March 2018 to April 2019).[147]

In providing this information to financial institutions, CFSEU asked them to:

- consider the information and, where appropriate, carry out an internal review and file suspicious transaction reports with FINTRAC; and
- implement changes to their internal practices in order to add the purchaser's name to all bank drafts issued by the financial institution.[148]

Sergeants Ben Robinson and Paddon emphasized that it was left to the discretion of the financial institution to determine what to do with the information; it was a strictly voluntary process, and CFSEU did not direct financial institutions to investigate the information or to file suspicious transaction reports. Further, any reports filed with FINTRAC would be disclosed to law enforcement only if FINTRAC determined that the threshold to do so under the *PCMLTFA* was met.[149] However, other witnesses appeared to feel that there was more of an *expectation* that financial institutions would investigate the information and file suspicious transaction reports when warranted.[150]

While I elaborate on constitutional and privacy law concerns associated with tactical information sharing in Chapter 7, I note for present purposes that the request to make a change to bank drafts – which was separate from the disclosure of patron names – did not involve *tactical* information sharing. In other words, it did not involve any information sharing about particular clients of financial institutions. Rather, this was purely *strategic*

146 Exhibit 460, Email from Melanie Paddon re Project Athena June 2018, August 14, 2018 (redacted). See also Exhibit 459, Email from Melanie Paddon to Pierre McConnell re Project Athena, December 3, 2018, p 4; and Exhibit 463, Email from Melanie Paddon re Project Athena, Jan 2019, March 21, 2019 (redacted), p 1.

147 Exhibit 460, Email from Melanie Paddon re Project Athena June 2018, August 14, 2018 (redacted), p 1 (referring to an email sent on June 27, 2018); Evidence of M. Bowman, Transcript, January 20, 2021, p 92; Exhibit 466, Email from Melanie Paddon to Anna Gabriele, June 27, 2019, pp 2–3.

148 Evidence of A. Gabriele, Transcript, January 20, 2021, pp 10–13; Evidence of B. Robinson, Transcript, April 14, 2021, pp 53–54.

149 Evidence of B. Robinson, Transcript, April 14, 2021, pp 53–55, 154–55, 158–59, 161–62; Evidence of M. Paddon, Transcript, April 14, 2021, pp 55, 155, 159–60.

150 Evidence of A. Gabriele, Transcript, January 20, 2021, pp 10–11; Evidence of M. Bowman, Transcript, January 20, 2021, pp 125–26.

information sharing: law enforcement communicated a money laundering vulnerability to financial institutions and asked for a change in the institution's processes to address the vulnerability. As such, the constitutional and privacy law concerns do not arise in relation to the request to make changes to bank drafts.

As time went on, several banks demonstrated commendable engagement with the initiative. At a January 2019 meeting, a representative of HSBC indicated that the bank had started putting the purchaser's name on its bank drafts, and representatives of RBC provided an update on their reviews based on the tactical information provided by CFSEU.[151] An "action item" following that meeting was for financial institutions to add the purchaser's name to their bank drafts.[152]

At a meeting in April 2019, HSBC repeated that its tellers had started to write purchaser information on its drafts and noted that it was looking into a system to embed this information on its drafts. The meeting minutes indicate that this change "took no time to implement[;] all it took was communication to each bank staff."[153] BMO was also looking into a system to embed this information on its drafts. Scotiabank concluded that it did not distribute a high enough volume of drafts to justify the change. RBC tellers had started to write purchaser names on their drafts in May 2019, and the bank was looking into a long-term solution. CIBC's drafts already had the purchaser information embedded on them. Finally, TD indicated it "was looking to engage their new leadership and get their buy-in."[154]

As this discussion shows, most banks were engaged with Project Athena and took proactive actions in response to information being shared by CFSEU. Specifically, they agreed to actively participate in the project, to receive and make use of the information being shared, and to address the systemic vulnerabilities. In short, the initiative provided information to financial institutions that would allow them to identify potentially suspicious activity involving their clients, report it to FINTRAC where warranted, and make changes to their processes intended to address a money laundering vulnerability.

Unfortunately, not all banks were engaged to the same degree. As I expand below, TD did not participate at a level that would be reasonably expected given its particular circumstances. Throughout the project, TD was the largest source of bank drafts flagged as suspicious by CFSEU.[155] By May 2019, the executives of TD's anti–money laundering group were aware of this fact and that TD risked being out of step with its peers if it did not take action to reduce the anonymity of its drafts.[156] By July 2019, TD was one of only

151 Evidence of A. Gabriele, Transcript, January 20, 2021, pp 26–27; Exhibit 461, CFSEU-BC, Project Athena Stakeholders Meeting – Agenda, January 23, 2019.

152 Exhibit 462, Email from Ben Robinson re Project Athena Update, January 24, 2019 (redacted), p 1.

153 Exhibit 458, Meeting Minutes – Project Athena, April 24, 2019, p 3.

154 Ibid, p 4.

155 Evidence of A. Gabriele, Transcript, January 20, 2021, pp 31, 41–42; Evidence of M. Paddon, Transcript, April 14, 2021, pp 68–70.

156 Evidence of A. Gabriele, Transcript, January 20, 2021, pp 54–55.

two banks[157] not to have implemented either a manual solution (in which tellers wrote customer names on bank drafts) or an automated solution (in which the information was embedded on the drafts).[158] Despite the foregoing, TD did not make changes to its bank drafts until September 2020.[159] The change implemented at that time seems to have been prompted by the March 2020 inquiry by Commission counsel about TD's participation in Project Athena.[160]

I find it troubling that TD's changes to its bank drafts came over a year later than its peers. I emphasize at the outset that TD has put in place a variety of strong anti–money laundering measures and invests a great deal into its anti–money laundering program. The discussion that follows should not be taken as a critique of TD's anti–money laundering program generally. I also emphasize that Project Athena was a voluntary initiative and that aspects of it – particularly the fact that law enforcement was providing tactical information to banks – had not occurred in previous information-sharing arrangements. It is understandable that some banks, including TD, may have been uncomfortable with the sharing of tactical information in this way (see Chapter 7). However, it is fair to conclude that TD's delay in addressing the bank draft issue created a significant gap, given that other major banks had implemented changes to reduce anonymity by summer 2019. This in turn raised the possibility that TD could be exploited by criminals to launder significant sums of money through BC casinos.

I also note that Project Athena seems to have had difficulty engaging with others, including OSFI and the Canadian Banking Association, on the issue of bank draft anonymity.[161] These two institutions could presumably have provided valuable insight and assistance to the initiative, and possibly even required financial institutions to make changes to their drafts.

I heard testimony from two representatives of TD on its involvement in Project Athena: Michael Bowman, the chief anti–money laundering officer at TD, and Anna Gabriele, formerly a manager in TD's special investigations unit.[162] The evidence before me also includes transcripts of interviews conducted by Commission counsel with Mr. Bowman and with Caitlin Riddolls, the vice-president and head of anti–money laundering for Canadian bank invasion technology and shared services at TD, which were tendered during the evidentiary hearings.[163]

157 The other bank (Scotiabank) was not a significant source of suspicious bank drafts.

158 Exhibit 473, Caitlin Riddolls Interview, October 21, 2020, pp 29–30; Evidence of M. Paddon and B. Robinson, Transcript, April 14, 2021, p 67.

159 Evidence of M. Bowman, Transcript, January 20, 2021, pp 138–139; Evidence of A. Gabriele, Transcript, January 20, 2021, p 62.

160 Exhibit 478, Michael Bowman Interview, October 22, 2020, p 73.

161 Evidence of B. Robinson, Transcript, April 14, 2021, pp 59–61.

162 The special investigations unit is part of TD's financial intelligence unit. TD has two financial intelligence units (one Canadian and one American). These units (alongside other supporting units) form the global anti–money laundering operations team: Evidence of M. Bowman, Transcript, January 20, 2021, p 86.

163 Exhibit 478, Michael Bowman Interview, October 22, 2020; Exhibit 473, Caitlin Riddolls Interview, October 21, 2020.

TD began participating in Project Athena in early 2018. At that time, the bank was represented by a member of its global security and investigations team.[164] With time, responsibility for Project Athena shifted from the global security and investigations team to the financial intelligence unit.[165]

CFSEU began providing monthly reports to TD in June 2018.[166] In her August and September 2018 reports, Sergeant Paddon noted that TD had not yet addressed earlier reports on the March to June 2018 period.[167]

Ms. Riddolls stated that she became aware of Project Athena and the typology identified by it in December 2018 in a meeting with the "big six" banks, FINTRAC, and the RCMP.[168] She subsequently sent emails to Aaron Clark, the vice-president of Everyday Banking (the division responsible for deposit products and services including bank drafts), in December 2018 and May 2019. She inquired about TD's practice about including payor names on drafts and noted the typology identified by Project Athena, the fact that other banks were implementing changes to their drafts, and that "if [TD's] control frameworks were not similarly updated, there was the potential risk that we could be targeted by money launderers who wanted to leverage this typology."[169]

Ms. Riddolls did not receive a response to either email.[170] She then engaged with others at TD's Everyday Banking group to determine TD's current practice and consider the feasibility of a manual solution or an automated solution.[171] It was estimated that the cost of an automated solution would be around $1 million.[172] By July 2019, after consulting with her peers at other banks, Ms. Riddolls was aware that all but one of TD's peers (Scotiabank) had implemented either a manual or automated solution.[173]

At the April 2019 meeting of Project Athena, CFSEU had reviewed data from the beginning of the initiative in March 2018 until January 2019. Over that 11-month period, the number of drafts sold by each of the banks that were subsequently flagged as suspicious by CFSEU (because the casino patron tendering the draft used three or more

164 Evidence of M. Bowman, Transcript, January 20, 2021, p 92. The global security and investigations team is responsible for the physical security of banks. It is separate from the financial intelligence unit, which is responsible for anti–money laundering. The two teams used to have different reporting channels but now share a similar reporting structure: Evidence of M. Bowman, Transcript, January 20, 2021, pp 89–92.

165 Evidence of A. Gabriele, Transcript, January 20, 2021, p 5; Exhibit 459, Email from Alexandra Andreu re Project Athena casino patrons list Oct 2018, January 9, 2019 (redacted).

166 Evidence of M. Bowman, Transcript, January 20, 2021, p 92; Evidence of A. Gabriele, Transcript, January 20, 2021, p 18.

167 Exhibit 460, Email from Melanie Paddon re Project Athena – June 2018, August 14, 2018 (redacted), p 1; Exhibit 472, Email from M. Paddon to P. McConnell re Project Athena – Bank Drafts for July 2018, September 27, 2018 (redacted).

168 Exhibit 473, Caitlin Riddolls Interview, October 21, 2020, p 4.

169 Ibid, pp 6–10, 13.

170 Ibid, pp 7–8, 14.

171 Ibid, pp 16–17.

172 Ibid, p 21.

173 Ibid, p 30.

bank drafts in a single month, or used multiple drafts from different banks) ranged from 21 drafts purchased from the bank at the low end to 510 drafts from the bank at the high end.[174] Following that meeting, Ms. Gabriele asked a member of her team to compile and analyze the information that had been provided by CFSEU between March 2018 and January 2019. The analysis, which took a couple of days to complete, confirmed that a high volume of bank drafts was coming from TD – it was the bank from which the 510 bank drafts were purchased, and the value of these drafts totalled $26 million.[175] This was the first use that TD made of the intelligence it had been receiving every month from CFSEU since mid-2018; however, it was still only a preliminary review and compilation rather than an investigative use of the information.[176]

On May 13, 2019, Ms. Gabriele met with Amy Hellen, the bank's global head of anti–money laundering; Kevin Doherty, head of the Canadian financial intelligence unit; and John Hamers, a senior anti–money laundering manager at the financial intelligence unit and Ms. Gabriele's direct boss.[177] Ms. Gabriele prepared a slide deck, which identified the two aspects of Project Athena (the tactical information provided by CFSEU and the request to make changes to bank drafts), presented the findings of her team's preliminary analysis of the data, and noted the high volumes of TD drafts and the fact that all the big banks were participating. It also noted Ms. Gabriele's view that "if TD did not participate, I believed that we would have been the only financial institution" not to; however, she understood that "that was never on the table for discussion" because TD was going to participate.[178]

Ms. Gabriele made two recommendations: to add more resources to the team in order to start acting on the information from CFSEU, and to take action on the bank draft anonymity issue. In relation to the first recommendation, she asked for a team of four investigators and a manager.[179] She understood from the meeting that TD would be participating in Project Athena but needed to figure out its approach. She was directed to continue working on current regulatory priorities and demands until further meetings took place at the executive level. Ms. Gabriele did not receive direction to start with the "end-to-end reviews" of the intelligence being provided by CFSEU.[180]

In June 2019, Ms. Gabriele asked Mr. Doherty whether she should attend the upcoming meeting of Project Athena on July 24, 2019.[181] He responded that "no action [was] required on Project Athena at this time," noting that discussions were occurring among the financial intelligence unit and the Global Senior Executive Team about "the appropriate way to deal with initiatives like [Project] Athena."[182]

174 Exhibit 458, Meeting Minutes – Project Athena, April 24, 2019, p 2.

175 Evidence of A. Gabriele, Transcript, January 20, 2021, pp 31, 41–42; Evidence of M. Paddon, Transcript, April 14, 2021, pp 68–70.

176 Evidence of A. Gabriele, Transcript, January 20, 2021, pp 35, 50.

177 Ibid, pp 21, 50–51; Evidence of M. Bowman, Transcript, January 20, 2021, p 87.

178 Exhibit 464, TD – Project Athena – A Public/Private Partnership Presentation (undated) (redacted); Evidence of A. Gabriele, Transcript, January 20, 2021, pp 53–56.

179 Evidence of A. Gabriele, Transcript, January 20, 2021, pp 56–57.

180 Ibid, pp 55–59.

181 Exhibit 466, Email from Kevin Doherty re Project Athena, June 21, 2019 (redacted), pp 1–4.

182 Ibid, p 1; Evidence of A. Gabriele, January 20, 2021, pp 65–66.

On July 11, 2019, Mr. Doherty emailed Ms. Hellen advising that, in line with recent discussions, "I will be asking Anna [Gabriele] to stand down from attending the next session in Vancouver later this month" as they had not yet identified which team should be responsible for the project and nothing was being done with the data outputs. Ms. Hellen agreed with this approach.[183] Mr. Doherty later told Ms. Gabriele that they were "standing down on Athena for now" and would not be attending the July 2019 meeting.[184]

Mr. Bowman testified that he does not recall having any communications with Mr. Doherty about Project Athena, nor was he aware of any "stand down" order.[185] He believes there was a miscommunication that led to this decision, in which an inquiry he made about what his team members were engaged in was misinterpreted as a direction for Ms. Gabriele to stand down.[186] He also noted that the July 2019 Project Athena meeting was the only one that TD did not attend, as TD attended the November 2019 meeting.[187]

The July 2019 meeting minutes of Project Athena note that suspicious bank drafts in descending order of dollar value were coming from TD, BMO, CIBC, RBC, HSBC, and Scotiabank. In 2018, a total of 2,955 bank drafts / certified cheques going to BC casinos were received from 17 different financial institutions, for a total value of $151.9 million. Of those, 98 percent originated from the top six financial institutions, and the top two – TD and BMO – accounted for 66 percent of the dollar value amount or 63 percent of the count volume.[188]

By July 2019, it was clear that all but one of TD's peers (Scotiabank, which was not a significant source of drafts flagged by Project Athena) had implemented either a manual or automated solution to the bank draft issue.[189] However, TD determined that other regulatory changes and issues should be prioritized at that time and that the bank draft issue would be revisited as part of a larger anti–money laundering project that was set to be delivered in June 2021.[190] Indeed, some documents before me suggest that TD's involvement in Project Athena was put on hold due to "other operational priorities."[191] Mr. Bowman emphasized that the financial intelligence unit was "drained" at the

183 Exhibit 467, Email from Kevin Doherty to Amy Hellen re Project Athena, July 11, 2019. The Canadian banking direct channels team is part of the anti–money laundering team managed by Caitlin Riddolls: Exhibit 478, Michael Bowman Interview, October 22, 2020, p 45.

184 Exhibit 468, Message from Kevin Doherty to Anna Gabriele re Decision on TD's involvement with Project Athena, July 11, 2019.

185 Exhibit 478, Michael Bowman Interview, October 22, 2020, pp 20–23, 43–44; Evidence of M. Bowman, Transcript, January 20, 2021, pp 114–15.

186 Evidence of M. Bowman, Transcript, January 20, 2021, pp 114–15; Exhibit 478, Michael Bowman Interview, October 22, 2020, pp 20–23, 43–44.

187 Evidence of M. Bowman, Transcript, January 20, 2021, pp 114–16.

188 Exhibit 469, Project Athena Meeting Minutes, July 24, 2019, pp 4–5; Evidence of M. Paddon, Transcript, April 14, 2021, p 69.

189 Exhibit 473, Caitlin Riddolls Interview, October 21, 2020, p 30; Evidence of M. Paddon, Transcript, April 14, 2021, p 67.

190 Exhibit 473, Caitlin Riddolls Interview, October 21, 2020, pp 30–35.

191 Exhibit 471, Email from M. Crowley to A. Gabriele re Project Athena, December 30, 2019 (redacted), p 1.

time and "did not have a person to spare" to focus on Project Athena.[192] He noted that operational work, generating alerts, name matching, transaction monitoring, and filing of reports are "a huge amount of work with a tremendous focus on us around workforce management and around productivity, and that … was the number one priority."[193] Further, in his view, it would not have been appropriate to bring in contractors to participate on TD's behalf, as they would not have sufficient knowledge of the bank's systems, data infrastructure, technology, and the like.[194]

I fully appreciate that banks have significant mandatory anti–money laundering and other obligations. I accept, as Mr. Bowman noted, that complying with all these obligations requires a significant amount of time and effort. I also appreciate that banks were never *obligated* (by OSFI or the *PCMLTFA*) to make changes to their bank drafts. However, it is important to recognize that TD's peers operate under the same legal frameworks, and they were presumably dealing with similar pressures to comply with mandatory obligations while also participating in Project Athena. It is significant, in my view, that despite these pressures, TD's peers were able to implement a change to their bank drafts over a year before TD did so.

It appears that TD Bank did not make any investigative use of the information from CFSEU until December 2019.[195] Ms. Gabriele testified that "end-to-end reviews" of the data provided by Project Athena ultimately occurred between December 2019 and March 2020.[196]

In March 2020, Commission counsel contacted TD to learn about its participation in Project Athena. Following a request for information from the Commission, TD advised in June 2020 that "[w]hile there is no legal or regulatory requirement for TD to add purchaser identifying information on bank drafts, TD has determined that there are likewise no legal or regulatory restrictions against doing so." TD indicated that, given the potential practical benefits identified by Project Athena, it would be proceeding with the change and was "exploring a technology solution to print the name of the purchaser on each draft, which it would target to be deployed nationally." TD's letter indicates that, given other operational changes and challenges related to the COVID-19 pandemic, the plan was to deploy the new solution no later than June 2021.[197]

Mr. Bowman agreed that the Commission's contact with TD in March 2020 prompted renewed focus and attention on the bank draft issue.[198] TD subsequently confirmed that the request to initiate a change to TD's bank drafts was submitted in April 2020.

192 Evidence of M. Bowman, Transcript, January 20, 2021, p 118–119; Exhibit 478, Michael Bowman Interview, October 22, 2020, p 50.

193 Exhibit 478, Michael Bowman Interview, October 22, 2020, p 48.

194 Evidence of M. Bowman, Transcript, January 20, 2021, pp 117–21.

195 Evidence of A Gabriele, Transcript, January 20, 2021, p 78; Evidence of M. Bowman, Transcript, January 20, 2021, pp 104, 132, 138.

196 Evidence of A. Gabriele, Transcript, January 20, 2021, p 59.

197 Exhibit 475, Letter from Michael Bowman re Misuse of Bank Drafts, TD's Response, June 15, 2020, p 3.

198 Exhibit 478, Michael Bowman Interview, October 22, 2020, p 73.

In September 2020, TD implemented a change in all BC branches under which a customer's name would be manually written on a bank draft.[199] A national, automated solution was rolled out in September 2021.

Mr. Bowman and Ms. Riddolls emphasized that making a change to bank drafts — even a manual one — was not simple, as it required consultation with many departments.[200] They also explained that TD's general preference was for an automated solution on a national basis to reduce the risk of human error.[201] While I appreciate that TD had a preference for an automated solution, and that there are indeed benefits of adopting such a solution rather than a manual one, one does not preclude the other. Indeed, some of TD's peers chose to implement a temporary manual solution while they developed an automated solution. This approach seems to be a practical way of addressing a vulnerability promptly while developing a more long-term solution.

Mr. Bowman also expressed the view that the channels used at TD to become involved in Project Athena were not particularly effective. In particular, it was not ideal or typical that the anti–money laundering team at TD got involved through informal requests by the global security and investigations team.[202] He emphasized that Project Athena was a novel type of public-private partnership in that law enforcement provided actual intelligence to banks, and his impression from fellow chief anti–money laundering officers at other banks was that their corporate security and investigations units, rather than their anti–money laundering units, may have been involved.[203] He also expects that there were concerns at some levels of TD relating to the propriety of sharing information with the RCMP without a production order and the implications of privacy legislation.[204]

I accept that TD may have been uncertain about the propriety of the information sharing in Project Athena and indeed that others had similar concerns (see Chapter 7). However, I am troubled by TD's delay in implementing a change to its bank drafts (which did not involve tactical information sharing) to address a money laundering vulnerability

199 Evidence of M. Bowman, Transcript, January 20, 2021, pp 138–139.

200 They explained that such changes involve considerations including: how to respond to customer questions; how to escalate situations where a customer refuses to have their name on the draft; how to provide information to the financial intelligence unit; how to communicate information to employees who are students or part-time; and how to ensure proper oversight and controls exist to verify that the change is being made: Evidence of M. Bowman, Transcript, January 20, 2021, pp 140–42; Exhibit 478, Michael Bowman Interview, October 22, 2020, pp 65–66; Exhibit 473, Caitlin Riddolls Interview, October 21, 2020, pp 26, 54–55.

201 Exhibit 473, Caitlin Riddolls Interview, October 21, 2020, p 18; Exhibit 478, Michael Bowman Interview, October 22, 2020, p 66.

202 Exhibit 478, Michael Bowman Interview, October 22, 2020, pp 32–33; Evidence of M. Bowman, Transcript, January 20, 2021, p 105.

203 Evidence of M. Bowman, Transcript, January 20, 2021, pp 105–106, 123–127; Exhibit 478, Michael Bowman Interview, October 22, 2020, pp 32–33, 36–37.

204 Evidence of M. Bowman, Transcript, January 20, 2021, pp 122–23, 148–49. Indeed, at the October 2018 meeting, it appears that TD expressed some concerns early on about the implications of the *Privacy Act* and information sharing with police in the absence of a production order: Exhibit 476, Project Athena Stakeholders Meeting Minutes, October 24, 2018, p 1.

flagged by law enforcement. It appears that, as early as December 2018, the vice-president of Everyday Banking was advised of the Project Athena typology, the actions that other banks had taken to change their bank drafts, the potential for TD to be the sole bank among its peers not to do so, and the fact that failing to do so could make TD vulnerable for money laundering. Yet, no change was made to its bank drafts until September 2020. Further, this action appears to have been prompted by inquiries by Commission counsel, raising the question of whether it would have occurred otherwise.

This delay is surprising given that senior management in TD's anti–money laundering unit were aware by at least May 2019 that their bank was the single largest source of suspicious bank drafts being tendered at BC casinos, representing a sum of $26 million from March 2018 to January 2019 alone. Despite this information, a request for a five-person investigation team was declined, and it appears that TD determined it did not have a single person it could spare to analyze the data being provided by Project Athena. Instead, Ms. Gabriele was told to stand down from the initiative. Although this may have involved some miscommunication, I find it concerning that one of Canada's largest financial institutions was so delayed in addressing a vulnerability to bank drafts that had been identified by law enforcement. There were costs to these decisions, with millions of dollars of potentially suspicious funds entering BC casinos through TD bank drafts in the meantime.[205]

The story of Project Athena illustrates the need for all participants in public-private partnerships to be engaged, responsive, and willing to take concrete measures to address money laundering threats. Failing to do so can hinder the effectiveness of such partnerships and possibly enable continued criminal activity — this occurs when bad actors identify and then target institutions that are slower to implement changes. Further, it appears that the situation at TD was due, in part, to a failure to ensure that the correct department had carriage of the project. It is crucial that financial and other institutions have processes in place to allow the appropriate people to be advised of and involved in anti–money laundering initiatives.

Private-Private Information Sharing

A second category of information sharing relates to collaboration between financial institutions themselves, referred to as "private-private information sharing." Nicholas Maxwell, one of the world's leading experts on public-private financial information-sharing partnerships, expresses the view that there has been inadequate private-private information sharing to detect money laundering in Canada.[206] In particular, in recent years, there has been a push to implement a "safe harbour"

205 Sgt. Paddon agreed there was reason to think that money launderers began to target banks that did not have measures to address bank draft anonymity, although she noted there were also other reasons for that shift: Transcript, April 14, 2021, pp 70–71.

206 Exhibit 411, Nicholas Maxwell, Future of Financial Intelligence Sharing Briefing Paper – Canada in Context (January 4, 2021, updated December 11, 2021), p 9.

provision for money laundering. In a report prepared for the Commission, Barbara McIsaac, a lawyer with expertise in privacy law, described the concept as

> a provision in a statute or in a regulation or rule that specifies that certain conduct will not create liability if certain conditions are met. Generally, such a provision would exempt the entity that has shared the information from liability or censure by a regulator if it acted in good faith in doing so.[207]

Ms. McIsaac notes that a number of organizations, including the Canadian Bankers Association, have recommended that a safe harbour provision be adopted with respect to money laundering.[208] An example of a safe harbour provision can be found in section 314(b) of the US *Patriot Act*, which states that American financial institutions may

> share information with one another regarding individuals, entities, organizations, and countries suspected of possible terrorist or money laundering activities. A financial institution or association that transmits, receives, or shares such information for the purposes of identifying and reporting activities that may involve terrorist acts or money laundering activities *shall not be liable to any person under any law or regulation of the United States.* [Emphasis added.][209]

Mr. Maxwell's report explains that section 314(b) creates a voluntary program allowing reporting entities to share information for purposes of identifying and, where appropriate, reporting activities that may involve money laundering or terrorist financing.[210] According to the report, the number of institutions using the process in section 314(b) has nearly doubled between 2014 and 2018, and it has enabled US banks to "develop a more effective network intelligence picture of financial crime threats across participating entities."[211]

In Canada, the federal *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 (known as "*PIPEDA*") contains a kind of safe harbour provision in relation to fraud. Section 7(3)(d.2) states that an organization may disclose personal information with another organization where it is "reasonable for the purpose of detecting or suppressing fraud or of preventing fraud that is likely to be committed and it is reasonable to expect that the disclosure with the knowledge or consent of the individual would compromise the ability to prevent, detect or suppress the fraud." Notably, it refers

207 Exhibit 319, Barbara McIsaac Law, Report for the Cullen Commission on Privacy Laws and Information Sharing (November 17, 2020), pp 109–110.

208 Ibid.

209 *Uniting and Strengthening America By Providing Appropriate Tools Required To Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001*, 115 Stat 272, online: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107.pdf.

210 Exhibit 411, Nicholas Maxwell, Future of Financial Intelligence Sharing Briefing Paper – Canada in Context (January 4, 2021, updated December 11, 2021), p 24.

211 Ibid. He has observed that US banks now work together to flag transactions that will impact another bank, resolve certain risks, and ultimately report more efficiently to the financial intelligence unit: Evidence of N. Maxwell, Transcript, January 14, 2021, pp 102–103.

only to fraud; it does not encompass money laundering.[212] As a result, Mr. Maxwell took the view that there is "no legal gateway to share information between financial institutions for the prevention and suppression of money laundering and to support collaborative analytics between multiple financial institutions as there is for fraud."[213]

The issue may not be that straightforward, however. Ms. McIsaac expresses the view that, properly understood, provincial and federal privacy laws do not prevent the disclosure of personal information for the purposes of combatting money laundering. Rather, there is a strong *assumption* that they do. She concludes that "the principal way in which Canadian privacy laws may be detrimental to combatting money laundering is in their perception," noting that in the absence of clear guidance as to when information sharing is permitted, "potential information sharers will be more likely to err on the side of caution and default to the position of non-disclosure."[214] The problem is that, under provincial and federal legislation, the sharing of personal information is left to the discretion of the public or private entity (unless there is a legal requirement to provide it), and they can be penalized – through reputational harm or potential civil liability – if they are found to have shared information in a manner that does not comply with the legislation.[215] Ms. McIsaac believes that public and private entities must have a better understanding — and regulators and privacy commissioners must give clearer direction — of when information can be shared for the purposes of combatting money laundering.[216]

Despite the foregoing, Ms. McIsaac notes that a safe harbour provision would likely provide "more confidence" to public and private bodies that they will be protected from liability or censure by a regulator if they disclose personal information in good faith for the purposes of combatting money laundering.[217] She does not, however, express a view as to whether such a provision *should* be implemented.[218]

The chief anti–money laundering officers at the credit unions I heard from supported the development of a safe harbour provision. Ms. Herring testified that a provision similar to section 314(b) of the *Patriot Act* "would be ideal" in ensuring that credit unions have protection when sharing information in the context of complex investigations.[219] I also heard from Ms. Tolfo that there is a certain "conservatism" among credit unions given their heavy regulation:

212 Interestingly, the *Patriot Act* appears to have the opposite effect, providing an exception for money laundering and terrorist financing but not for fraud: Evidence of N. Maxwell, Transcript, January 14, 2021, p 102.

213 Evidence of N. Maxwell, Transcript, January 14, 2021, pp 100–101.

214 Exhibit 319, Barbara McIsaac Law, Report for the Cullen Commission on Privacy Laws and Information Sharing (November 17, 2020), pp 6, 109.

215 Ibid, p 109; Evidence of B. McIsaac, Transcript, December 3, 2020, p 81.

216 Evidence of B. McIsaac, Transcript, December 3, 2020, pp 30–31.

217 Exhibit 319, Barbara McIsaac Law, Report for the Cullen Commission on Privacy Laws and Information Sharing (November 17, 2020), p 7.

218 Evidence of B. McIsaac, Transcript, December 3, 2020, p 115.

219 Evidence of L. Herring, Transcript, January 19, 2021, pp 25–26.

> [T]he challenge that [financial institutions] have is we are so heavily regulated, it's complex. There are a lot of laws and regulations that often conflict with one another … I think that often tends to end up with individuals and institutions taking a really conservative approach around things … [For example, when] choosing to no longer work with a business or a consumer because you've decided that the risk is too high [that is, de-risking] … we are challenged in terms of not being able to share those details, specific details because of privacy law challenges … [T]here's a lot of validity to the privacy law area, but it also makes it is very challenging in that each institution is … on their own in the sense that they have to separately catch indicators around why someone may be coming to open up a new bank account having no idea that a financial institution down the street has just chosen to no longer do business with that person. So it's a fine balance in terms of not wanting to supply information that is going to enable the people who want to launder money to get smarter to be able to improve their ability versus making sure that we can freely share the information to try and support ultimately FINTRAC and law enforcement in using the data we provide.[220]

To similar effect, in evidence from the national bank CAMLOs, I heard that the lack of a safe harbour provision in Canada was a significant concern. The bank CAMLOs were supportive of such a provision, which would provide protection for banks that decide to share information while also ensuring a proper balance with privacy rights.

Mr. Maxwell noted that it is a common technique for money launderers to spread their accounts and money laundering activity across multiple institutions and that it can be difficult for individual institutions to understand what is occurring because they have only a small window into the criminal activity.[221] He opined that in the absence of a safe harbour provision, when one financial institution de-risks a client, that individual can enter the financial system at another point, learning along the way what tipped off the previous institution.[222] In his view, a safe harbour provision would "allo[w] a network to defeat a network":

> There [are] networks of organized crime who are fantastic at collaborating. They're fantastic at sharing information and they absolutely spread their risk across multiple reporting entities. [E]stablishing a clear legal basis for private/private sharing to detect money laundering between reporting entities … [would] support reporting entities and identify unknown threats to law enforcement, the criminality they are not already tracking, the suspects they don't already know about … It also should support a more effective preventive function, which is a huge pillar of what the system should be achieving.[223]

220 Evidence of E. Tolfo, Transcript, January 19, 2021, pp 26–28.

221 Evidence of N. Maxwell, Transcript, January 14, 2021, pp 101–102.

222 Ibid, pp 108–110; Exhibit 411, Nicholas Maxwell, Future of Financial Intelligence Sharing Briefing Paper – Canada in Context (January 4, 2021, updated December 11, 2021), p 25.

223 Ibid, pp 116–17.

From Mr. Maxwell's interviews with reporting entities, he observed that many were interested in safe harbour provisions and that, despite raising the issue with the federal government, "the response has so far been very negative towards that proposal. So interviewees were sceptical it would happen."[224]

The BC Civil Liberties Association strongly disagrees that a safe harbour provision is necessary. It submits that privacy legislation already allows for information sharing for the purposes of combatting money laundering in appropriate cases, referring to Ms. McIsaac's view that I noted above. It also points to findings by the Office of the Privacy Commissioner of Canada that entities already report excessive information to FINTRAC. In the BC Civil Liberties Association's view, any hesitancy about engaging in legal information sharing for the purposes of combatting money laundering can be addressed through education and clear direction from regulators. It further submits that any provisions that are adopted should be very carefully worded and tightly constrained to avoid undermining privacy rights any more than is absolutely necessary.[225]

I am persuaded that a safe harbour provision could have a meaningful impact on anti–money laundering activity in this province. The evidence before me suggests that both provincial and federal financial institutions are supportive of a safe harbour provision and consider the lack of such a provision to be problematic, particularly because a similar one exists for fraud-related information. It is also notable the Canadian Bankers Association expressed support for a safe harbour provision (with appropriate balances for privacy considerations) before the House of Commons' Standing Committee on Finance. The committee subsequently recommended in its 2018 report that the Government of Canada consider tabling legislation to introduce a safe harbour provision.[226] A response from the Government of Canada dated February 21, 2019, indicates that it agreed substantively with the recommendation to create a safe harbour provision and that it was "reviewing the Recommendations to enhance public-private and private-private information sharing options."[227]

It may be, as Ms. McIsaac and the BC Civil Liberties Association suggest, that a safe harbour provision for money laundering is not technically necessary because existing privacy legislation already permits sharing between financial institutions to combat money laundering. However, I am satisfied that financial institutions do not currently believe they are able to do so without facing liability in the absence of a specific safe harbour provision relating to money laundering. I am also satisfied that a formal safe harbour provision would provide needed comfort and clarity for financial institutions

224 Ibid, pp 105–106.

225 Closing submissions, BC Civil Liberties Association, paras 73–75; see also Evidence of B. McIsaac, Transcript, December 3, 2020, pp 117–18.

226 Exhibit 436, House of Commons, *Confronting Money Laundering and Terrorist Financing: Moving Canada Forward, Report of the Standing Committee on Finance* (November 2018), pp 41, 44 (Recommendation 18).

227 Standing Committee on Finance, Reports, 42nd Parliament, 1st Session (December 3, 2015–September 11, 2019), Government Response to Report 24, online: https://www.ourcommons.ca/Committees/en/FINA/Work?show=reports&parl=42&session=1.

when deciding to share information relating to money laundering and that a legislated measure would ensure that sufficient protections for privacy have been considered.

For a safe harbour provision to be most effective, it would need to apply to both provincially and federally regulated financial institutions. Ideally, the provision would be located in *PIPEDA* alongside the provision relating to fraud. As *PIPEDA* is a federal statute, I cannot make recommendations to the federal government on this point directly. However, given the importance of such a provision for British Columbia, I am of the view that the provincial government should urge the federal government to implement a safe harbour provision allowing financial institutions to share information related to potential money laundering activity.

Recommendation 48: I recommend that the Attorney General of British Columbia urge the appropriate federal minister to introduce amendments to the federal *Personal Information Protection and Electronic Documents Act*, providing for a "safe harbour provision" allowing financial institutions to share information related to potential money laundering activity.

Although a federal provision is important to enable federally regulated financial institutions to engage in this type of information sharing, the Province can equally make changes to allow provincially regulated financial institutions (notably credit unions) to do so. The Province should begin the process of introducing such a provision. This should be done in consultation with the Office of the Information and Privacy Commissioner to ensure that the proper protections for privacy are put in place. There should also be consultation with the appropriate federal minister to ensure that the safe harbour provisions are compatible.

Recommendation 49: I recommend that the Province introduce, in consultation with the Office of the Information and Privacy Commissioner, a safe harbour provision allowing provincially regulated financial institutions to share information related to potential money laundering activity.

Before concluding on safe harbour provisions, I note that a related issue is the concept of "keep open" requests. As Mr. Maxwell explained, keep open requests are

> a formal process whereby law enforcement can request an account be kept open and that's basically saying to the reporting entity, "keep open this account; we understand that you've identified suspicion, but we are interested in receiving the reports and we don't want you to close the account because it would harm our investigation."[228]

228 Evidence of N. Maxwell, Transcript, January 14, 2021, p 110.

Mr. Maxwell's interviews with stakeholders revealed that some believed FINTRAC would support financial institutions keeping an account open in such an instance, while others were concerned about a lack of clarity and the potential for civil action and other penalties if they complied with the request from law enforcement.[229] Mr. Maxwell's report to the Commission notes that currently, in the absence of a formal framework for "keep open" requests, a reporting entity may simply close an account when it receives information from law enforcement (such as a production order), which could undermine or disrupt the law enforcement investigation (closing an account prematurely or inexplicably tipping off a bad actor). [230] Mr. Maxwell concluded that the law of a legal framework for "keep open" requests and clear regulatory guidance is a challenge in Canada.[231]

Mr. Maxwell's report notes that FinCEN (the US equivalent to FINTRAC) has made guidance available since 2007 about keep open requests. The guidance states, among other things, that law enforcement agency requests to keep an account open must be in written form, last no longer than six months, and be recorded by the financial institution for five years. The process is voluntary, with the decision to maintain or close an account ultimately left to the financial institution. However, Mr. Maxwell notes that 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."[232]

It appears there may be room for improvement in the American regime in terms of ensuring sufficient legal and reputational protection for financial institutions assisting with keep open requests. Nonetheless, on the evidence before me, I am persuaded that a formal keep open regime similar to that in effect in the United States would be beneficial in British Columbia. It appears that such a regime would require federal legislative change. I therefore recommend that the BC Attorney General engage with his federal counterpart and other stakeholders to implement a formal keep open regime for financial institutions.

Recommendation 50: I recommend that the Attorney General of British Columbia engage with his federal counterpart and other stakeholders to implement a formal "keep open" regime for financial institutions in which they can, at the request of law enforcement, keep an account suspected of involvement in money laundering open in order to further a law enforcement investigation.

229 Ibid, pp 110–11.

230 Exhibit 411, Nicholas Maxwell, Future of Financial Intelligence Sharing Briefing Paper – Canada in Context (January 4, 2021, updated December 11, 2021), p 25.

231 Evidence of N. Maxwell, Transcript, January 14, 2021, p 111.

232 Exhibit 411, Nicholas Maxwell, Future of Financial Intelligence Sharing Briefing Paper – Canada in Context (January 4, 2021, updated December 11, 2021), p 26.

Conclusion

In this chapter, I have reviewed the money laundering risks facing financial institutions, both provincial and federal. Financial institutions play a key role in the anti–money laundering regime: as gatekeepers to the financial system, they likely encounter suspicious activity far more often than other reporting entities, and they are also well placed to observe suspicious activity involving those other entities when they are on the other side of transactions. Financial institutions are therefore important partners for law enforcement and FINTRAC alike.

Based on the evidence before me, financial institutions in this province are aware of the important role they play in combatting money laundering. The credit unions and banks I heard from have cogent anti–money laundering programs in place, although I cannot go the next step to evaluate the effectiveness in particular of federally regulated banks' programs. I am also of the view that the new BCFSA takes anti–money laundering seriously, though I have made recommendations above that will enhance its focus on the issue. Finally, I have outlined in this chapter the vital importance of information sharing, both between financial institutions and public authorities, as well as among financial institutions themselves. Information sharing certainly presents unique legal and constitutional difficulties that need to be addressed; however, it is clear that a constitutional information-sharing regime is key to the fight against money laundering.

Chapter 21
Money Services Businesses

Money services businesses, often referred to as MSBs, provide services that are similar, but not identical, to those offered by banks and credit unions. They are commonly known to handle money transfers and foreign currency exchange. Many tend to be much smaller than banks or credit unions, and their business structures less formal.

It is widely recognized that there are significant money laundering vulnerabilities associated with MSBs. They are frequently associated with professional money launderers and informal value transfer systems, which I discuss in more detail in Chapters 2, 3, and 37. Although MSBs are required to register with FINTRAC, many remain unregistered. This leaves FINTRAC and law enforcement in the dark about their activities. Further, given the risks inherent to MSBs, financial institutions often "de-risk" them – in other words, refuse to provide banking services to them – forcing some MSBs to operate underground and further hiding their activities from the authorities.

In this chapter, I begin by explaining what MSBs are and the regulatory framework applicable to them. I then examine the money laundering risks arising in this sector, which include risks associated with the business model as well as the consequences of de-risking and the existence of unregistered MSBs. I then discuss investigation challenges associated with MSBs. Finally, I consider the desirability of a provincial regulator for MSBs.

What are MSBs?

MSBs are non-bank persons or entities that provide transfer and exchange services. Clients use MSBs to exchange or transfer value and to purchase or redeem negotiable instruments. MSBs do *not*, however, accept deposits or make loans in the same way as

banks, credit unions, or trusts.[1] Under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, SC 2000, c 17 (*PCMLTFA*), MSBs include persons or entities that have a place of business in Canada and are engaged in the business of providing at least one of the following services:

- foreign exchange dealing (for example, converting USD into CAD);
- remitting funds or transmitting funds by any means or through any person, entity, or electronic funds transfer network;
- issuing or redeeming money orders, traveller's cheques, or other similar negotiable instruments except for cheques payable to a named person or entity; or
- dealing in virtual currencies.[2]

This definition includes alternative money remittance systems, such as the *hawala*, *hundi*, *chitti*, and *undiyal* systems (discussed further in Chapter 37).[3] The *PCMLTFA* also covers foreign MSBs, which are defined as persons or entities that do not have a place of business in Canada but provide one of the above services to persons or entities in Canada.[4]

A report prepared by FINTRAC in 2010 notes that many kinds of MSBs operate in Canada. These include large multinational companies with thousands of employees, branches, and franchised agents, as well as very small independent businesses with no employees and engaged in very low volumes of transactions.[5] Donna Achimov, deputy director and chief compliance officer at FINTRAC, testified that the vast majority of MSBs are "mom and pop" organizations located in a residence, convenience store, or the like.[6]

Although much of this chapter focuses on ways in which MSBs can be misused, it is important to emphasize that they have legitimate uses as well. Many MSBs provide convenient and affordable services to disadvantaged and vulnerable groups, including low-income, rural, and undocumented migrants. They also help individuals remit funds to family and friends in low- and middle-income countries.[7] Further, many new financial

1 Exhibit 441, FINTRAC, *Money Laundering and Terrorist Financing (ML/TF) Typologies and Trends for Canadian Money Services Businesses (MSBs)*, July 2010, p 2; Exhibit 440, BC Ministry of Finance, Money Services Businesses Public Consultation Paper (March 2020), p 3.

2 *Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations*, SOR/2002-184 [*PCMLTF Regulations*], s 1(2), "money services business"; *PCMLTFA*, s 5(h); Evidence of J. Iuso, Transcript, January 18, 2021, pp 7–8.

3 Exhibit 441, FINTRAC, *Money Laundering and Terrorist Financing (ML/TF) Typologies and Trends for Canadian Money Services Businesses (MSBs)*, July 2010, p 3.

4 *PCMLTF Regulations*, s 1(2), "foreign money services business"; *PCMLTFA*, s 5(h.1).

5 Exhibit 441, FINTRAC, *Money Laundering and Terrorist Financing (ML/TF) Typologies and Trends for Canadian Money Services Businesses (MSBs)*, July 2010, p 3.

6 Evidence of D. Achimov, Transcript, January 18, 2021, p 132.

7 Exhibit 440, BC Ministry of Finance, Money Services Businesses Public Consultation Paper (March 2020), p 4.

technology firms (sometimes referred to as "FinTech") are considered MSBs because they develop and apply new technologies to existing bank infrastructure.[8] The MSB definition in the *PCMLTFA* has also been expanded recently to encompass virtual asset service providers, which play an important role in the virtual asset space (see Chapter 35).

I heard evidence from Michael Cox, chief compliance officer and director of finance and risk management at the Vancouver Bullion and Currency Exchange, a large registered MSB in Greater Vancouver. The exchange provides services including transfers to individual and corporate clients, as well as currency exchange. It is also registered with FINTRAC as a dealer in precious metals and stones, which is not a common service provided by most MSBs. The exchange does not, however, provide cryptocurrency services. Mr. Cox testified that the exchange's main competitors are the big five Canadian banks. Significantly, at the request of its banking partners, the exchange does not provide services to other MSBs[9] – a point I return to later in this chapter.

The Canadian Money Services Business Association

The Canadian Money Services Business Association (CMSBA) was founded to provide advocacy, training, networking, and education for its members.[10] Importantly, it is not a regulator. Members of CMSBA include registered MSBs as well as partial and full associate members. The latter are not MSBs but offer services to them, such as consulting firms, law firms, and corporate entities. CMSBA verifies an MSB's registration with FINTRAC when the MSB signs up for membership.[11]

Joseph Iuso, executive director of CMSBA, testified that the association had between 80 and 100 registered members at the time of the hearing. Most are small and medium-sized MSBs, with the exception of the Vancouver Bullion and Currency Exchange, Ria Money Transfer (one of the world's largest money transfer services), and Canada Post. Mr. Iuso's experience is that larger MSBs are less inclined to join CMSBA than smaller ones, which, he believes, stems from a disinclination for larger MSBs to engage with smaller ones.[12]

Regulation of MSBs

At the time of writing, MSBs are not subject to provincial regulation in British Columbia. They do, however, have a variety of obligations under the *PCMLTFA*, and they are addressed by the Financial Action Task Force's 40 recommendations.

8 Ibid, p 5.

9 Evidence of M. Cox, Transcript, January 18, 2021, pp 11–13.

10 Evidence of J. Iuso, Transcript, January 18, 2021, pp 9–10, 74.

11 Ibid, pp 10–11, 68–69, 73.

12 Ibid, pp 73–74.

Requirements under the *PCMLTFA*

MSBs are subject to a number of requirements under the *PCMLTFA*. My discussion in this section focuses largely on domestic MSBs; however, foreign MSBs operating in Canada have similar obligations.

MSBs must implement a compliance program, which has six aspects. They must:

- appoint a compliance officer responsible for implementing the program;
- develop and apply written compliance policies and procedures that are kept up to date;
- conduct a risk assessment of the business to assess and document the risk of a money laundering offence or a terrorist activity financing offence occurring in the course of the business's activities;
- develop and maintain a written, ongoing compliance training program for employees, agents, mandataries, or other authorized persons;
- institute and document a plan for the ongoing compliance training program and deliver the training; and
- institute and document a plan for a review (at least every two years) of the compliance program for the purpose of testing its effectiveness.[13]

MSBs must also verify their clients' identities in a variety of situations, including when they:

- receive $10,000 or more in cash;[14]
- receive the equivalent of $10,000 or more in virtual currency;[15]
- issue or redeem $3,000 or more in traveller's cheques, money orders, or similar negotiable instruments;[16]
- initiate an electronic funds transfer of $1,000 or more;[17]
- transfer virtual currency in an amount equivalent to $1,000 or more;[18] and
- exchange virtual currency for funds, funds for virtual currency, or one virtual currency for another in an amount equivalent to $1,000 or more.[19]

13 *PCMLTFA*, s 9.6(1); *PCMLTF Regulations*, s 156(1).
14 *PCMLTF Regulations*, ss 84(a), 105(7)(a), 109(4)(a), and 112(3)(a).
15 Ibid, ss 84(b), 105(7)(a), 109(4)(a), and 112(3)(a).
16 Ibid, ss 95(1)(a) and 105(7)(a).
17 Ibid, ss 95(1)(b) and 105(7)(a).
18 Ibid, ss 95(1)(d) and 105(7)(a).
19 Ibid, ss 95(1)(e) and 105(7)(a).

MSBs have a variety of record-keeping obligations relating to the above situations.[20] They must also take reasonable measures to verify the identity of every person or entity that conducts or attempts to conduct a suspicious transaction.[21] MSBs are also required to verify the identity of beneficiaries of remittances and electronic funds transfers of $1,000 or more,[22] and of corporations or other entities 30 days after beginning a service agreement with them.[23] Further, they must obtain beneficial ownership information when verifying the identity of a legal entity and take reasonable measures to verify the accuracy of that information.[24] MSBs are also required to take reasonable measures to determine if a third party is involved in a transaction,[25] and they have obligations with respect to politically exposed persons.[26]

The *PCMLTFA* imposes a number of reporting obligations on MSBs. These include reporting to FINTRAC:

- the receipt of $10,000 or more in cash in a single transaction[27] from a person or entity;[28]
- the initiation or receipt of an international electronic funds transfer of $10,000 or more in a single transaction;[29]
- the receipt of the equivalent of $10,000 or more in virtual currency in a single transaction;[30] and
- every financial transaction that occurs or is attempted in the course of the MSB's activities and in respect of which there are reasonable grounds to suspect that the transaction is related to the commission or attempted commission of a money laundering or terrorist activity financing offence.[31]

Mr. Cox testified that the Vancouver Bullion and Currency Exchange has implemented a compliance program that is, in some respects, more stringent than the FINTRAC requirements. For example, it conducts an annual external compliance review and verifies its clients' identities for transactions at a lower threshold than is required by the *PCMLTFA*. It also has a policy that clients who attempt to alter a transaction to avoid showing identification (for example, if a client wanted to change a transaction

20 Ibid, ss 31–37.

21 *PCMLTFA*, s 7; *PCMLTF Regulations*, ss 85(1), 105(7)(c), 109(4)(b), and 112(3)(b).

22 *PCMLTF Regulations*, ss 95(1)(e.1), (f), and 105(7)(a).

23 Ibid, ss 95(3), (4), 109(4)(g), and 112(3)(g).

24 Ibid, ss 138(1), (2), and 123.1(b).

25 Ibid, ss 134(1) and 136(1).

26 Ibid, s 120.

27 A "single transaction" includes two or more transactions conducted in a 24-hour period if they are conducted by or on behalf of the same person or entity or for the same beneficiary: ibid, ss 126–129.

28 *PCMLTF Regulations*, s 30(1)(a).

29 Ibid, ss 30(1)(b), (e).

30 Ibid, ss 30(1)(c), (f).

31 *PCMLTFA*, s 7.

amount from $2,000 to $1,950 to come within a threshold) are not permitted to conduct a transaction until they are identified.[32] The exchange also runs transaction monitoring scenarios, which identify scenarios having the potential for money laundering based on the exchange's observations, feedback from banking partners or FINTRAC, external compliance reviews, or elsewhere.[33] Further, it has a policy (which is not required by FINTRAC) of waiting 48 hours before paying out precious metals on transactions that raise concerns, such as concerns about fraudulent bank drafts.[34]

MSBs must also conduct ongoing monitoring of their business relationships with clients.[35] This involves implementing a process to review all the information obtained about a client in order to detect suspicious transactions, keeping information up to date, re-assessing the level of risk associated with the client's transactions and activities, and determining whether the client's transactions and activities are consistent with the information obtained about them and their risk assessment.[36] This monitoring must be done periodically based on the MSB's risk assessment of the client, and enhanced monitoring is necessary for high-risk clients.[37] The MSB must keep a number of records relating to this ongoing monitoring.[38]

MSBs are required to register with FINTRAC.[39] The registry of MSBs is available online, meaning anyone who wishes to look at the registry can do so through the FINTRAC website.[40] According to figures provided by FINTRAC to CMSBA, there were 1,903 MSBs registered with FINTRAC at the time of hearing.[41] Of these, 1,569 provided money transmission and remission services, 1,430 provided foreign exchange services, 226 issued and redeemed negotiable instruments, and 471 were dealers in virtual currency.[42] There were 65 registered foreign MSBs, which have been required to register with FINTRAC since June 1, 2020.[43]

Ms. Achimov testified that a record-high number of MSBs are registered nationally. In the few weeks prior to her testimony, FINTRAC had registered 1,923 MSBs, 398 of which were in BC and 115 of which offered virtual currencies.[44] Ms. Achimov explained that, prior to registering an MSB, FINTRAC checks to ensure that an applicant is

32 Evidence of M. Cox, Transcript, January 18, 2021, pp 40–41.

33 Ibid, pp 42–43.

34 Ibid, pp 45–46.

35 *PCMLTF Regulations*, s 123.1. An MSB enters a business relationship with a client the second time it is required to verify the client's identity within a five-year period or when entering a service agreement: *PCMLTF Regulations*, ss 4.1(b), (d), and (e).

36 *PCMLTF Regulations*, s 123.1.

37 Ibid, ss 123.1, 157(b)(ii).

38 Ibid, s 146(1).

39 *PCMLTFA*, s 11.1.

40 FINTRAC, "Money Services Businesses (MSB) Registry Search," online: https://www10.fintrac-canafe.gc.ca/msb-esm/public/msb-search/search-by-name/.

41 Evidence of J. Iuso, Transcript, January 18, 2021, pp 8–9.

42 Ibid. Mr. Iuso noted that it is unclear how many MSBs provided multiple services: ibid, p 9.

43 Evidence of J. Iuso, Transcript, January 18, 2021, p 9.

44 Evidence of D. Achimov, Transcript, January 18, 2021, pp 178–79.

a registered Canadian business. It also does criminal record checks of applicants (including of the directors, owners, and president of applicants that are corporations) and other checks such as consulting terrorist listings and media mentions.[45] In the absence of effective beneficial ownership registry data, FINTRAC does not have access to that sort of information about MSBs.[46] Although there are currently no restrictions on where an MSB might operate, FINTRAC considers the place of operation (for example, MSBs that operate from a residence).[47]

Section 11.11 of the *PCMLTFA* lists persons and entities that are not eligible for registration. These include (but are not limited to) persons or entities who:

- are subject to sanctions;
- are listed as terrorist entities under the *Criminal Code*;
- have been convicted of a money laundering or terrorist financing offence; or
- have been convicted of other listed offences.

Ms. Achimov testified that FINTRAC can only refuse registration if an applicant has been *convicted* of specified offences. It is insufficient if there has been only an investigation or a charge.[48] However, FINTRAC may consider ongoing investigations to inform its compliance activities and risk rating.[49] FINTRAC keeps track of MSBs that are refused registration.[50]

I appreciate that section 11.11 of the *PCMLTFA* provides that certain listed persons and entities are ineligible for registration, and that the focus is on *convictions*. Notably, however, the section does not state that *only* people or entities who have been convicted of such offences are ineligible. It may be (but I do not resolve the point) that certain individuals or entities could, or should, be found ineligible for registration on other bases.

In this regard, the situation of Silver International Investment Ltd. (Silver International) is illustrative. As I discuss in more detail in Chapter 3, Silver International was investigated by the RCMP as part of Project E-Pirate, the only major money laundering investigation in British Columbia to result in criminal charges between 2015 and 2020.[51] The RCMP was investigating an alleged money laundering scheme involving informal value transfer, cash facilitation at BC casinos,

45 Ibid, pp 129–131.

46 Ibid, p 131.

47 Ibid, p 132.

48 Ibid, pp 133, 161, 194.

49 Ibid, pp 133–34.

50 Ibid, p 177.

51 Note, however, that the Crown entered a stay of proceedings on November 22, 2018, with the result that the matter did not proceed to trial: Exhibit 663, Affidavit of Cpl. Melvin Chizawsky, February 4, 2021, Exhibit A, para 125.

and an unlicensed gaming house. Between April 2015 and February 2016, the RCMP conducted 40 days of surveillance on an individual named Paul Jin and his associates.[52] The surveillance revealed that Mr. Jin was frequently attending the offices of Silver International, and police came to believe that he was moving cash from Silver International to another property for repackaging and that he was running an unlicensed gaming house.[53]

On October 15, 2015, the RCMP executed search warrants at Silver International and several other locations, which resulted in the seizure of large sums of cash as well as financial ledgers and daily transaction logs.[54] An analysis conducted by a financial analyst at the RCMP concluded that Silver International had conducted 474 debit transactions totalling $83,075,330 and 1,031 credit transactions totalling $81,462,730 for the 137-day period between June 1, 2015, and October 15, 2015, which corresponded on an annual basis to approximately $221 million in debit transactions and $217 million in credit transactions.[55]

Surprisingly, despite the lengthy investigation by the RCMP culminating in several search warrants in October 2015, Silver International was registered with FINTRAC as a money services business three months later in December 2015.[56] When asked about this, Ms. Achimov stated that she was not at liberty to discuss specific cases. However, she testified that suspected criminality in isolation would not qualify as a reason for FINTRAC to refuse registration of an MSB, noting that a criminal conviction would be required.[57]

I recommend later in this chapter that the Province subject money services businesses to regulation by BCFSA. In my view, the anomalous result that an applicant for registration as an MSB could be the subject of a major and active money laundering investigation by law enforcement that had revealed significant evidence of criminality and still be registered by FINTRAC calls for added scrutiny, which could be achieved through regulation by BCFSA.

MSBs must re-register with FINTRAC every two years.[58] Ms. Achimov testified that this is where FINTRAC does the "deeper dive."[59] It also does a periodic review of MSBs to verify whether they have any convictions.[60] As I expand below, although a more detailed analysis of an MSB's eligibility after two years is a good start, I do not believe it is sufficient and am recommending that BCFSA conduct compliance examinations prior to the two-year mark.

52 Exhibit 663, Affidavit of M. Chizawsky, para 116.

53 Ibid, paras 38, 107, 108, 115.

54 Ibid, paras 65–66.

55 Ibid, para 99. See **Chapter 3** for a more detailed discussion of these findings.

56 Evidence of M. Chizawsky, Transcript, March 1, 2021, p 104.

57 Evidence of D. Achimov, Transcript, January 18, 2021, p 133.

58 *PCMLTFA*, s 11.19.

59 Evidence of D. Achimov, Transcript, January 18, 2021, p 175.

60 Ibid.

Money Laundering Risks

There are a number of money laundering risks associated with MSBs. This section addresses the risks relating to more traditional MSBs. I discuss virtual asset service providers (which are now deemed to be MSBs) in Chapter 35 and informal value transfer services (which are also considered MSBs) in Chapters 3 and 37.

Although there are particular risks associated with MSBs, as outlined below, it is important to note that many of the risks apply equally to credit unions, banks, and other financial institutions.[61] Barry MacKillop, deputy director of intelligence at FINTRAC, testified that, in terms of the quantity of money being moved, much more is moved through the formal financial system using banks than through MSBs. However, he acknowledged that there may be higher risks relating to certain aspects of MSBs, for example, unregistered ones.[62]

Risk Assessments

Canada's 2015 national risk assessment and the Financial Action Task Force's 2016 mutual evaluation of Canada both addressed the risks relating to MSBs. In the national risk assessment, MSBs were rated as having a "medium" to "very high" risk.[63] The assessment notes that "[a]lthough the MSB sector is broadly vulnerable, the degree of vulnerability is not uniform largely because of the variations in terms of size and business models."[64] It adds that the MSB sector handles billions of dollars in transactions every year and estimates that MSBs registered with FINTRAC handle approximately $39 billion per year.[65]

National full-service MSBs and small independent MSBs were rated as having a "very high" vulnerability rating. The former conduct a large amount of transactional business of products and services that have been found vulnerable to money laundering and terrorist financing, and these products and services are accessible to clientele in vulnerable businesses or locations.[66] Meanwhile, small independent MSBs, which are predominantly family owned, provide wire transfer services largely through informal networks. They can be used by high-risk clients to wire funds to high-risk jurisdictions, and because they tend to be small and low profile, they are vulnerable to exploitation.[67]

The products and services that were said to be used for money laundering and terrorist financing most frequently were international electronic funds transfers, currency exchanges, negotiable instruments, and cash transactions. The assessment report also identifies five main money laundering methods or techniques involving MSBs:

61 Evidence of B. MacKillop, Transcript, January 18, 2021, p 104.

62 Ibid.

63 Exhibit 3, Overview Report: Documents Created by Canada, Appendix B, Department of Finance, *Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada, 2015* (Ottawa: 2015), p 32.

64 Ibid, p 38.

65 Ibid, p 35

66 Ibid, p 32.

67 Ibid.

- structuring or attempting to circumvent record-keeping requirements;
- attempting to circumvent client identification requirements;
- smurfing, using nominees and/or other proxies;
- exploiting negotiable instruments; and
- refining.[68]

The 2016 mutual evaluation similarly found that full-service MSBs are vulnerable to money laundering because they are widely accessible, are exposed to clients in vulnerable businesses or are conducting activities in locations of concern, and may attract clientele such as drug traffickers.[69] The evaluation found that MSBs that operated globally were aware of the risks they face and had developed criteria to evaluate risks and determine controls. However, smaller MSBs seemed "far less aware" of their obligations and vulnerabilities.[70]

Typologies

Many of the money laundering risks associated with MSBs arise due to the involvement of professional money launderers and informal value transfer systems.[71] Indeed, both FINTRAC and the Criminal Intelligence Service British Columbia / Yukon Territory consider that the use of MSBs by professional money launderers poses a high threat in this province.[72] They have observed that organized crime groups use professional money launderers who own MSBs operating in BC to launder funds.[73] The use of MSBs by professional money launderers is said to be high threat because it involves complex, long-term money laundering operations, manipulation of the money transfer system, and transnational organized crime groups. Further, the professional money launderer is often detached from the predicate offence, posing difficulties for law enforcement seeking to investigate and prosecute them.[74]

68 Ibid, p 48.

69 Exhibit 4, Overview Report: Financial Action Task Force, Appendix N, FATF, *Anti-Money Laundering and Counter-Terrorist Financing Measures – Canada, Fourth Round Mutual Evaluation Report* (Paris: FATF, 2016), p 16, para 55.

70 Ibid, p 79, para 210.

71 I discuss informal value transfer systems and the involvement of professional money launderers further in Chapters 2, 3, and 37.

72 Exhibit 437, Criminal Intelligence Service BC / Yukon, "Criminal Market Narrative – Money Laundering" (2018) p 8; Exhibit 438, Criminal Intelligence Service BC / Yukon, "Professional Money Launderers Who Own/Control Money Services Businesses" (November 2018); Exhibit 442, FINTRAC, "Financial Intelligence Report: Professional Money Laundering in Canada" (2019).

73 Exhibit 437, Criminal Intelligence Service BC / Yukon, "Criminal Market Narrative – Money Laundering" (2018), p 7; Exhibit 438, Criminal Intelligence Service BC / Yukon, "Professional Money Launderers Who Own/Control Money Services Businesses" (November 2018), pp 1, 5–6; Exhibit 442, FINTRAC, "Financial Intelligence Report: Professional Money Laundering in Canada" (2019), pp 1, 9.

74 Exhibit 437, Criminal Intelligence Service BC / Yukon, "Criminal Market Narrative – Money Laundering" (2018), p 8; Exhibit 438, Criminal Intelligence Service BC / Yukon, "Professional Money Launderers Who Own/Control Money Services Businesses" (November 2018), p 1.

Money laundering using MSBs owned by professional money launderers often feature a variety of complex transactions. A diagram[75] in a 2019 FINTRAC report is illustrative (Figure 21.1):

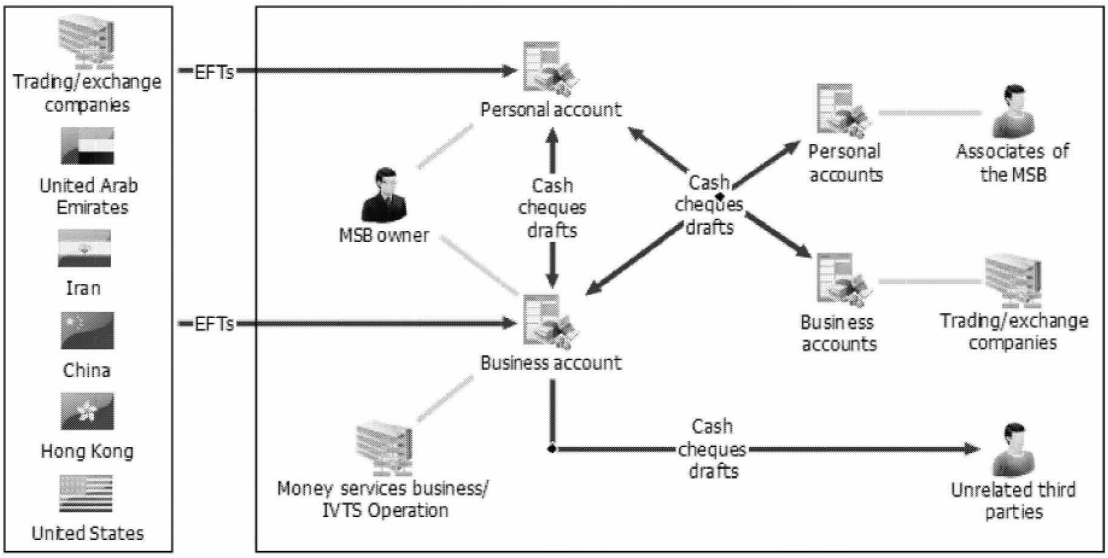

Figure 21.1: Typical Professional Money Laundering Services Through MSBs

Source: Exhibit 442, FINTRAC, "Financial Intelligence Report: Professional Money Laundering in Canada" (2019), p 8

This diagram depicts a variety of transactions being made between foreign trading and exchange companies; transfers between an MSB owner's personal and business accounts; and transfers of cash, cheques, and drafts to associates of the MSB, trading and exchange companies, and unrelated third parties.[76] When foreign trading or exchange companies are involved, the scheme may involve trade-based money laundering in which goods may be undervalued, overvalued, or non-existent.[77]

Mr. MacKillop testified that these kinds of schemes occur in BC, noting that once the money is in Canada, it can be further laundered through casinos and real estate. He explained that the money is not truly being transferred: rather, money is deposited into a bank account in another country, withdrawn in Canada, and provided to individuals who can then use it in casinos or in real estate.[78] He noted that financial institutions are effectively intermediaries in these scenarios because all MSBs would need a bank account to move the money; FINTRAC can therefore see reports from these institutions.[79] Indeed, given the value of the information coming in from the financial

75 Exhibit 442, FINTRAC, "Financial Intelligence Report: Professional Money Laundering in Canada" (2019), p 8.

76 Ibid.

77 Evidence of B. MacKillop, Transcript, January 18, 2021, p 111.

78 Evidence of B. MacKillop, Transcript, January 18, 2021, pp 115–16.

79 Ibid, pp 111–12.

institution in these scenarios, de-risking is unpalatable: if the financial institution de-risks an MSB, FINTRAC will no longer have a lens into the activity.[80]

Megan Nettleton, acting supervisor at the RCMP's Financial Crime Analysis Unit, described a typical scheme involving a foreign national and criminally controlled MSB as follows. The scheme is essentially one of informal value transfer. It begins with a foreign national seeking to transfer funds to Canada from a country that has restrictions on capital flight. A deposit is made in that foreign country through a bank account that is controlled by someone associated with an MSB in Canada. A cash courier working for organized crime drops off cash at the MSB, which lends the money to the foreign national (who may or may not realize the funds are illicit in Canada). The money is loaned at a commission and then paid back to the MSB or professional money launderer who owns it. The foreign national then uses the money to gamble or for other purposes, thereby laundering it on behalf of the organization. The MSB may also provide loans as a private mortgage lender to the foreign national for the purpose of buying a house, or might set up, with the assistance of lawyers, registered numbered companies that can purchase real estate with minimal detection. Ms. Nettleton noted that these kinds of schemes can involve millions of dollars.[81]

A 2018 report by the Criminal Intelligence Service BC / Yukon describes the various techniques that may be used by professional money launderers who own or control MSBs, including:

- structuring transactions between various MSBs;
- using nominees to manage and move millions of dollars through various accounts;
- collaborating worldwide with other money launderers;
- using informal value transfer systems to assist organized crime clientele;
- using structuring or smurfing methods to break down large transactions so they fall below the $10,000 reporting threshold;
- layering transactions using other MSBs to facilitate electronic funds transfers;
- creating false bookkeeping to conceal the "real" books from FINTRAC; and
- using underground banking channels such that goods of value or money are moved while the money remains in the original country.[82]

A 2010 FINTRAC report on typologies and trends for Canadian MSBs contains a similar list of techniques, including structuring (which is the most prevalent technique observed

80 Evidence of A. Ryan, Transcript, January 18, 2021, pp 113–14.

81 Evidence of M. Nettleton, Transcript, January 18, 2021, pp 19–22.

82 Exhibit 438, Criminal Intelligence Service BC / Yukon, "Professional Money Launderers Who Own/Control Money Services Businesses" (November 2018), pp 1, 3–4.

by FINTRAC); attempting to circumvent client identification and verification measures; smurfing and using nominees and/or other proxies; exploiting negotiable instruments; and refining.[83] It also highlights that an emerging issue at the time was the convergence and combination of new payment methods (including prepaid cards, internet payment services, and mobile payment services), sometimes alongside traditional payment methods. The risks that arise in this regard include that prepaid payment methods can be funded anonymously or by a third party, meaning that customer due diligence will not be done; withdrawals and conversion of funds can be done more quickly than with traditional channels, rendering it more difficult to follow the money trail; and the payment systems are distributed through the internet, making the establishment of a customer relationship on a non-face-to-face basis difficult, if not impossible.[84]

I note that many MSBs are aware of the risks in their sector and comply with the *PCMLTFA*. Mr. MacKillop noted that many suspicious transaction reports submitted by MSBs flag conduct such as very quick movement of funds, the use of different agents during a 24- or 36-hour period, and movement of money that is inconsistent with one's level of employment or status.[85] He added that some larger MSBs are uniquely positioned to report to FINTRAC, as they can identify transactions involving individuals in other countries.[86] However, FINTRAC tends to receive many more reports from banks, trust loans, credit unions, and *caisses populaires* than from MSBs, which Mr. MacKillop stated "speaks to the percentage of the financial transactions that actually occur," as well as changes to the reporting system of *caisses populaires* that have led to higher quality reports being submitted.[87]

De-risking

Most MSBs need accounts at mainstream financial institutions to process transfers and settle accounts. An issue arises, however, because some financial institutions avoid doing business with MSBs, perceiving them as high risk in terms of their anti–money laundering and counterterrorist financing obligations (or sometimes as competitors).[88] The practice of declining a customer (or sometimes a market segment) because of such concerns is known as "de-risking."[89]

83 Exhibit 441, FINTRAC, *Money Laundering and Terrorist Financing (ML/TF) Typologies and Trends for Canadian Money Services Businesses (MSBs)*, July 2010, pp 5–6. Mr. MacKillop believes this is the most recent typology report on MSBs from FINTRAC's intelligence branch: Evidence of B. MacKillop, Transcript, January 18, 2021, pp 102–103.

84 Exhibit 441, FINTRAC, *Money Laundering and Terrorist Financing (ML/TF) Typologies and Trends for Canadian Money Services Businesses (MSBs)*, July 2010, p 16.

85 Evidence of B. MacKillop, Transcript, January 18, 2021, p 118.

86 Ibid, pp 118–19.

87 Ibid, pp 121–22.

88 Exhibit 440, BC Ministry of Finance, Money Services Businesses Public Consultation Paper (March 2020), p 5; Exhibit 311, BC Ministry of Finance, Briefing Document: Money Services Businesses Consultation – Summary (June 8, 2020), p 4.

89 Exhibit 440, BC Ministry of Finance, Money Services Businesses Public Consultation Paper (March 2020), p 5.

De-risking has caused serious issues for some MSBs, as well as for virtual asset service providers (see Chapter 35). Some MSBs have trouble maintaining accounts with financial institutions, which has a serious impact on their business model: it limits their ability to transmit remittances and may cause them to conduct transactions through less transparent informal channels.[90] Further, existing MSB-banking relationships may be very restrictive and costly, and there is always a concern that the bank will close the account.[91]

Between 2009 and 2015, the number of MSBs shrunk from over 2,400 to approximately 800. CMSBA heard from its members that this was because of de-risking.[92] Indeed, de-risking has been a significant concern at meetings of CMSBA. Mr. Cox testified that being de-risked can be the difference between an MSB staying open or closing.[93] Similarly, Mr. Iuso described banking services as being

> like a utility, like a telco providing the phone line service or an internet provider providing the internet service. It's necessary for us to operate. Otherwise, the MSBs end up going further underground or further obfuscating their business practices, which leads to, we believe, more activity that isn't caught or isn't reported.[94]

A further issue arises because some larger MSBs, at the request of their financial partners, do not offer services to other MSBs. For example, the Vancouver Bullion and Currency Exchange does not provide services to other MSBs at the request of its banking partners.[95] As Mr. Cox explained:

> MSBs are an inherently high-risk industry … [T]he potential for money laundering is well known … [O]ur banking partners seem to be comfortable with vetting [the Vancouver Bullion and Currency Exchange]. They have reviewed our system and are comfortable that we are handling our clients and transactions appropriately. I believe their concern is that although they have vetted our company, they are not able to vet our customer's customers, the clients of another MSB that we might have onboarded. So [it is] just one level removed from what they are comfortable with.[96]

From March 6 to April 30, 2020, the Province sought input from the MSB industry on the potential for provincial regulation of the sector.[97] During the consultation, it

90 Ibid.

91 Exhibit 311, BC Ministry of Finance, Briefing Document: Money Services Businesses Consultation – Summary (June 8, 2020), p 4.

92 Exhibit 440, BC Ministry of Finance, Money Services Businesses Public Consultation Paper (March 2020), p 5; Evidence of J. Iuso, Transcript, January 18, 2021, pp 58–59.

93 Evidence of M. Cox, Transcript, January 18, 2021, pp 61–62.

94 Evidence of J. Iuso, Transcript, January 18, 2021, pp 59–60.

95 Evidence of M. Cox, Transcript, January 18, 2021, p 13.

96 Evidence of M. Cox, Transcript, January 18, 2021, pp 13–14.

97 See Exhibit 311, BC Ministry of Finance, Briefing Document: Money Services Businesses Consultation – Summary (June 8, 2020); and Exhibit 440, BC Ministry of Finance, Money Services Businesses Public Consultation Paper (March 2020).

heard suggestions that banks and credit unions should be required to provide reasons for declining to provide banking services to MSBs and that MSBs should have redress or an appeal process if they were unable to obtain a bank account.[98] Indeed, Mr. Iuso and Mr. Cox were both supportive of a requirement that financial institutions provide banking services to MSBs that meet certain requirements.[99] Mr. Cox added that it would be ideal for MSBs to have access to services offered by banks, although services from credit unions may also assist.[100] Relatedly, CMSBA suggested that BC financial institutions should be required to remove registered MSBs from their "high-risk" anti–money laundering category if they have no history of non-compliance.[101]

While I understand the difficulties that arise for MSBs who are unable to secure reliable banking services, I do not see it as tenable to require that financial institutions accept a certain category or group of clients. Financial institutions have numerous requirements under the *PCMLTFA* and other legislation, leading to risk assessments that can be quite complex. They should not be forced to accept clients that do not meet their risk tolerance. However, given the clear difficulties that de-risking poses for MSBs, I urge CMSBA and financial institutions to discuss this issue and understand each other's respective concerns in the hope of expanding the availability of financial services for MSBs. It seems that it would be best to have an agreed-upon protocol that facilitates MSBs securing the services of financial institutions. Such a protocol will, I hope, be considered and developed collaboratively by financial institutions and MSBs.

Unregistered MSBs

As I noted above, MSBs are required to register with FINTRAC every two years. However, some MSBs do not register. As unregistered MSBs do not report to FINTRAC, the latter lacks visibility into their activities.[102] Unregistered MSBs may seek to use registered MSBs to wire funds or settle transactions, which in turn presents risks for registered MSBs. This leads to opportunities for anonymity (given the lack of reporting) and can create investigative obstacles and reputational risk for registered MSBs who could be unwittingly facilitating illegal activity.[103] Indeed, the Province's consultation revealed that CMSBA and mid-sized MSBs in BC had significant concerns around unregistered MSBs operating without oversight.[104]

98 Exhibit 311, BC Ministry of Finance, Briefing Document: Money Services Businesses Consultation – Summary (June 8, 2020), p 4.

99 Evidence of M. Cox, Transcript, January 18, 2021, pp 62–63; Evidence of J. Iuso, Transcript, January 18, 2021, pp 59–60.

100 Evidence of M. Cox, Transcript, January 18, 2021, p 63.

101 Exhibit 311, BC Ministry of Finance, Briefing Document: Money Services Businesses Consultation – Summary (June 8, 2020), p 5.

102 Evidence of B. MacKillop, Transcript, January 18, 2021, pp 103, 122–23.

103 Exhibit 441, FINTRAC, *Money Laundering and Terrorist Financing (ML/TF) Typologies and Trends for Canadian Money Services Businesses (MSBs)*, July 2010, pp 15–16.

104 Exhibit 311, BC Ministry of Finance, Briefing Document: Money Services Businesses Consultation – Summary (June 8, 2020), p 3; Evidence of J. Iuso, Transcript, January 18, 2021, p 55.

The main way that FINTRAC can become aware of unregistered MSBs is when another reporting entity, such as a bank, identifies an individual or entity acting as an MSB, realizes the individual or entity is not on the public registry, and files a suspicious transaction report.[105] If someone other than a reporting entity comes across an unregistered MSB, they can submit a voluntary information record, which FINTRAC can then analyze and disclose to law enforcement if the threshold for disclosure is met.[106] Through its annual review of MSBs, FINTRAC also considers whether all registered MSBs are still operating, their registration has expired or ceased, they have been denied registration, or they are no longer operating.[107] Although unregistered MSBs may be uncovered through such steps, identifying unregistered MSBs remains one of the "constant challenges" in this sector.[108]

Ms. Nettleton testified that the RCMP had recently carried out a project (known as the Money Services Businesses Compliance Project) to examine unregistered MSBs. It found that most are difficult to find because they do not readily advertise themselves.[109] The project examined over 529 MSBs that were unregistered or had their registration revoked or lapsed. It did not find significant criminality among the 529 MSBs; however, the RCMP used its own data banks rather than doing door knocks or conducting surveillance on specific entities. Further, the fact that an MSB is registered and compliant does not necessarily eliminate the money laundering risk.[110] For example, sometimes an MSB is subject to regulatory action and simply re-registers with a different address. Such a simple step may permit it to continue its illegal activity despite being registered.[111] Indeed, the fact that Silver International was able to obtain registration despite being actively investigated by law enforcement suggests that both registered and unregistered MSBs may be able to conduct criminal or suspicious activity for some time without detection, or, even if detected, without action that interrupts their operation.

It appears that some MSBs are unregistered due to language barriers and a resulting lack of awareness in some cultural and linguistic groups.[112] Ms. Achimov testified that FINTRAC is aware of these barriers and tries to reach those MSBs through professional associations. She added that some regional offices have multiple linguistic capabilities and that FINTRAC has produced some basic information about compliance in several languages.[113] It also attempts to create awareness with unregistered MSBs, including through social media, and works with different communities in an effort to reach MSBs that may not be members of professional associations.[114]

105 Evidence of B. MacKillop, Transcript, January 18, 2021, pp 122–23; Evidence of D. Achimov, Transcript, January 18, 2021, p 123.

106 Evidence of B. MacKillop, Transcript, January 18, 2021, pp 126–27.

107 Evidence of D. Achimov, Transcript, January 18, 2021, pp 160–61.

108 Exhibit 448, FINTRAC, Report to the Minister of Finance on Compliance and Related Activities (September 2018), pp 8–9; see also Evidence of D. Achimov, Transcript, January 18, 2021, pp 140–41.

109 Evidence of M. Nettleton, Transcript, January 18, 2021, pp 51–52, 57.

110 Ibid, pp 53–54, 75–76.

111 Ibid, p 52.

112 Evidence of M. Nettleton, Transcript, January 18, 2021, p 52; Evidence of J. Iuso, Transcript, January 18, 2021, pp 54–56.

113 Evidence of D. Achimov, Transcript, January 18, 2021, pp 154, 166–67.

114 Ibid, pp 167–68.

A 2016 FINTRAC report notes that one way of identifying unregistered MSBs is by enhancing the reporting it receives from financial institutions.[115] Mr. MacKillop testified that this continues to be the case, noting that FINTRAC consistently does outreach with financial institutions and other reporting entities.[116]

Compliance Examinations by FINTRAC

FINTRAC conducts relatively few compliance examinations of MSBs. Canada helpfully provided tables setting out the number of MSBs examined nationally and in BC between 2015 and 2020.[117] Table 21.1 indicates, in relation to MSBs located in this province:

Table 21.1: Number of MSBs Operating in BC Between 2015 and 2020

Fiscal Year	Number of MSBs	Number of Onsite Examinations[118]	Number of Desk Examinations
2015–16	164	33	14
2016–17	155	24	6
2017–18	190	13	1
2018–19	222	24	0
2019–20	317	13	3

Source: Exhibit 446, FINTRAC Statistics Letter (January 15, 2021), p 1

It is notable that the number of MSBs nearly doubled between the 2015–16 and 2019–20 fiscal years, growing from 164 to 317. During that time, the number of onsite examinations, however, dropped from 33 to 13. Similarly, the number of desk examinations fell from 14 to three. When asked why FINTRAC conducted fewer examinations in 2019–20 when the number of MSBs in BC had almost doubled since 2015–16, Ms. Achimov explained that there are a number of factors that inform FINTRAC's examinations. The main one is risk scoring, but others include FINTRAC's capacity, difficulties relating to the COVID-19 pandemic, and the situation of the MSB (for example, a desk examination may be more suitable than an onsite one for an MSB that is operating virtually).[119]

On the subject of FINTRAC's capacity, I was advised that the BC office has approximately 15 people who examine all the reporting entities in this province.[120]

115 Exhibit 445, FINTRAC, *Financial Intelligence Report: Criminal Informal Value Transfer Systems (IVTS)* (February 2016), p 6.

116 Evidence of B. MacKillop, Transcript, January 18, 2021, pp 127–28.

117 Exhibit 446, FINTRAC Statistics Letter (January 15, 2021), p 1.

118 An onsite examination involves FINTRAC compliance evaluators visiting the MSB's premises, whereas a "desk examination" is conducted over the phone: Evidence of D. Achimov, Transcript, January 18, 2021, pp 136–37.

119 Evidence of D. Achimov, Transcript, January 18, 2021, pp 142–143, 144–45.

120 Evidence of D. Achimov, Transcript, January 18, 2021, pp 145–146.

FINTRAC's report to the federal Minister of Finance in 2018 explains that a decrease in the number of examinations was due in part to a "higher than expected employee turnover in the regional offices" as well as "regional restructuring to ensure sufficient coverage of the higher-risk areas, including major financial entities."[121] Ms. Achimov explained that there was a high turnover in the Toronto regional office at that time, which led to a reallocation of some resources and a need to train new employees.[122]

I also note that these figures do not take account of MSBs whose status had expired or that were not registered at the end of the fiscal year.[123] I understand from that caveat that the figures would not take account of applicants who, for example, were found ineligible on the basis of a prior criminal conviction or had their status revoked for that reason. It is therefore unclear how many non-successful applicants there were and if any had links to criminality.

Canada also provided statistics on the number of examinations done in the first two years of an MSB's existence (see Table 21.2).[124] This is of interest given that MSBs must re-register every two years. Further, as Ms. Achimov noted, many MSBs are by their existence very short-lived. She explained that many MSBs are "small mom and pop organizations" and are very volatile.[125]

Table 21.2: Number of MSBs in BC Examined in the First Two Years of Registration

Fiscal Year	New Registration Count	Examined Within 2 Years of Registration	Examined After 2 Years of Registration	MSB Registration Active and Available in the Pool	MSB Registration Inactive[126]
2015–16	34	10	3	2	19
2016–17	29	5	4	3	17
2017–18	59	4	1	23	31
2018–19	65	3	0	52	10
2019–20	124[127]	1	0	111	12

Source: Exhibit 446, FINTRAC Statistics Letter (January 15, 2021), p 3

121 Exhibit 448, FINTRAC, Report to the Minister of Finance on Compliance and Related Activities (September 2018), p 8.

122 Evidence of D. Achimov, Transcript, January 18, 2021, p 159.

123 Exhibit 446, FINTRAC Statistics Letter (January 15, 2021), p 2.

124 Exhibit 446, FINTRAC Statistics Letter (January 15, 2021), p 3.

125 Evidence of D. Achimov, Transcript, January 18, 2021, pp 142, 151.

126 This includes registrations that are ceased, expired, cancelled, or revoked: Exhibit 446, FINTRAC Statistics Letter (January 15, 2021), p 3.

127 The marked increase from 65 to 124 MSBs can be attributed to the pre-registration of MSBs dealing in virtual currency and of foreign MSBs. A similar increase occurred nationally, from 321 to 532: Exhibit 446, FINTRAC Statistics Letter (January 15, 2021), pp 2–3.

It is notable that of the 59 new MSBs registered in 2017–18, only four were examined in the first two years, and only one after that. The figures in 2018–19 (65 new registrations, three examined within the first two years, and zero after that) and 2019–20 (124, one, and zero, respectively) are striking as well (although I am mindful that these figures were provided in January 2021, meaning those relating to the 2019–20 registrations may have since changed). I also note that the figures do not include (a) situations where FINTRAC attempted to conduct an examination but was not able to because the MSB was no longer operating, or (b) any follow-up examinations of MSBs with deficiencies.[128]

Ms. Achimov testified that FINTRAC's methodology looks at a cross-section of both established MSBs and those that are just starting up.[129] Indeed, FINTRAC's report to the Minister from 2020 indicates that it conducts annual MSB validations to identify those that may be operating with expired, ceased, revoked, or denied registrations; those that may no longer be operating; and those that are suspected of operating but are not registered.[130] Examinations of MSBs operating for under two years might be triggered by intelligence, regional knowledge, media coverage, or themed examinations (for example, requirements in a ministerial directive).[131] Ms. Achimov explained that, as with any business, MSBs must "have the opportunity to have a bit of a track record. They have to have the ability to file their reports, to have something that we can review." She continued that FINTRAC tends to look six to eight months in the past but may decide to look at very new organizations within six months if there is media coverage, they are alerted to suspicious activity, or other reasons warrant moving up an examination.[132]

It strikes me that it would be useful for there to be more scrutiny of MSBs in the first two years of registration. Early examinations would presumably deter those seeking to use MSBs for criminal purposes and would seem to encourage better practices among MSBs from the beginning. Given the low numbers of examinations done by FINTRAC in the first two years of an MSB's existence, the Province should fill this gap. As I discuss below, I am of the view that BCFSA, acting as a regulator for MSBs, would be well placed to examine MSBs in their early years.

Annette Ryan, chief financial officer and deputy director of the enterprise policy research and program sector at FINTRAC, noted that FINTRAC's fall 2020 policy snapshot had an increased focus on penalties and administration relating to registration. It speaks of tightening the registration process and adjusting penalties.[133] She also noted that FINTRAC released an operational alert[134] relating to MSBs in July 2018, flagging certain

128 Exhibit 446, FINTRAC Statistics Letter (January 15, 2021), p 2.

129 Evidence of D. Achimov, Transcript, January 18, 2021, pp 141–42.

130 Exhibit 1021, Overview Report: Miscellaneous Documents, Appendix 15, FINTRAC Report to the Minister of Finance on Compliance and Related Activities (September 30, 2020), pp 21–22.

131 Exhibit 446, FINTRAC Statistics Letter (January 15, 2021), p 2.

132 Evidence of D. Achimov, Transcript, January 18, 2021, p 147.

133 Evidence of A. Ryan, Transcript, January 18, 2021, pp 107, 162.

134 An operational alert is a public document intended to inform reporting entities about emerging trends that constitute suspicious activity. It is meant to help the community flag certain transactions, adjust their reporting process, etc.: Evidence of A. Ryan, Transcript, January 18, 2021, p 109.

kinds of MSBs of concern. That alert referred to MSBs engaged in legitimate activities that allow some money laundering as part of their business (knowingly or unwittingly), as well the potential for MSBs to be owned or operated by illicit actors.[135]

Mr. MacKillop testified that FINTRAC's compliance department cannot share information with the intelligence group. This is because compliance examinations do not require warrants.[136] However, the intelligence group can share limited information with the compliance group. For example, it could share reports indicating suspicious activity flagged by an MSB or by another reporting entity relating to a potential unregistered MSB.[137] Mr. MacKillop stated that FINTRAC does not often come across entities that are acting as MSBs, however. More commonly, it encounters a lack of reporting or insufficient information in a report, in which case it would communicate this to the compliance department so that they can provide some awareness and understanding to the MSB about what reports require.

Investigative Challenges

MSBs present unique investigative challenges for both law enforcement and FINTRAC. A key challenge is that the use of MSBs by organized crime and professional money launderers is almost certainly underreported.[138] Ms. Nettleton testified that this intelligence gap still exists.[139] She explained that there are several reasons for this, including that:

- FINTRAC reporting does not capture all the relevant activity (such as bulk cash smuggling or domestic transfers);
- the RCMP's intelligence group focuses not only on money laundering but other offences;
- uncovering such activity often requires use of tools such as phone data, human sources, and intercepts, which the RCMP typically considers as "last resorts" given how intrusive they are;
- reports from FINTRAC are not sources of "live" intelligence (they are necessarily after the fact);
- under the *PCMLTFA*, FINTRAC can only disclose information that meets its threshold and is related to money laundering (that is, not with respect to other offences that may be of interest to law enforcement); and

135 Evidence of A. Ryan, Transcript, January 18, 2021, p 109.

136 Evidence of B. MacKillop, Transcript, January 18, 2021, pp 98–99.

137 Ibid.

138 Exhibit 437, Criminal Intelligence Service BC / Yukon, "Criminal Market Narrative – Money Laundering" (2018), pp 2, 8; Exhibit 438, Criminal Intelligence Service BC / Yukon, "Professional Money Launderers Who Own/Control Money Services Businesses" (November 2018), p 7; Evidence of M. Nettleton, Transcript, January 18, 2021, pp 28–29, 33.

139 Evidence of M. Nettleton, Transcript, January 18, 2021, p 33.

- law enforcement lacks capacity (both in terms of experienced investigators and civilian staff such as translators and analysts) to effectively investigate MSBs.[140]

In its 2017 report to the Minister of Finance, FINTRAC notes that it made one "non-compliance disclosure" to law enforcement relating to an MSB.[141] Non-compliance disclosures are made "where there is extensive non-compliance with the *PCMLTFA* or little expectation of immediate or future compliance by the reporting entity."[142] FINTRAC's 2020 report indicates it made seven non-compliance disclosures in relation to the 114 MSBs it examined.[143] Ms. Achimov testified that, in the four years prior to her testimony, FINTRAC had made 27 non-compliance disclosures in relation to all reporting entities (that is, not specifically relating to MSBs).[144] While I appreciate that FINTRAC must comply with its disclosure threshold in the *PCMLTFA*, these numbers strike me as low. I assume, though I am unable to determine on the evidence before me, that they are low in part because of the recognized underreporting by MSBs, the fact that some MSBs do not register with FINTRAC, and the relatively low number of compliance examinations done by FINTRAC.

Mr. Iuso testified that CMSBA does not receive any information relating to anti–money laundering from the RCMP or FINTRAC. It does, however, receive annual reports from FINTRAC on the number of suspicious transactions and other reports by MSBs and the number of MSBs that have been examined. CMSBA does not currently have a memorandum of understanding with FINTRAC.[145] It does, however, participate in working groups with FINTRAC about updates to legislation, policy interpretations, and guidance, and FINTRAC has an outreach employee dedicated to dealing with CMSBA.[146] FINTRAC engaged with MSB associations (including CMSBA and virtual currencies dealers) multiple times between 2019 and 2020,[147] and it provides notices and alerts to CMSBA to forward to its members.[148]

Mr. Cox testified that the Vancouver Bullion and Currency Exchange receives regular requests for information from the RCMP and the Canada Revenue Agency. While it does receive many requests from FINTRAC, they are also in contact about future guidelines and rules.[149] Mr. Cox explained that his experience with FINTRAC was that it was initially adversarial to the Vancouver Bullion and Currency Exchange – focused

140 Ibid, pp 26–31, 33–34.

141 Exhibit 447, FINTRAC Report to the Minister of Finance on Compliance and Related Activities (September 30, 2017), p 15.

142 Ibid.

143 Exhibit 1021, Overview Report: Miscellaneous Documents, Appendix 15, FINTRAC Report to the Minister of Finance on Compliance and Related Activities (September 30, 2020), pp 20–21.

144 Evidence of D. Achimov, Transcript, January 18, 2021, pp 156–57.

145 Evidence of J. Iuso, Transcript, January 18, 2021, pp 60–61.

146 Ibid, pp 64–65.

147 Exhibit 449, List of FINTRAC Engagement Activities with Different Stakeholders, April 1, 2017 to December 4, 2020, pp 1, 2, 7, 8, 11, 14, 15, 17, 18, 20, 22.

148 Evidence of J. Iuso, Transcript, January 18, 2021, pp 65–66.

149 Evidence of M. Cox, Transcript, January 18, 2021, p 63.

on finding out what it had done wrong – but that FINTRAC had shifted toward a more collaborative approach. However, he finds that FINTRAC can be slow to respond to requests to clarify policy interpretations or rules.[150]

In Chapter 41, I recommend the creation of a provincial law enforcement unit dedicated to anti–money laundering. My hope is that this new unit will be able to avoid some of the pitfalls I have just described. In particular, as I expand in that chapter, I recommend that the new unit have a dedicated intelligence division and access to surveillance teams. The unit should also be responsible for developing tactical information-sharing initiatives with the private sector, which should include entities such as CMSBA and individual MSBs. Indeed, as I discuss next, I am recommending that BCFSA serve as a regulator for MSBs in this province, which will be well placed to engage with the new anti–money laundering unit.

A Provincial MSB Regulator

As I have noted throughout this chapter, the Province has been contemplating a potential provincial MSB regulator. This step was recommended by both Dr. Peter German and Professors Maloney, Unger, and Somerville.[151] The latter suggested that it would make sense for FICOM (now the British Columbia Financial Services Authority or BCFSA[152]) to operate the regulatory regime, noting that this solution would give BCFSA visibility over all the activities in the financial sector and would be less disruptive and costly than creating a new regulator.[153]

At the time of writing, Quebec is the only province that regulates MSBs. Under the Quebec *Money Services Businesses Act*,[154] MSBs are defined as businesses engaged in currency exchange; funds transfer; the issue or redemption of traveller's cheques, money orders, or bank drafts; cheque cashing; and the operation of ATMs.[155] All MSBs must hold a licence for the particular activities they are engaged in.[156] The Quebec Minister of Finance maintains a registry of all registered MSBs.[157]

When applying for a licence, an applicant must provide a variety of documents disclosing information about its legal structure, its agents, the financial institutions and lenders it deals with, a business plan, and government-issued identification for

150 Ibid, p 67. Mr. Iuso added that depending on the kind of question, FINTRAC can take 30 to 90 days to respond to requests by CMSBA: Transcript, January 18, 2021, pp 67–68.

151 Exhibit 832, Peter M. German, *Dirty Money: An Independent Review of Money Laundering in Lower Mainland Casinos Conducted for the Attorney General of British Columbia* (March 31, 2018), p 218, Recommendation 46; Exhibit 330, Maureen Maloney, Tsur Somerville, and Brigitte Unger, "Combatting Money Laundering in BC Real Estate," Expert Panel, March 31, 2019 [Maloney Report], pp 80–81.

152 I discuss BCFSA in more detail in Chapter 20.

153 Exhibit 330, Maloney Report, p 80.

154 *Money Services Businesses Act*, CQLR c E-12.000001.

155 Ibid, s 1.

156 Ibid, ss 3, 4.

157 Ibid, s 58.

key individuals.[158] Notably, these documents must include the name, date of birth, address, and phone number of each of the applicant's officers, directors or partners, and branch managers; any person or entity who directly or indirectly owns or controls the money services business; and each of the applicant's employees working in Quebec.[159] Applicants must also provide the same kind of information for any of their mandataries (the civil law equivalent of agents).[160] These requirements, which I will refer to as "business relationship" requirements, are essential in order to identify "straw" applicants and to prevent criminals from using "clean" operators to hold the MSB licence when they would not be eligible themselves.

Applications are sent to the provincial police force, the Sûreté du Québec, to conduct police checks.[161] MSBs can be refused registration for several reasons, including that they are "not of good moral character," are insolvent or bankrupt, have specified convictions, or have demonstrated a lack of compliance with the Act or other statutes.[162]

I pause here to note the significance of the "good moral character" provision, which states:

> A lack of good moral character is determined in light of such factors as the connections the persons or entities referred to in the first paragraph maintain with a criminal organization within the meaning of subsection 1 of section 467.1 of the *Criminal Code* (R.S.C. 1985, c. C-46) or with any other person or entity who engages in money laundering for criminal activities or in trafficking in a substance included in any of Schedules I to IV to the *Controlled Drugs and Substances Act* (S.C. 1996, c. 19). It is also determined in light of any other event of such a nature as to affect the validity of the licence or give the Minister cause to act under any of sections 11 to 17.[163]

It seems likely that such a provision would have led Silver International to be denied registration, or at least be further scrutinized prior to being registered. As noted above, applications in Quebec are sent to the Surêté du Québec for police checks. I expect that law enforcement would have serious concerns about registering an applicant at the centre of a large financial crime investigation and whose premises had recently been the target of search warrants that revealed large amounts of suspicious cash. I am not suggesting that any applicant that is being investigated should be denied registration as a matter of course. However, the Quebec approach allows for consideration of suspicious activity by an applicant that falls short of a criminal conviction, which differs from FINTRAC's current practice.

158 Ibid, s 6.

159 Ibid, s 6(1).

160 Ibid, s 6(2).

161 Ibid, ss 7–9.

162 Ibid, ss 11, 12, 14, 15, 23.

163 Ibid, s 23.

An applicant can also be refused registration under the Quebec regime if its business activities are not commensurate with its legal sources of financing, if a reasonable person would conclude that it is lending money to a business that would be unable to obtain a licence, or if its structure enables it to evade the Act or another fiscal law.[164]

Other aspects of the Quebec regime include that MSBs must verify the identity of their customers,[165] hold a bank account with a financial institution, keep specified records, and report transactions for which they have reasonable grounds to believe may constitute an offence under the Act.[166]

The Quebec Minister of Finance is authorized to enter into agreements with other governments and international organizations for the purpose of facilitating the administration or enforcement of the Act. Under such an agreement, the Minister may share personal information without the consent of the MSB if there are reasonable grounds to believe that the MSB (or an individual associated with it) has committed or is about to commit a criminal or penal offence.[167] The Minister can also apply to the provincial court for authorization to share information with the police for similar reasons.[168] The Act provides for monetary administrative penalties and penal provisions.[169]

The Government of British Columbia's consultation relating to MSB regulation revealed that CMSBA and medium-sized MSBs based in BC are generally not opposed to a provincial licensing regime for MSBs. However, they are concerned about increasing regulatory burdens on existing MSBs.[170] Mr. Iuso testified that he has heard from Quebec MSBs that some feel they are "put under a microscope" more than they need to be through, for example, mystery shoppers.[171] Mr. Cox noted that the Vancouver Bullion and Currency Exchange has decided not to operate in Quebec in part because of the licensing regime; however, he added that the extra regulatory burden could be lessened by aligning the provincial requirements with the *PCMLTFA* as much as possible.[172]

The consultation paper notes that FINTRAC provided seven "lessons learned" from working with the Quebec regime to address overlap:

164 Ibid, s 12.1.

165 The regulations explain the circumstances in which MSBs must verify a customer's identity, which are very similar to the situations set out in the *PCMLTFA*: see *Regulation under the Money-Services Businesses Act*, c E-12.000001, r 1, ss 7–12.

166 *Money Services Businesses Act*, ss 28–31. The Act explicitly says that an MSB will not incur civil liability as a result of reporting a suspicious transaction: ibid, s 31.

167 Ibid, ss 37–38.

168 Ibid, s 39.

169 Ibid, ss 65.1, 66–69.

170 Exhibit 311, BC Ministry of Finance, Briefing Document: Money Services Businesses Consultation – Summary (June 8, 2020), p 2; Evidence of J. Primeau, Transcript, December 1, 2020, p 137.

171 Evidence of J. Iuso, Transcript, January 18, 2021, pp 48–49.

172 Evidence of M. Cox, Transcript, January 18, 2021, pp 49–50.

1. Align a provincial MSB definition with FINTRAC's definition to reduce confusion/complexity.
2. Have similar timelines for same business processes ([e.g.,] licensing renewals).
3. Align eligibility criteria ([e.g.,] criminal/police records).
4. Licensing costs – FINTRAC does not charge fees (keep this in mind).
5. Have [a memorandum of understanding] for sharing information (the existing FINTRAC-[Financial Services Authority memorandum of understanding] would need to be expanded to include MSBs).
6. Registry should be similar and publicly available/searchable.
7. Avoid duplication of compliance activities/timing.[173]

The consultation also heard from Revenu Québec, which administers the Quebec regulatory regime. Notably, Revenu Québec stated that the regime's impact on the involvement of criminals in MSBs is likely small and that the identification and record-keeping requirements do not act as a disincentive to money laundering. Indeed, it has reason to suspect that MSBs continue to operate using nominees and the principal-agent model, despite the business relationship requirements. It has also found that the "good moral" principle is difficult to apply and can be challenged by MSBs. Further, obtaining a licence may actually facilitate money laundering or terrorist financing by giving MSBs an appearance of legitimacy. Revenu Québec also noted that the resources needed to investigate violations of the Act have so far been disproportionate to the results obtained, that ignorance of the law (for example, due to language barriers) has been an issue, and that law enforcement has so far made little use of the avenues available to it.[174]

CMSBA and mid-sized MSBs based in BC support the creation of a local specialized unit, possibly as part of the new regulator, that could effectively investigate, prosecute, and shut down unlicensed MSBs.[175] CMSBA noted during the consultation that MSBs that are newly registered with FINTRAC may operate for two years or more without a FINTRAC examination,[176] which is consistent with my discussion above. Accordingly, CMSBA strongly encouraged future provincial legislation to establish a way to confirm MSB compliance as soon as it becomes registered, noting that the Quebec regime has been successful in doing so.[177] Mr. Iuso has heard that although some MSBs have been displeased with random spot checks, "it seems like it's working [in] the sense that it's

173 Exhibit 311, BC Ministry of Finance, Briefing Document: Money Services Businesses Consultation – Summary (June 8, 2020), p 3.

174 Ibid, p 4.

175 Ibid, p 3.

176 Ibid; see also Evidence of J. Primeau, Transcript, December 1, 2020, p 130.

177 Exhibit 311, BC Ministry of Finance, Briefing Document: Money Services Businesses Consultation – Summary (June 8, 2020), p 4.

pushing them to be more available and ready for suspicious [customers] when they do come in."[178]

Revenu Québec and FINTRAC have a memorandum of understanding, pursuant to which FINTRAC shares the same kind of information with Revenu Québec that it does with BCFSA (see Chapter 20). It also works to reduce duplication and administrative burden by, for example, not examining MSBs that Revenu Québec is in the process of examining.[179] Ms. Achimov testified that this agreement with Revenu Québec has given FINTRAC some insight into unregistered MSBs. It is "a reliable source; it feeds our risk score and it allows us to do a cross-reference in terms of making sure that we're not missing any that are identified."[180] She added that the Quebec regime has an anti–money laundering "checklist" that is "also very instructive for us"[181] and noted that the licensing regimes are different in the sense that Quebec's licensing requirements have additional requirements beyond checking for criminal convictions.[182]

Joseph Primeau, acting executive director of the policy branch of the finance, real estate, and data analytics unit at the BC Ministry of Finance, testified that although the Ministry of Finance has not been able to measure or estimate the number of unregistered MSBs in this province, it has heard from law enforcement that unregistered activity presents risks.[183] He stated that a provincial regulatory regime would assist in understanding the size and composition of the sector.[184] The Ministry of Finance is considering the issue of MSBs operating out of locations such as private residences or post offices, which, Mr. Primeau noted, ties in to the difficulty of understanding the size and nature of the industry.[185] The Province would like to have a better understanding of the size and nature of the industry before imposing new requirements, in order to ensure that it understands the impact they will have on the industry.[186] The Province is also considering the potential for MSBs to be operating through nominees.[187]

In my view, the Province should regulate MSBs, and this regulation should be undertaken by BCFSA. This chapter has demonstrated that there are significant vulnerabilities associated with MSBs. Although MSBs are subject to the *PCMLTFA*, FINTRAC conducts relatively few compliance examinations in this sector. In my view, further scrutiny in this high-risk area is required. This is especially so with respect to new MSBs, given that FINTRAC conducts very few compliance examinations of

178 Evidence of J. Iuso, Transcript, January 18, 2021, p 47.
179 Evidence of D. Achimov, Transcript, January 18, 2021, pp 170, 177–78.
180 Ibid, pp 169–70.
181 Ibid, p 170.
182 Ibid, pp 179–80.
183 Evidence of J. Primeau, Transcript, December 1, 2020, pp 124–25.
184 Ibid, p 126.
185 Ibid, pp 132–33.
186 Ibid, p 134.
187 Ibid, pp 139–41.

MSBs in their first two years of existence. This leads to a real vulnerability in which individuals or entities can use MSBs for criminal purposes and stop operating (or re-register with different information) before the two-year mark, thereby evading a compliance examination. Further, as FINTRAC has taken the view that it can only deny registration when an individual or entity has a prior *conviction*, it remains possible – and has occurred, as demonstrated by the situation of Silver International – that an applicant who is currently under investigation (or even charged) but not *convicted* of an offence related to financial crime can nonetheless be registered. This is not to say that such circumstances should lead to a denial as a matter of course, but it strikes me that denial should be possible where appropriate.

As I discuss in Chapter 20, BCFSA is responsible for regulating various provincial institutions, including credit unions, insurance and trust companies, mortgages, pensions, and the Credit Union Deposit Insurance. BCFSA's supervision over these various sectors demonstrates that it has broad expertise in financial matters and would be well suited to adding MSBs to its purview. Further, expanding BCFSA's mandate in this way avoids the necessity to create another regulator and leverages BCFSA's experience in regulating financial entities. I am, however, mindful of the significance of expanding BCFSA's mandate in this way: the authority has already undergone various changes in its organizational structure in the past few years, and it will need to grapple with a sector that includes various unregistered and unknown actors. For this reason, I have recommended in Chapter 20 that the Province provide BCFSA with sufficient resources to create or staff a group focused on anti–money laundering specifically. It will be crucial that BCFSA have capacity – in terms of both financial and staff resources – to fulfill this new aspect of its mandate.

In extending BCFSA's mandate to cover MSBs, the Province will need to continue its consultations with Revenu Québec and FINTRAC. Consultations with the former will ensure that the Province is aware of hurdles that Revenu Québec – the sole MSB regulator in Canada at the time of writing – has encountered and to learn from its experiences. It will be particularly important to learn from Revenu Québec's difficulties regarding the "good moral character" provision and the business relationships requirements. These requirements strike me as sound in principle and should be included in British Columbia's regime; however, it will be important for the Province to learn from the challenges that Revenu Québec has had in enforcing these requirements in order to avoid such difficulties in British Columbia. Meanwhile, consultations with FINTRAC will help minimize duplication and burden for MSBs, which will need to comply with both the *PCMLTFA* and rules set out by BCFSA. A memorandum of understanding with FINTRAC (similar to that in place between FINTRAC and Revenu Québec) will be essential in this regard and should, among other things, set out how and when the two agencies will conduct their respective compliance examinations.

While the Province is best placed to determine all the functions that BCFSA will need for its regulation of MSBs, the regulatory scheme should include, at minimum:

- a definition of "MSB" that aligns with the definition in the *PCMLTFA*, except that virtual asset service providers should not be included at this stage;
- a capacity to identify unregistered MSBs and sanction them;
- a registration process in which the suitability of applicants is assessed in a broader manner than is done under the *PCMLTFA* (in particular, there should be an ability to deny registration for reasons apart from a criminal *conviction* and to require disclosure of business relationships in the same way as the Quebec regime);
- a compliance examination process that applies in the early years of an MSB's existence (that is, prior to the two-year mark);
- the ability to enter information-sharing arrangements with FINTRAC and other relevant entities; and
- administrative and monetary penalties.

As I explain in Chapter 35, I am not prepared to recommend, at this stage, that virtual asset service providers be brought under BCFSA's regulatory authority. Although I consider it essential that virtual asset service providers be subject to provincial regulation, I have recommended in Chapter 35 that the Province engage with the AML Commissioner proposed in Chapter 8, BCFSA, the British Columbia Securities Commission, industry members, and other stakeholders to determine which regulatory authority would be best suited to become the regulator of virtual asset service providers. If the Province determines that BCFSA is the appropriate regulator, it should ensure that BCFSA has sufficient resources and education to regulate a sector whose activities likely differ significantly from the financial institutions it currently oversees.

The registry of MSBs should be publicly accessible and similarly designed to the FINTRAC registry to ensure ease of use by the public, MSBs, and other reporting entities. The registration process should also be aligned as much as possible with the *PCMLTFA* regime, although it will, as noted, be important that ineligibility not be limited to criminal convictions.

I do not recommend at this stage that the regulatory scheme involve customer due diligence, record-keeping, and reporting measures in the same way as the Quebec regime for two reasons. First, as noted above, it appears that Revenu Québec expressed doubts in the Province's consultation on MSBs that these requirements were having any effect on deterring money laundering. Second, MSBs have these obligations already under the *PCMLTFA*, and I see no need to duplicate those measures at present. It may become apparent to BCFSA that such measures are desirable or necessary, in which case it should have a mechanism of communicating that view to the Province and obtaining the necessary regulatory authority.

Recommendation 51: I recommend that the Province expand the mandate of the British Columbia Financial Services Authority to encompass regulation of money services businesses. The regulatory scheme should include (but not be limited to) the following:

- a definition of "money services business" that aligns with the definition in the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (*PCMLTFA*), except that virtual asset service providers should not be included at this stage;
- a capacity to identify unregistered money services businesses and sanction them;
- a registration process in which the suitability of applicants is assessed in a broader manner than is done under the *PCMLTFA* to include consideration of whether a money services business has been investigated or charged with criminal activity, whether or not this has resulted in a conviction, as well as a requirement to disclose business relationships in the same way as the Quebec regime;
- a compliance examination process that applies in the early years of a money services business's existence;
- the ability to enter information-sharing arrangements with the Financial Transactions and Reports Analysis Centre of Canada and other relevant entities; and
- the availability of administrative and monetary penalties.

Mr. Primeau testified that the Province is considering the possibility of a whistle-blower line.[188] This is in response to suggestions by CMSBA and mid-sized MSBs during the Province's consultation that there should be a dedicated "whistle-blower" line that could be used to anonymously report unregistered MSBs.[189] As these discussions appear to be in their early stages, I am not prepared to make a recommendation that such a line should be created at present. However, in the course of expanding BCFSA's mandate, the Province should consult with BCFSA about how it can best become alerted to non-compliant MSBs.

Conclusion

In this chapter, I have outlined the significant money laundering risks that arise in the MSB sector, while also noting that there are many legitimate uses and users of these

188 Evidence of J. Primeau, Transcript, December 1, 2020, pp 139–41.

189 Exhibit 311, BC Ministry of Finance, Briefing Document: Money Services Businesses Consultation – Summary (June 8, 2020), p 3.

services. In my view, the risks in this sector are such that the Province should regulate MSBs and that this responsibility should fall to BCFSA. It will be essential for BCFSA to have the resources it needs to engage in this activity, which will increase its workload substantially. It will also be important for the AML Commissioner to monitor the implementation and progress of this regulation.

Chapter 22
White-Label Automated Teller Machines

I have just discussed the risks inherent to banks and credit unions, and the well-known risks in the money services business sector. A lesser-known sector is that of white-label automated teller machines (white-label ATMs). Simply put, these are ATMs that are not owned by banks, and indeed are sometimes called "non-bank ATMs."[1] They can be found in locations such as bars, restaurants, convenience stores, gas stations, and grocery stores.[2]

There was debate in the evidence before me on the question of whether white-label ATMs pose a money laundering risk. They are not subject to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, SC 2000, c 17 (*PCMLTFA*) and therefore have no reporting or other obligations under that regime. However, white-label ATMs depend on accessing the Interac network to operate and are subject to Interac's rules, many of which resemble obligations under the *PCMLTFA*. I heard from industry members that white-label ATMs are an ineffective method of laundering money and that the Interac rules are sufficient to guard against any risks. Conversely, I heard from RCMP witnesses that white-label ATMs pose significant money laundering risks.

In this chapter, I first discuss in more detail what white-label ATMs are and how they operate. I then describe the Interac network and how white-label ATMs use that network to conduct their business. I then turn to the more contentious aspect of this chapter: the question of whether white-label ATMs pose a money laundering risk. Finally, I consider whether additional regulation in this sector is desirable.

1 Evidence of C. Chandler, Transcript, January 15, 2021, p 117.

2 Ibid, p 118.

What Are White-Label ATMs?

White-label ATMs are cash machines that are not owned by traditional financial institutions. The industry started around 1996 following challenges before the federal Competition Bureau to the banks' use of the ATM network. In two decisions, the Competition Bureau found that major financial institutions' practices with respect to ATMs were monopolistic and exclusive, and allowed a surcharge to be made on ATM transactions.[3] Following those decisions, the number of ATMs in Canada grew significantly – from an estimated 18,426 in 1996 to 55,562 in 2007 (a 202 percent increase). Much of this growth was due to the new white-label ATM industry.[4]

Any individual can own or operate a white-label ATM. Christopher Chandler, president of the ATM Industry Association, testified that there are around 50,000 ATMs in Canada, of which approximately two-thirds are white-label ATMs.[5] He highlighted that whereas many bank ATMs are grouped together at a bank branch, white-label ATMs are often not; he estimates that there are approximately 34,000 white-label ATM cash access points compared to 7,000 bank access points. As a result, white-label ATMs make up around 80 percent of all cash access points in Canada.[6]

In 2020, there were 4,912 white-label ATMs in British Columbia on the Interac network. Mr. Chandler testified that we can safely assume that all or almost all of those white-label ATMs are connected to the Interac network, given that it is the leading ATM network in Canada.[7]

White-label ATMs are essentially products for merchants. Merchants can own their white-label ATMs or use the services of an independent sales organization to run the machines.[8] Depending on the arrangement, a white-label ATM can be loaded with cash by the merchant itself, by an independent sales organization, or by a cash-loading business.[9]

White-label ATMs can serve three purposes for a merchant:

- They can draw customers into the store.
- They can give cash in hand to customers while they are in the store, which they will hopefully spend.
- Merchants can generate revenue from the ATM because they typically receive a share of the fees charged to the customer.[10]

3 Exhibit 429, RCMP Criminal Intelligence Project Scot, "An Assessment of Money Laundering Activities and Organized Crime Involvement Within the 'White Label' ATM Industry," November 10, 2008 [RCMP Project Scot Report], p 5.

4 Ibid.

5 Evidence of C. Chandler, Transcript, January 15, 2021, p 117.

6 Ibid, pp 117–18.

7 Ibid, pp 119, 121.

8 Exhibit 429, RCMP Project Scot Report, p 18.

9 Evidence of C. Chandler, Transcript, January 15, 2021, pp 133–34.

10 Ibid, pp 118–119.

Indeed, fees are the primary source of income for white-label ATM owners. Fees associated with these machines include regular transaction fees, which are charged by the customer's financial institution; network access fees, which are paid when accessing an ATM other than one owned by the customer's financial institution; and convenience fees, which are charged by the white-label ATM operator and can be charged by other financial institutions to non-customers.[11]

The Interac Network

Interac is the organization responsible for the development and operation of "shared cash dispensing" at ATMs and for Interac Payment Direct, the leading debit service in Canada.[12] Interac's "Inter-Member Network" links financial institutions and "direct" and "indirect connectors."[13] Direct connectors – almost all of which are deposit-taking financial institutions – can connect directly to the network to provide ATM and debit services.[14] Indirect connectors access the network through a direct connector.[15]

White-label ATMs connect to the network through an "acquirer" (a third-party processor and/or indirect connector) and a financial institution (a direct connector).[16] Acquirers have direct relationships with Interac and maintain responsibility for satisfying Interac's rules. Kirkland Morris, vice-president of enterprise initiatives and external affairs at Interac, testified that the idea is to "apply scrutiny up the chain."[17] Settlement agents clear financial obligations of other members through the Canadian Payments Association's Automated Clearing Settlement System.[18] Independent sales organizations have contractual relationships with acquirers to market or sell services on their behalf.[19] Finally, sub-independent sales organizations may be involved: they maintain contractual relationships with independent sales organizations to market or provide services on their behalf.[20]

To understand how a white-label ATM operates, it is useful to consider how a typical ATM transaction works (that is, a customer using an ATM belonging to the customer's bank), and then to compare it to transactions using ATMs owned by other financial institutions and white-label ATMs.

11 Exhibit 429, RCMP Project Scot Report, p 19.

12 Exhibit 430, WLTM Brief – Department of Finance (March 5, 2020), p 1.

13 Exhibit 429, RCMP Project Scot Report, p 6; Evidence of C. Chandler, Transcript, January 15, 2021, pp 123–24; Evidence of K. Morris, Transcript, January 15, 2021, p 125.

14 Exhibit 429, RCMP Project Scot Report, p 6; Evidence of K. Morris, Transcript, January 15, 2021, pp 125–26; Exhibit 430, WLTM Brief – Department of Finance (March 5, 2020), p 2.

15 Exhibit 429, RCMP Project Scot Report, p 6; Evidence of K. Morris, Transcript, January 15, 2021, pp 126–27.

16 Exhibit 430, WLTM Brief – Department of Finance (March 5, 2020), p 2.

17 Evidence of K. Morris, Transcript, January 15, 2021, pp 127–28.

18 Exhibit 429, RCMP Project Scot Report, p 7.

19 Ibid, p 16. Mr. Chandler explained that independent sales organizations find merchant locations, install the ATMs, service them, and gather information such as know-your-client information and source-of-funds declarations: Evidence of C. Chandler, Transcript, January 15, 2021, pp 128–29.

20 Exhibit 429, RCMP Project Scot Report, p 17.

Beginning with a typical ATM transaction, we can imagine a customer who banks with the Royal Bank of Canada (RBC) and uses an RBC ATM.[21] The customer places their card in the ATM and makes a request for withdrawal. RBC verifies that the funds requested are available in the customer's bank account. The transaction is validated and approved, and the approval is sent to the ATM. The cash is then dispensed.[22] In this scenario, Interac's Inter-Member Network has *not* come into the mix because the customer is using their own bank.[23] Depending on the account, there may be no fee or a small service fee to RBC in this example.

Let us assume now that the RBC customer uses an ATM owned by the National Bank of Canada (National Bank).[24] The customer places their card into a National Bank ATM and makes a request for withdrawal. A request for approval is made through Interac's Inter-Member Network to RBC, which then verifies that the funds are available in the customer's account. Once RBC verifies and approves the transaction, that approval is sent through the Inter-Member Network back to the ATM. The transaction is then settled through the Canadian Payment Association's Automated Clearing Settlement System, and the funds are credited to National Bank's account. A debit memo is then posted to the customer's account, and the customer receives the cash.[25] The customer often faces an additional charge for this sort of transaction on a different bank's ATM.

Finally, let us assume that the RBC customer uses a white-label ATM. The customer puts their card into the ATM. This time, the request for approval must go through an independent sales organization and the indirect connector to the Inter-Member Network. There may also be other actors involved, such as a sub-independent sales organization. Once the transaction enters the Inter-Member Network, the process proceeds as above: RBC approves the transaction and communicates the approval to the white-label ATM through the Inter-Member Network. The transaction is settled, debited to the customer's account, and credited to the white-label ATM owner's account.[26] The customer will pay a fee that goes to the white-label ATM operator for this transaction.

"Regulation" of White-Label ATMs

Mr. Chandler testified that white-label ATMs are subject to two forms of "regulation": they must settle to a single bank account, and they must comply with Interac's rules.[27] Indeed, witnesses before me frequently referred to the "regulation" done by Interac. In my view, it is more accurate to speak of Interac's *rules*, as Interac is not a regulator;

21 See ibid, p 14, for a diagram of this scenario.

22 Exhibit 429, RCMP Project Scot Report, p 14.

23 Ibid, p 14.

24 See ibid, p 16, for a diagram of this scenario.

25 Ibid, p 15.

26 Ibid, pp 16–17.

27 Evidence of C. Chandler, Transcript, January 15, 2021, pp 132, 183.

rather, it is a private, for-profit (though highly regarded) body that services a network. In any event, Interac's rules are relevant and worth reviewing.

Interac's Rules for White-Label ATMs

Interac's rules – called the "Requirements for White Label ABM Cash Owners"[28] – were adopted in March 2009 at the request of the federal Department of Finance. This in turn followed commentary in the Financial Action Task Force's third mutual evaluation of Canada in 2008, which identified the white-label ATM sector as a potential source of money laundering risk and recommended strengthening controls.[29] The mutual evaluation noted that white-label ATMs were a high-risk area not covered by the *PCMLTFA*, that the RCMP had observed their use by organized crime groups, and that a 2007 FINTRAC report had highlighted the vulnerability of these ATMs to money laundering.[30] The fourth mutual evaluation report similarly found that white-label ATMs were a high-risk area not covered by the regime and recommended that Canada "[s]trengthen policies and strategies to address emerging [money laundering] risks (in particular white-label ATMs and online casinos)."[31]

Mr. Morris testified that the federal government appeared to favour an industry-led solution rather than a public policy or regulatory response.[32] It appears, however, that the RCMP would have preferred white-label ATMs to be subject to the *PCMLTFA* and required to register as money services businesses.[33] The rules were finalized following discussions between Interac, Visa, Mastercard, the ATM Industry Association, the RCMP, the Ontario Provincial Police, the Department of Finance, FINTRAC, and industry.[34]

The rules address four areas:

- customer due diligence (know-your-client requirements);
- source of funds;
- criminal background checks; and
- annual reviews to monitor compliance.[35]

28 Exhibit 434, Interac – Overview WLCO Regs (2020). Note that white-label ATMs are sometimes referred to as white-label ABMs, short for "automated banking machines" rather than "automated teller machines."

29 Evidence of K. Morris, Transcript, January 15, 2021, p 174; Exhibit 434, Interac – Overview WLCO Regs (2020), p 1; Exhibit 4, Overview Report: Financial Action Task Force, Appendix L, FATF, *Third Mutual Evaluation on Anti–Money Laundering and Combating the Financing of Terrorism, Canada* (Paris: FATF, 2008), p 247, para 1379.

30 Exhibit 4, Overview Report: Financial Action Task Force, Appendix L, FATF, *Third Mutual Evaluation on Anti–Money Laundering and Combating the Financing of Terrorism, Canada* (Paris: FATF, 2008), pp 5, 16, 115–16.

31 Exhibit 4, Overview Report: Financial Action Task Force, Appendix N, FATF, *Anti–Money Laundering and Counter-Terrorist Financing Measures – Canada, Fourth Round Mutual Evaluation Report* (Paris: FATF, 2016), p 31.

32 Evidence of K. Morris, Transcript, January 15, 2021, p 174.

33 Exhibit 429, RCMP Project Scot Report, p 12.

34 Exhibit 434, Interac – Overview WLCO Regs (2020), p 3; Evidence of K. Morris, Transcript, January 15, 2021, pp 174–75.

35 Exhibit 434, Interac – Overview WLCO Regs (2020), p 3; Evidence of K. Morris, Transcript, January 15, 2021, p 175.

Acquirers are responsible for verifying the identity of white-label ATM cash owners and obtaining source-of-funds documents for any white-label ATM they connect to the network.[36] "Cash owners" are defined as those persons or entities that own or possess the cash that is loaded into the ATM or own the account through which the ATM funds are settled.[37] The source-of-funds declaration must be maintained with each white-label ATM cash owner's documentation and must be updated when changes occur.[38] Interac verifies the identity of each prospective acquirer and conducts background checks on key personnel, including directors and officers.[39]

The rules classify cash owners as low risk or high risk. Cash owners are considered low risk if they:

- supply cash to a single ATM;
- supply cash to between two and four ATMs with a daily average settlement not exceeding $5,000 in the aggregate;
- are a publicly traded company;
- have a provincial or federal gaming certificate; or
- are a public body.[40]

Cash owners that do not qualify as one of the above are considered high risk. Criminal record checks are required for all high-risk cash owners. If the cash owner is not an individual, a criminal record check must be obtained for all individuals who own or control over 25 percent of the entity, or for individuals with signing authority.[41] At the time of the Commission's hearings, there were 84 high-risk cash owners in BC.[42]

Mr. Morris agreed that a cash owner could still be considered low risk even if they supply substantial amounts of cash to one ATM. Similarly, an entity or individual could have a combined settlement value of just under $5,000 a day for up to four ATMs, totalling around $1.8 million per year, and still be considered low risk.[43]

Acquirers are responsible for ensuring that reviews by a qualified auditor are conducted for each cash owner they connect to the Interac network.[44] The auditor ensures that the proper documentation is being collected and the rules are being followed. They must also report non-compliance or suspicions of criminal activity to Interac, so that the

36 Exhibit 434, Interac – Overview WLCO Regs (2020), p 3.
37 Ibid, pp 3–4.
38 Evidence of K. Morris, Transcript, January 15, 2021, p 176.
39 Exhibit 434, Interac – Overview WLCO Regs (2020), p 3.
40 Evidence of K. Morris, Transcript, January 15, 2021, pp 176–77.
41 Ibid, pp 176–78.
42 Exhibit 435; Evidence of K. Morris, Transcript, January 15, 2021, p 181.
43 Ibid, p 182.
44 Exhibit 434, Interac – Overview WLCO Regs (2020), p 9.

latter can take steps to refer the matter to authorities where appropriate. Mr. Morris is not aware, however, of an auditor uncovering any criminal activity since Interac's rules have been in effect or of any referrals relating to money laundering.[45]

The most extreme "sanction" that Interac can impose for failure to comply with its rules is disconnecting the ATM from the network. Mr. Morris testified that Interac would disconnect a user if it was aware of any money laundering or suspected money laundering activity or other criminal activity. However, he is not aware of any white-label ATM being disconnected for non-compliance or of any referrals being made to law enforcement.[46]

Interac's Investigation Unit

In addition to its rules, Interac has an investigation unit that deals with payment fraud and financial crime. This unit is meant to act as a liaison between Interac and stakeholders such as financial institutions and law enforcement.[47] It was implemented to enhance the flow of information between Interac and law enforcement and to provide a point of contact for the latter for assistance in its investigations.[48]

Mr. Morris believes that the unit has existed since approximately 2008.[49] Its primary activities relate to the prevention, detection, management, and ongoing investigation of payment card fraud.[50] It supports law enforcement directly and through the fulfillment of court orders, and also works with financial institutions and law enforcement to prevent, detect, and manage fraud and related activity.[51] Interac also provides education to the law enforcement community on the means of identifying and detecting criminal activity in the payment space and works with law enforcement on community messaging.[52]

To Mr. Morris's knowledge, the investigation unit has never received a request for information from Interac relating to potential money laundering or proceeds-of-crime investigations involving white-label ATMs.[53] It is unclear whether the lack of referrals by Interac, or inquiries from law enforcement, stems from a lack of money laundering activity through white-label ATMs or from other factors such as the generally low numbers of investigations into money laundering in this province and the difficulties in obtaining convictions (see Part XI). Whatever the reason for the low referral numbers, I elaborate on the *risks* in this sector below.

45 Evidence of K. Morris, Transcript, January 15, 2021, pp 178, 184.

46 Ibid, pp 184–85.

47 Ibid, p 186.

48 Exhibit 430, WLTM Brief – Department of Finance (March 5, 2020), p 2.

49 Evidence of K. Morris, Transcript, January 15, 2021, p 188.

50 Ibid, p 186.

51 Ibid, pp 186–87. Mr. Morris explained that Interac typically requires a production order to share information with law enforcement, though it has some participation agreements that address information sharing with law enforcement, government, and regulatory authorities: ibid, p 193.

52 Ibid, p 187.

53 Ibid, p 188.

Other Codes and Standards

White-label ATMs are subject to other codes and standards apart from the Interac rules. The Standards Council of Canada has a voluntary code of standards applying to ATMs, which covers the construction and security performance and seeks to provide protection against the unauthorized removal of currency.[54] The Office of Consumer Affairs also has a voluntary code of practice for consumer debit card services, which outlines industry practices and consumer and industry responsibilities.[55] Finally, the Canadian Payments Association's rules address information protection and verification requirements during the encryption and decryption of PINs.[56] Although it is good that white-label ATMs are subject to these standards, I note that none of them appear to address anti–money laundering.

Money Laundering Risks

There was dispute in the evidence before me on the question of whether white-label ATMs pose money laundering risks and, if so, how significant they are.

The RCMP takes the view that there are significant risks. An RCMP project known as "Criminal Intelligence Project Scot"[57] focused on white-label ATMs and resulted in a November 2008 intelligence report.[58] Melanie Paddon, a former sergeant at the RCMP and an investigator with the Joint Illegal Gaming Investigation Team, testified that this is the most recent RCMP report on white-label ATMs of which she is aware.[59] I note that this report precedes the adoption of Interac's rules in 2009.[60]

Some key conclusions from the report include the following:

- Lack of government regulation in the white-label ATM industry has "allowed it to grow at unprecedented levels and be used by organized crime to launder proceeds of crime and commit other crimes."[61]
- Organized crime groups including the Hells Angels Motorcycle Club have infiltrated the white-label ATM industry at levels close to 5 percent of the sector (or possibly higher). This could grow to 20 percent of all white-label ATMs.[62]

54 Exhibit 430, WLTM Brief – Department of Finance (March 5, 2020), p 1.

55 Ibid.

56 Ibid.

57 Project Scot was "intended to establish the nature and scope of the 'white label' ATM industry in Canada and to assess the current situation, demonstrate the potential vulnerabilities of criminal activities, specifically money laundering, and to identify criminal organizations operating within the industry": Exhibit 429, p 4. Its name is inspired by the inventor of ATMs, Scot John Shepherd-Barron: ibid, p 4, footnote 3.

58 Exhibit 429, RCMP Project Scot Report.

59 Evidence of M. Paddon, Transcript, January 15, 2021, p 139.

60 The report is dated November 10, 2008, while the rules were adopted in March 2009: Evidence of K. Morris, Transcript, January 15, 2021, p 174.

61 Exhibit 429, RCMP Project Scot Report, p 1.

62 Ibid, pp 1, 3.

- Outlaw motorcycle gangs have laundered money through white-label ATMs since the late 1990s in several provinces, including British Columbia.[63]
- There are reports of proceeds of crime from drug trafficking, loan sharking, illegal gaming operations, prostitution, and other crimes being laundered through white-label ATMs.[64]
- "The potential amount that could be laundered through the 'white label' ATM industry is approximately $315 million and could easily reach $1 billion annually."[65]

The report calls for a registry and monitoring system to address the fact that white-label ATMs are not subject to the *PCMLTFA*.[66] It also lists the following major concerns relating to white-label ATMs:

- Anyone can own or operate a white-label ATM.
- There are few due diligence requirements.
- Owners can load cash into the machine themselves.
- Owners are asked on a one-time basis to identify the source of their funds.
- White-label ATMs are not subject to any government regulation.[67]

The report further notes that white-label ATMs are not subject to the federal *Bank Act* and are therefore not regulated by the Office of the Superintendent of Financial Institutions.[68]

As I understand it, the concerns about money laundering through white-label ATMs are as follows. The white-label ATM can be loaded with illicit cash, in whole or in part. When customers withdraw cash from the white-label ATM, they may or may not be aware that some or all of the cash is illicit. As the white-label ATM facilitates a withdrawal from a financial institution, that transaction is later settled and the money that was withdrawn is ultimately sent to the bank account associated with the white-label ATM. In this way, the white-label ATM has provided illicit cash to customers and the cash owner receives "clean" money from the financial institution through the settling process.[69]

The RCMP's 2008 report notes that using a white-label ATM can skip the "placement" stage of money laundering because money loaded into the machine is electronically

63 Ibid, pp 3, 30.

64 Ibid, p 1.

65 Ibid. These figures were arrived at by considering institutions known to be used by organized crime groups to launder money and assumes that they would be making monthly withdrawals of $15,000 and monthly disbursements of $60,000 to $80,000: ibid, p 29.

66 Ibid, p 1.

67 Ibid, pp 2, 5.

68 Ibid, p 2.

69 Ibid, p 27.

deposited into the bank account associated with it.[70] Further, use of a white-label ATM avoids face-to-face contact with employees of the financial sector who could detect suspected activities and fulfill know-your-client requirements.[71] Sergeant Paddon explained that illicit and legitimate funds can be intermingled, thereby complicating police investigations. She added that, because of the lack of government regulation or oversight, criminal organizations can continue their activity without having to report to FINTRAC or elsewhere.[72] The RCMP report further notes that use of white-label ATMs can circumvent cross-border currency and electronic funds transfer requirements because:

- funds can be wired to offshore accounts and then sent back as a cheque, which can then be deposited in Canada;
- white-label ATMs can be linked to a foreign bank account and avoid the $10,000 reporting threshold, given that the activity is usually less than that;
- use of a white-label ATM can avoid the involvement of cash couriers; and
- cash deposited in Canada can be accessed anywhere in the world through ATM networks, which essentially allows for international transfer of money into local currency and circumvention of currency import and export restrictions.[73]

Other issues involve the possibility of counterfeit bills being loaded into machines, skimming operations (in which a white-label ATM skims information from a credit card or a person's bank account information), tax evasion, and fraud.[74] Sergeant Paddon added that because white-label ATMs are not regulated, law enforcement relies on its partners (including FINTRAC and financial institutions) to flag issues for it.[75]

A briefing note from the federal Department of Finance dated March 5, 2020, discusses money laundering and terrorist financing risks relating to white-label ATMs.[76] It notes that some observed money laundering and terrorist financing risks include:

- that an ATM can be loaded with illicit cash without the owner's knowledge;
- that a business owner involved in criminal activity or with connections to organized crime can load an ATM with illicit cash; and
- that a company can be created that purportedly owns or operates white-label ATMs, but can be used as a cover for criminal activities, given that these are cash-based businesses.[77]

70 Ibid, pp 2, 25; Evidence of M. Paddon, Transcript, January 15, 2021, pp 139–40.
71 Exhibit 429, RCMP Project Scot Report, pp 2, 25; Evidence of M. Paddon, Transcript, January 15, 2021, p 140.
72 Evidence of M. Paddon, Transcript, January 15, 2021, pp 140–41.
73 Exhibit 429, RCMP Project Scot Report, p 27.
74 Ibid, pp 5, 24–25; Evidence of M. Paddon, Transcript, January 15, 2021, pp 142–43.
75 Evidence of M. Paddon, Transcript, January 15, 2021, p 142.
76 Exhibit 430, WLTM Brief – Department of Finance (March 5, 2020).
77 Ibid, pp 2–3.

The briefing note concludes that there are money laundering vulnerabilities in the white-label ATM sector. It also expresses concerns about the ownership structure, in the sense that Interac may not be aware of owners and operators, who rely on and interface with direct and indirect connectors.[78] It emphasizes, however, that the risks do not relate to *withdrawals* by clients:

> The money laundering vulnerability does not lie with the clients withdrawing funds from the WLATMs [white-label ATMs]. Authorized third parties, independent of the ATM cash owner, record and retain information about every dollar that passes through a WLATM in Canada. The information recorded by third parties includes a transaction record number, the amount withdrawn, the date and time of the withdrawal and the Canadian bank account to which the funds withdrawn are electronically settled. *There are no WLATM withdrawals and settlements of any amount, at any time, that are anonymous*. Independent third parties clearly record and retain the details of the money flow. *The WLATM vulnerability lies in the loading of the machines, which can be done anonymously*. Companies owning and loading WLATMs for themselves or other legitimate businesses may be criminally controlled. Criminals can offer ATM services within different legitimate businesses or set them up in their own businesses, and load those ATMs with illicit cash. [Emphasis added.][79]

Like the RCMP report, the briefing note highlights the unregulated nature of the industry and the lack of oversight, which can "provide organized crime a favourable environment to use ATMs to conduct various illegal activities, including money laundering, fraud and distribution of counterfeit money."[80]

I heard a very different account of the money laundering risks in this sector from industry witnesses. Mr. Chandler emphasized that there is no evidence that people are actually laundering money through white-label ATMs. He notes that there have been only a handful of cases since 1996, which does not line up with the RCMP report's estimate of the activity reaching $300 million to $1 billion per year.[81] He added that white-label ATMs need to comply not only with Interac's rules but also with BC Gaming Commission regulations (where the ATM is located in a casino).[82]

Mr. Chandler argues that there has been undue focus on white-label ATMs. He testified that business owners can get cash into a bank account by depositing it through:

- a bank deposit-taking ATM;
- a bank night depository;

78 Ibid, p 3.
79 Ibid, p 4.
80 Ibid, p 4.
81 Evidence of C. Chandler, Transcript, January 15, 2021, pp 160–61.
82 Ibid, p 161.

- a bank teller; or
- a white-label ATM.[83]

In Mr. Chandler's view, the first two options are just as anonymous as a white-label ATM.[84] Further, while the first three options accept any quality and denomination of cash, white-label ATMs accept only "ATM-quality" cash – flat, undamaged $20 bills.[85] He added that the first three options could involve deposits into multiple bank accounts; in contrast, white-label ATMs can be associated with only one account and must satisfy that bank's know-your-client requirements.[86] Another distinction is that the first three options require large cash transaction reports and source-of-funds declarations for transactions of $10,000 or more; in contrast, white-label ATMs must fill out source-of-funds declarations for transactions of $5,000 or more, as well as provide a background check if they operate multiple white-label ATMs.[87] Finally, Mr. Chandler pointed out that transactions through an ATM are tracked and recorded by third-party processors, whose records are provided to the Interac Association, audited annually, and made available to law enforcement upon request.[88]

A position paper prepared by the ATM Industry Association expresses the view that exaggerating the risks in the white-label ATM sector is harmful to small businesses and causes unnecessary doubts for customers about the safe, reliable, and convenient access to cash that white-label ATMs provide.[89] It opines that media stories about the risks associated with these ATMs are based on anecdotal evidence only, and notes that the one case where a conviction was obtained – the *Banayos* case, reviewed below – is the only one since 1996 that has involved a conviction.[90] On this point, Sergeant Paddon testified that she is aware of investigations involving white-label ATMs that have not resulted in a charge or conviction, noting that it is difficult to obtain money laundering convictions.[91] Mr. Chandler responded that this singles out the white-label ATM industry when other industries also involve investigations that do not result in charges.[92]

I was referred to one case in which the owner of a white-label ATM was found to be involved in money laundering: the *Banayos* case.[93] I note at the outset that my discussion of this case is reliant on the findings of the Manitoba courts, and I make no findings of my own. The case was the culmination of a Winnipeg Police Service

83 Ibid, p 135.
84 Ibid, pp 163–64.
85 Ibid, pp 164–65.
86 Ibid, pp 164, 166.
87 Ibid, pp 165–67.
88 Ibid, p 167.
89 Exhibit 432, Actual versus Perceived Risks of Money Laundering at White-Label ATMs in Canada (2017), p 5.
90 Ibid, pp 7, 9.
91 Evidence of M. Paddon, Transcript, January 15, 2021, pp 169–70.
92 Evidence of C. Chandler, Transcript, January 15, 2021, pp 170–71.
93 *R v Banayos and Banayos*, 2017 MBQB 114, aff'd 2018 MBCA 86, leave to SCC denied 38296.

investigation called "Project Sideshow" that took place from early 2012 until February 2014.[94] It involved a sister and brother who were charged with money laundering (among other things). The trial judge found that Mr. Banayos was operating a drug trafficking business and an ATM business involving several ATMs.[95] Although Mr. Banayos operated the ATM business, Ms. Banayos was listed as the owner and operator because of the requirement to obtain a criminal record check.[96] She indicated on her source-of-funds declaration that the cash used to load the ATM would come from her RBC bank account. However, the trial judge determined that in at least two instances – when the sister's account balance was $0 and when the account was frozen – the cash could not have come from the RBC account.[97] Given those circumstances, as well as others, the trial judge concluded that the cash used to load the ATM had come from the brother's drug trafficking business, which was done in furtherance of a money laundering scheme.

Mr. Chandler expressed the view that the *Banayos* case shows that money laundering through ATMs is not an effective method:

> [T]his case kind of supports what we've been saying … [M]y understanding of this case is they started money laundering and within six months and about $100,000 if that recollection is correct, they were caught and the documentation was there to convict them. And that has been our premise from the beginning. This is not a smart place to money launder because you will get caught, likely quickly and you will certainly have a high chance of being convicted. So this [case] supported that.[98]

Conversely, Sergeant Paddon testified that she has come across a number of files that involved white-label ATMs. Although the ATM may not have been the main focus of the cases, "often organized crime groups would use white-label ATMs to launder their funds."[99] She added that money laundering convictions are very difficult to obtain; therefore, while many cases involve white-label ATMs, they do not all result in charges.[100]

On the evidence before me, I am unable to arrive at conclusions on how frequently white-label ATMs are used to launder money. Clearly, it is possible to do so, as illustrated by the *Banayos* case. It also appears, from Sergeant Paddon's testimony, that the potential for using white-label ATMs to launder money is on law enforcement's radar, though it is less clear how often the ATMs are a main focus of such investigations. While I accept that there is a risk of white-label ATMs being used to launder money, I am unable to determine whether that risk is significant or greater

94 *R v Banayos and Banayos*, 2017 MBQB 114 at para 1.

95 *R v Banayos and Banayos*, 2018 MBCA 86 at para 10.

96 Ibid, para 17(b).

97 Ibid, paras 17(b), 35–37.

98 Evidence of C. Chandler, Transcript, January 15, 2021, p 213.

99 Evidence of M. Paddon, Transcript, January 15, 2021, p 158.

100 Ibid, pp 169–70.

than that attaching to various other forms of money laundering, or whether white-label ATMs have actually been exploited to a significant degree. In fact, the various rules applying to white-label ATMs – including that cash owners must settle with a single bank account, are subject to audits, are required to comply with various know-your-client obligations, and must load machines with ATM-quality cash – would seem to lessen the risks significantly. Indeed, the fact that cash owners are required to settle with a single bank account suggests that FINTRAC has at least some visibility into the activities of white-label ATMs, as financial institutions have obligations under the *PCMLTFA* in respect of those accounts.

It is also striking that despite the RCMP estimating, in 2008, that money laundering through white-label ATMs could "easily reach $1 billion annually,"[101] it appears that only one case has resulted in convictions for money laundering. Moreover, given that law enforcement has never made use of Interac's investigation unit in relation to potential money laundering or proceeds-of-crime investigations, it is impossible to know if inquiries by law enforcement would have established some suspicious activity, significant amounts, or none. I expect that, in future, law enforcement will make use of the unit when it has suspicions involving white-label ATMs.

The foregoing is *not* a conclusion that that no money laundering is occurring through white-label ATMs in this province. Rather, there has been insufficient use of investigative avenues to determine if such activity is occurring. In the absence of such investigative activity, I am unable to draw conclusions about the extent to which white-label ATMs have been used to launder money in British Columbia. Below, I discuss the role that the AML Commissioner recommended in Chapter 8 and new intelligence and investigation unit recommended in Chapter 41 might play in gaining further insight into money laundering risks and activity in this area.

Should White-Label ATMs Be Subject to Provincial Regulation?

In line with the debate surrounding money laundering risks associated with white-label ATMs, I heard differing views about whether white-label ATMs should be subject to regulation under the *PCMLTFA*, a provincial scheme, or both. As I explained above, white-label ATMs are not currently subject to the *PCMLTFA*, nor are they caught by the federal *Bank Act*. As a result, the only "regulation" to which they are subject is Interac's rules and the requirement that they be associated with only one bank account. They therefore have no reporting obligations, nor are cash owners required to implement a compliance program as they would be under the *PCMLTFA* regime. While the Interac regime does involve periodic audits of white-label ATM owners, it is not clear that these are equivalent to compliance exams conducted by FINTRAC, nor the kind of regulation that a provincial regulator could undertake. Further, the only "sanctions" to which white-label ATMs can be subject under the Interac regime

101 Exhibit 429, RCMP Project Scot Report , p 1.

is a loss of their ability to access the network. This is in contrast to penalties available under regulatory regimes, which typically include fines and loss of a licence.

The exception in this country is Quebec. As I discuss in Chapter 21, white-label ATMs are deemed to be money services businesses in that province and are therefore captured by the Quebec *Money Services Businesses Act,* CLQR c E-12.000001. I will not repeat all the aspects of that regime here (discussed in detail in Chapter 21), except to note that it involves provincial licensing; police checks; and requirements relating to customer identification, record-keeping, and reporting. The scheme also provides for administrative monetary fines and penal provisions.

The Financial Action Task Force's third mutual evaluation of Canada in 2008 concluded that the measures in place at that time (which pre-dated the Interac rules) did not adequately address the risks in the white-label ATM sector. It suggested that Canada consider a registration and monitoring system for owners of white-label ATMs.[102] Similarly, the fourth mutual evaluation in 2016 noted that all high-risk areas were covered by the *PCMLTFA* regime "with the notable exception of … white-label ATMs."[103] In the evaluators' opinion, white-label ATMs were vulnerable to money laundering and terrorist financing, referencing the RCMP's view that they are used by organized crime to launder proceeds of crime.[104] The report recommended that Canada "[s]trengthen policies and strategies to address emerging [money laundering] risks (in particular white label ATMs …)."[105]

Canada's 2015 national risk assessment noted that although white-label ATMs were excluded from the *PCMLTFA*, Canada would continue to assess the money laundering and terrorist financing risks associated with them.[106] A 2018 report of the House of Commons Standing Committee on Finance recommended that the white-label ATM sector be included in the *PCMLTFA* regime.[107]

British Columbia is considering the possibility of regulating white-label ATMs.[108] Joseph Primeau, acting executive director of the policy branch of the finance, real estate, and data analytics unit at the BC Ministry of Finance, testified that the Province is considering engaging an external expert to assess the money laundering risk associated with white-label ATMs.[109] He hopes that such a consultation would shed some light on the question of whether it is efficient to launder money through white-label ATMs, and added that the Province would like to clarify what happens in networks other than Interac.[110]

102 Exhibit 4, Overview Report: Financial Action Task Force, Appendix L, FATF, *Third Mutual Evaluation on Anti–Money Laundering and Combating the Financing of Terrorism, Canada* (Paris: FATF, 2008), p 245, para 1364.

103 Exhibit 4, Overview Report: Financial Action Task Force, Appendix N, FATF, *Anti–Money Laundering and Counter-Terrorist Financing Measures – Canada, Fourth Round Mutual Evaluation Report* (Paris: FATF, 2016), p 5, para 16.

104 Ibid, p 16, para 53.

105 Ibid, p 31.

106 Exhibit 3, Overview Report: Documents Created by Canada, Appendix B, Department of Finance, *Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada 2015* (Ottawa, 2015), p 32, Recommendation 7.

107 Exhibit 436, Confronting Money Laundering and Terrorist Financing – Standing Committee Report, p 30.

108 Exhibit 311, BC Ministry of Finance, Briefing Document: Money Services Businesses Consultation – Summary (June 8, 2020), pp 5–6.

109 Evidence of J. Primeau, Transcript, December 1, 2020, pp 142–43.

110 Ibid, pp 144–45.

Sergeant Paddon testified that, in her view, a registry of white-label ATM owners would be helpful in gathering intelligence and uncovering beneficial owners, overseas corporations, real estate assets, and bank accounts. It would also be useful for sharing information with partners, such as FINTRAC and the Canada Revenue Agency. However, she opined that it would likely be more effective for FINTRAC to be the central monitoring system rather than a provincial regulator.[111] The BC Ministry of Finance consultation on money services businesses (see Chapter 21) noted that the RCMP considers white-label ATMs to be vulnerable to money laundering because of the little or no oversight; believes that reporting by banks about white-label ATMs can be avoided by cash owners; is aware of money laundering activities through white-label ATMs based on specific cases and intelligence research; and considers that a regulatory regime would assist with investigations, which are challenging.[112]

According to the consultation paper, Revenu Québec expressed the view that "it is unclear whether the regime is working, although it certainly makes it more difficult to launder money; however, [white-label ATM] regulation does pose [a] volume problem with sprawling investigations with complex structures."[113]

The consultation paper equally notes, however, that the ATM Industry Association emphasized the rigour of Interac's rules, that white-label ATMs are an inefficient way to launder money, and that Quebec's regime is onerous on businesses.[114] Indeed, Mr. Chandler and the ATM Industry Association are strongly opposed to additional regulation. In Mr. Chandler's view, the Quebec regime is "wholly redundant with the Interac regulations" and in some ways, Interac's rules are more extensive than the *PCMLTFA*.[115] He testified that the Quebec regulator has had "extreme difficulties" implementing the legislation, noting that the regulator's difficulties locating ATM operators have led to "scandalous headlines" accusing operators of being untoward when there was no wrongdoing.[116] Further, he considers that operators are "persecut[ed] by association" when they may be associated with bad actors but are not bad actors themselves.[117]

Mr. Chandler believes that white-label ATMs were brought into the Quebec regime based on the RCMP's 2008 report, which he emphasized he had never seen before the Commission's hearing despite making requests.[118] The ATM Industry Association has unsuccessfully tried to persuade the Quebec government to remove white-label ATMs from the regime.[119] Mr. Chandler opined that further regulation would lead to half of all white-label ATMs leaving the marketplace because of the increased burden.[120] Overall,

111 Evidence of M. Paddon, Transcript, January 15, 2021, pp 206–9.

112 Exhibit 311, BC Ministry of Finance, Briefing Document: Money Services Businesses Consultation – Summary (June 8, 2020), p 6.

113 Ibid.

114 Ibid, p 5.

115 Evidence of C. Chandler, Transcript, January 15, 2021, pp 190, 199.

116 Ibid, pp 190–91.

117 Ibid, p 191.

118 Ibid, pp 194–95.

119 Ibid.

120 Ibid, pp 136–37.

he says that white-label ATMs are meeting a high standard through the Interac rules, that there is already a significant burden on small business owners, and that further regulation is not justified given the little evidence of money laundering in this sector.[121]

In my view, there are enough uncertainties with respect to white-label ATMs that the Province should not, as this time, subject them to regulation. Instead, the AML Commissioner proposed in Chapter 8 should study the money laundering risks attaching to white-label ATMs.

I arrive at this conclusion for several reasons. First, as I discussed above, the money laundering risks associated with white-label ATMs are not especially clear. While I accept that it can happen (and has, as demonstrated by the *Banayos* case), it is not obvious how widespread the problem is. Second, there are suggestions in the evidence that the Quebec regime is not seen as particularly effective as it relates to white-label ATMs. Before beginning what could be a costly process of identifying all white-label ATMs in the province and ensuring they are licensed, I believe it would be useful to first study the problem further. In this regard, the Province should continue to engage with Quebec to learn from its experiences. Third, it is striking that law enforcement has never made use of Interac's investigative unit to request documents or other information about suspected money laundering involving white-label ATMs. Before implementing a likely costly regulatory solution, the avenues that are currently available should be used. I would encourage the designated provincial money laundering intelligence and investigation unit recommended in Chapter 41 to explore and make use of information and intelligence available from Interac. Finally, it may be that regulation of white-label ATMs would be more appropriate at the federal level by subjecting them to the *PCMLTFA*, as Sergeant Paddon suggested. The Province should engage with the federal government to determine if this possibility is being explored.

Conclusion

This chapter has examined the white-label ATM sector and the money laundering risks that arise within it. Although one can intuitively describe risks that arise with white-label ATMs, the state of the evidence and the level of investigation by law enforcement are such that I am unable to draw firm conclusions about the extent of money laundering that is actually occurring through white-label ATMs. It will be important for the AML Commissioner to study this area and report to the Province on his or her findings. I also encourage the designated provincial money laundering intelligence and investigation unit recommended in Chapter 41 to be alive to the money laundering risks associated with white-label ATMs and to leverage intelligence available through Interac to further investigations in this area where appropriate. While I do not propose, at this time, that white-label ATMs be subject to provincial regulation, it may be that the AML Commissioner's further study reveals that such regulation would be desirable.

121 Ibid, pp 199–201.