Part X
The Underground Economy

Much of what I have discussed in this Report focuses on the legitimate economy – money laundering that occurs in the context of legitimate business sectors and takes advantage of regulatory gaps or a lack of understanding. However, money laundering occurs in the informal or "underground" economy as well, in the sense that it takes place outside the regulated financial system and may not be caught by countermeasures put in place by countries that have adopted the Financial Action Task Force model.

In Chapter 36, I discuss bulk cash smuggling, which, as its name suggests, involves physically transporting large quantities of cash across international borders. Chapter 37 considers informal value transfer systems, which allow for the transfer of *value* from one location to another without actually transferring *funds*. Finally, in Chapter 38, I examine trade-based money laundering, in which individuals abuse trade transactions to avoid the scrutiny of more direct forms of transfer and to move illicit funds (or more accurately, *value*) from one location to another. I have chosen to address trade-based money laundering in Part X because it is another way of moving value outside of the regulated financial system and is sometimes used in conjunction with informal value transfer systems.

Chapter 36
Bulk Cash Smuggling

Bulk cash smuggling is an important part of the underground economy. It is often thought of as the oldest and most basic form of money laundering – however, it still occurs frequently today.[1]

As the name suggests, bulk cash smuggling refers to the practice of moving large quantities of cash (that is, physical dollars or euros or other banknotes) across international borders. As I explain below, the Financial Action Task Force (FATF) has urged member countries, through its 40 recommendations, to require declarations or disclosure by travellers transporting cash over a certain threshold. With that in mind, another way of conceiving of bulk cash smuggling is as the "transfer of cash across the border in violation of currency reporting requirements, that is, above the permitted maximum threshold and without justification."[2]

The money laundering risks associated with bulk cash smuggling are self-evident. Given that much criminal activity continues to occur primarily in cash[3] and that it is increasingly difficult to conduct all of one's transactions in cash, criminals need to find ways to move large quantities of cash back into the legitimate economy. This often involves transporting the cash to another jurisdiction. Simon Lord, a senior officer with the UK's National Crime Agency and one of the world's leading experts on money laundering, explained the criminal's dilemma as follows:

1 Exhibit 4, Overview Report: Financial Action Task Force, Appendix LL, *FATF Report: Money Laundering Through the Physical Transportation of Cash* (October 2015) [*FATF Bulk Cash Report*], p 3; Evidence of J. Gibbons, Transcript, December 10, 2020, p 18.

2 Exhibit 24, Michele Riccardi and Michael Levi, "Cash, Crime and Anti–Money Laundering," in Colin King, Clive Walker and Jimmy Gurulé (eds), *The Palgrave Handbook of Criminal and Terrorism Financing Law* (Cham: Palgrave Macmillan, 2018), p 143.

3 Evidence of S. Lord, Transcript, May 29, 2020, p 5; Evidence of J. Sharman, Transcript, May 6, 2021, pp 15–16.

> [C]ash is still the raw material of most criminal activity – certainly all of the commodity-based crime that you can think of, so drug trafficking, robbery, smuggling cigarettes … even things like the trafficking of human beings, modern slavery, and all the rest of it.
>
> … [A]ll that type of crime generates cash. And so, criminals have to find something to do with the cash that they have made in part with their criminal activities. And cash actually, when you see it in large amounts, the thing that strikes you about it is just how big and heavy it is … it ceases almost to become money, but becomes a commodity in its own right. And so, what that means is, in order to sort of enjoy the fruits of your ill-gotten gains, you've got to try and find something to do with it. And in most western societies now, and certainly anybody who sort of complies with the [Financial Action Task Force's] 40 recommendations, it's actually extremely difficult to get rid of large amounts of cash now.
>
> So, one of the ways in which people deal with their cash is to move it away from the jurisdiction where it is, where maybe you can't get it into the banking system, and move it somewhere else … either to break the audit trail in between the possession of the cash and the commission of the crime, or … move it to a jurisdiction where you can bank it much more easily … And so physically moving the cash across borders is something that's on the up.[4]

In this chapter, I first review the regulation applicable to transportation of cash across international borders. In this area, the province of British Columbia is heavily reliant on the federal government, which is responsible for international trade, imports, exports, and national borders. I then discuss the continued prevalence of cash in the legitimate economy, despite the rise of alternative payment methods such as credit cards. Finally, I examine the role of cash in the criminal economy, ways in which it is smuggled across borders, and difficulties in detecting this activity.

Legal and Regulatory Framework

The transportation of cash across borders is addressed by both the FATF's 40 recommendations and domestically in the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, SC 2000, c 17 (*PCMLTFA*).

FATF Recommendation 32

FATF has addressed the movement of cash across international borders in Recommendation 32, titled "Cash Couriers," which states:

4 Evidence of S. Lord, Transcript, May 29, 2020, pp 5–6.

> Countries should have measures in place to detect the physical cross-border transportation of currency and bearer negotiable instruments,[5] including through a declaration system and/or disclosure system.
>
> Countries should ensure that their competent authorities have the legal authority to stop or restrain currency or bearer negotiable instruments that are suspected to be related to terrorist financing, money laundering or predicate offences, or that are falsely declared or disclosed.
>
> Countries should ensure that effective, proportionate and dissuasive sanctions are available to deal with persons who make false declaration(s) or disclosure(s). In cases where the currency or bearer negotiable instruments are related to terrorist financing, money laundering or predicate offences, countries should also adopt measures, including legislative ones consistent with Recommendation 4,[6] which would enable the confiscation of such currency or instruments.[7]

The interpretive note to Recommendation 32 expands on the obligations set out above.[8] I highlight a few points from it. First, Recommendation 32 is meant to ensure that countries can:

- detect physical cross-border transportation of currency and bearer negotiable instruments;
- stop or restrain currency and bearer negotiable instruments that are suspected to be related to terrorist financing or money laundering;
- stop or restrain currency or bearer negotiable instruments that are falsely declared or disclosed;
- apply appropriate sanctions for making a false declaration or disclosure; and

5 A "bearer instrument" is a type of instrument that requires no ownership information to be recorded: Exhibit 64, Europol Financial Intelligence Group, *Why Is Cash Still King? A Strategic Report on the Use of Cash by Criminal Groups as a Facilitator for Money Laundering* (European Police Office, 2015) [*Europol Cash Report*], p 51. The FATF recommendations define "bearer negotiable instrument" as including monetary instruments such as traveller's cheques; negotiable instruments (such as cheques, promissory notes, and money orders) that are in bearer form, endorsed without restriction, made out to a fictitious payee, or in some other form that allows title to pass upon delivery; and incomplete instruments that are signed but omit the payee's name: 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) [*FATF Recommendations*], p 113, general glossary.

6 Recommendation 4 refers to the confiscation of proceeds of crime and related measures: Exhibit 4, Appendix E, *FATF Recommendations*, p 10, Recommendation 4.

7 Ibid, p 23, Recommendation 32.

8 Ibid, pp 102–5, interpretive note to Recommendation 32.

- enable confiscation of currency or bearer negotiable instruments that are related to terrorist financing or money laundering.[9]

"Physical cross-border transportation" is defined to include:

- physical transportation by a natural person or in their accompanying luggage or vehicle;
- shipment of currency or bearer negotiable instruments through containerized cargo; and
- mailing of currency or bearer negotiable instruments by a natural or legal person.[10]

Countries can meet their obligations under Recommendation 32 by implementing either a declaration or disclosure system. A **declaration system** should require all persons transporting over 15,000 US dollars or euros to submit a truthful declaration (written, oral, or a combination of the two) to competent authorities.[11] Meanwhile, a **disclosure system** should require travellers to provide appropriate information to authorities upon request.[12] Whether the country adopts a declaration or disclosure system, the information should be available to the financial intelligence unit, and authorities should be able to stop or restrain cash when it is suspected to be connected to money laundering, terrorist financing, or a false declaration or disclosure.[13] There should also be effective, proportionate, and dissuasive sanctions for false declarations or disclosures, and authorities should be able to confiscate cash related to money laundering, terrorist financing, or a predicate offence.[14]

A 2015 FATF report entitled *Money Laundering Through the Physical Transportation of Cash* found that the methods of implementing Recommendation 32 varied considerably among the countries surveyed.[15] For example, some countries required cash declarations to be checked for accuracy by actually counting the cash; other countries said this was done only occasionally.[16] Further, some countries kept statistics on the amount of cash transported, while others did not.[17] The report also found that there was little collaboration between neighbouring countries in developing their systems, which led to significant incongruences.[18]

9 Ibid, p 102, para 1.
10 Ibid, p 105.
11 Ibid, p 102, para 3.
12 Ibid, p 103, para 4.
13 Ibid, para 5.
14 Ibid, p 104, para 6.
15 Exhibit 4, Appendix LL, *FATF Bulk Cash Report*, pp 15, 60–61.
16 Ibid, p 15.
17 Ibid.
18 Ibid, pp 15–16.

The *PCMLTFA*

Canada has implemented the requirements of Recommendation 32 in Part II of the *PCMLTFA* and the *Cross-Border Currency and Monetary Instruments Reporting Regulations*, SOR/2002-412 (*Currency Regulations*). The Canada Border Services Agency (CBSA) is responsible for administering the cross-border currency reporting regime.[19]

Travellers carrying, importing, or exporting $10,000 or more across Canada's borders must declare those funds to CBSA officers using one or more currency reporting forms.[20] CBSA shares all completed currency reporting forms with FINTRAC for further analysis.[21] It also gathers and analyzes intelligence in order to detect contraband and provide intelligence on travellers or transportation of funds that portray indicators of illicit activity.[22]

CBSA officers can search persons or vehicles when they have reasonable grounds to suspect that a person has concealed or failed to declare funds of $10,000 or more.[23] They can seize those funds if they have reasonable grounds to believe a person has concealed or failed to declare funds of $10,000 or more.[24] Officers are also empowered to open international mail where they have reasonable grounds to suspect that it contains $10,000 or more of undeclared funds, and they can seize the funds.[25]

Where a CBSA officer has seized undeclared funds, the latter will be forfeited if the officer has reasonable grounds to suspect that they are proceeds of crime or for use in the financing of terrorist activities.[26] This is referred to as a "Level 4 seizure."[27] Where the officer does not have reasonable grounds to suspect that funds are illicit, the funds will be returned upon payment of a penalty of $250 (a "Level 1 seizure"), $2,500 ("Level 2 seizure"), or $5,000 ("Level 3 seizure") depending on the circumstances of the concealment.[28]

Table 36.1 provides a summary of the number and total value of seizures of undeclared funds in British Columbia between 2016 and 2020:

19 Exhibit 1000, Affidavit #1 of Sara D'Ambrogio, affirmed May 3, 2021 [D'Ambrogio Affidavit], paras 7, 16–25.

20 *PCMLTFA*, s 12; *Currency Regulations*, s 2.

21 Exhibit 1000, D'Ambrogio Affidavit, paras 29–30.

22 Ibid, para 10.

23 *PCMLTFA*, ss 15, 16; Exhibit 1000, D'Ambrogio Affidavit, para 27.

24 *PCMLTFA*, s 18(1); *Currency Regulations*, s 18; Exhibit 1000, D'Ambrogio Affidavit, paras 31–37.

25 *PCMLTFA*, ss 17, 18(1); *Currency Regulations*, s 18; Exhibit 1000, D'Ambrogio Affidavit, paras 28, 31–37.

26 *PCMLTFA*, s 18(2); Exhibit 1000, D'Ambrogio Affidavit, paras 37, 40.

27 Closing submissions, Government of Canada, para 65.

28 *PCMLTFA*, s 18(1); *Currency Regulations*, s 18; Exhibit 1000, D'Ambrogio Affidavit, paras 33–36. The individual from whom the funds were seized or the lawful owner of the funds can request a review of the seizure and/or fine imposed: *PCMLTFA*, ss 24–35.

Table 36.1: Number and value of undeclared funds seizures in BC, 2016–2020

	2016		2017		2018		2019		2020	
	#	$	#	$	#	$	#	$	#	$
Level 1	597	9,190,847	496	7,511,148	564	8,637,316	365	5,459,126	103	1,551,367
Level 2	74	1,588,271	60	1,370,590	68	1,540,858	40	858,817	8	157,565
Level 3	NIL	NIL	2	148,734	NIL	NIL	3	30,049	NIL	NIL
Level 4	47	926,878	50	771,527	48	1,006,079	57	973,455	16	207,367

Source: Closing submissions, Government of Canada, para 66.

The total value of funds that were reported entering or leaving Canada through BC ports of entry between 2016 and 2020 are as follows:

- $1,380,679,435.88 (2016)
- $1,463,351,600 (2017)
- $1,879,120,057.97 (2018)
- $923,734,249.37 (2019)
- $161,761,260.26 (2020)[29]

FATF's 2016 mutual evaluation of Canada rated Canada as largely compliant with Recommendation 32, noting a few minor deficiencies.[30] The evaluators noted that the penalty provisions in the *PCMLTFA* – the fact that Level 1, 2, and 3 seizures of cash must be returned to the individual upon payment of a penalty of $250, $2,500, or $5,000 – was not proportionate or dissuasive for undeclared or falsely declared cash over the threshold.[31] Cambridge Professor Jason Sharman described this result as a "forgiving policy of often returning undeclared cash to those detected carrying it in through the border, with very small penalties. To an outsider, this policy seems like an incredible favour to international money launderers."[32] Given that penalties are low, these may seem to a criminal to be simply a cost of doing business, payable only in the event they are caught.[33] However, as I noted above, funds will be forfeited under the Canadian regime where a CBSA officer has

29 Exhibit 990, Affidavit #1 of Annette Ryan, affirmed April 27, 2021, para 8; Exhibit 991, Exhibit A to Affidavit #1 of Annette Ryan – FINTRAC CBCR Reports Data.

30 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 189–91.

31 Ibid, p 190.

32 Exhibit 959, Jason Sharman, *Report to the Cullen Commission: Money Laundering and Foreign Corruption Proceeds in British Columbia: A Comparative International Policy Assessment*, p 2; see also Evidence of J. Sharman, Transcript, May 6, 2021, pp 17–18.

33 Evidence of J. Sharman, Transcript, May 6, 2021, p 18.

reasonable grounds to suspect that they are proceeds of crime or for use in the financing of terrorist activities.[34]

A 2018 report by the federal Department of Finance acknowledges that Canada's penalties are low and advises that it is "revising the penalty structure is under consideration."[35] The report also notes some differences between the Canadian penalties and other countries:

- Some countries, such as Spain, impose a blanket minimum penalty over double the Canadian minimum of $250.
- In Australia, the minimum penalty varies based on the value of the currency that was not declared.
- In the United States, all currency may be seized and forfeited when there is a false or no declaration by assessing a penalty equal to the amount not declared.[36]

I expect that Canada will consider the view of the FATF evaluators and ensure that the fines under the *PCMLTFA* are proportionate and dissuasive.

Legitimate Cross-Border Transfer of Cash

It is important to emphasize that people transport cash across borders every day, and much of this activity is legitimate. It is not, in itself, illegal to transport cash. Movement of cash across borders *becomes* unlawful once it is not declared when required. In addition, bulk cash smuggling does not, in itself, necessarily constitute money laundering, though it is often a required step in the money laundering process.[37]

Despite increasing use of non-cash payment methods, cash "remains an important means of settlement across the globe, with an estimated USD 4 trillion in circulation and between 46% and 82% of all transactions in all countries being conducted in cash."[38] The FATF report notes that some 2 billion adults in the world today do not have access to banking services, which means that cash is the only form of payment they can rely on day to day. Indeed, the economies of many of the world's poorest and least developed countries rely on cash.[39]

34 *PCMLTFA*, s 18(2); Exhibit 1000, D'Ambrogio Affidavit, paras 37, 40.

35 Exhibit 960, Department of Finance, *Reviewing Canada's Anti–Money Laundering and Anti-Terrorist Financing Regime* (February 7, 2018), p 38.

36 Ibid.

37 Canada's 2015 national risk assessment noted that bulk cash smuggling is frequently used, including by professional money launderers and organized crime groups, as the first step in the money laundering process: 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), pp 21, 25, 42.

38 Exhibit 4, Appendix LL, *FATF Bulk Cash Report*, pp 3, 11.

39 Ibid, p 8.

That said, cash is also prevalent in many of the world's largest and wealthiest economies. Some reasons for a preference for cash include:

- **Cultural preference:** some cultures may prefer to use cash because of a distrust of governments and large financial institutions.
- **Retailer preference:** some retailers prefer cash for low-value transactions because it avoids processing fees.
- **Speed:** unlike transactions through the banking system that can take days, weeks, or months to clear, cash transactions occur immediately.
- **Reduction of spending:** people who purchase goods and services with cash tend to spend less than those who use credit or debit.
- **Reduction of debt:** using cash can help reduce indebtedness by limiting the individual to spending what they actually possess.
- **Discounts:** in some countries, it is possible to negotiate a lower price when paying in cash because the merchant can avoid paying fees for processing credit, debit, or cheque transactions.
- **Avoiding interest and fees:** using cash avoids paying interest and fees that would be charged for credit balances or bank accounts.
- **Dependable in a crisis:** cash is dependable in the event that a financial institution's operations are affected by a crisis or otherwise.
- **Store of value:** cash is often used to store wealth in volatile economies or jurisdictions threatened by war or natural disaster (including foreign currencies that are perceived to be more stable than the local one).[40]

However, cash also has some disadvantages:

- Large amounts are heavy and bulky.
- Large amounts are vulnerable to theft.
- Cash hoarding can restrict wealth, as the individual collecting the cash loses access to currency markets and investments and does not earn interest.
- Cash reduces purchasing options, given that it cannot be used for certain goods or in large amounts due to anti–money laundering regulations.
- To make a remote payment using cash, the cash needs to be physically transported.
- It can be costly to count and process cash.

40 Ibid, p 9.

- Using cash can restrict access to other financial services because, by deliberately choosing to transact in cash, an individual does not build a financial profile that is needed to save, invest earnings, or apply for loans, insurance, and the like.[41]

The FATF report found that although legitimate cross-border transportation of cash is common, it is not well understood by many countries both in terms of the methods and extent. This in turn hinders the ability of customs officials to determine if a shipment is legitimate or not.[42] A 2015 report by the European Police Office (Europol) Financial Intelligence Group similarly notes that there is little, if any, concrete data available on the legitimate use of cash beyond figures relating to the volume and value of bank notes issued and in circulation. As a result, much is unknown about the legitimate use of cash, although observations on consumer patterns show that cash continues to be the preferred method of payment for low-value purchases.[43]

The Europol report notes that, despite the steady growth of non-cash payment methods and a decline in the use of cash, the total number of euro banknotes in circulation continues to rise beyond the rate of inflation year after year. It states that cash is used mostly for low-value payments, and its use for transaction purposes is estimated to account for approximately one-third of bank notes in circulation. Yet, the demand for high-denomination notes that are not commonly associated with payments (for example, the 500-euro note) has been sustained. This apparent contradiction is likely explained by criminal activity.[44] High-value banknotes are not convenient for the average shopper, but they are highly convenient for money laundering and cash smuggling, as they can substantially reduce the size and weight of the funds and make them easier to transport.

Capital Flight

At various points of this Report, I have referred to "capital flight," which has been defined as "a large scale exodus of financial assets and capital from a nation due to events such as political or economic instability, currency devaluation or the imposition of capital controls."[45] The last factor (imposition of capital controls) refers to situations where a state places restrictions on the amount of cash that can legally be exported, by whom, and for what purpose.[46] The main "driver" for capital flight is that funds are perceived to be under threat for some reason (for example, avoidance of strict exchange controls, an illicit source, or cultural considerations), which causes the owner to want to move the funds abroad to a place of safety.[47]

41 Ibid, pp 9–10.
42 Ibid, pp 13–14.
43 Exhibit 64, *Europol Cash Report,* pp 6, 11.
44 Ibid, pp 6, 11–16.
45 Exhibit 4, Appendix LL, *FATF Bulk Cash Report,* p 36.
46 Ibid, p 15.
47 Ibid, p 36.

Capital flight is, in a sense, in a grey zone between legitimate and illegitimate transfer of cash. The capital being moved in such a situation is often *not* derived from criminal activity. However, according to the FATF report, anecdotal evidence suggests that the capital may sometimes be derived from tax fraud or other illicit activity.[48]

Criminal Cross-Border Transportation of Cash

As I noted above, there is a disconnect between the fact that cash use is generally on the decline and yet circulation of cash, particularly high-denomination notes, is on the rise. The Europol report posits that this disparity is due at least in part to criminal activity.[49] In this section, I discuss the prevalence of cash in criminal activity, methods in which it is smuggled across borders, and difficulties in detecting such activity.

Why Do Criminals Rely on Cash?

Despite the rise of non-cash payment methods, cash continues to be "the raw material of most criminal activity."[50] Professor Sharman testified that people often assume cash laundering is no longer relevant or common, given that "cash is something of the oldest and crudest way of money laundering" and that anti–money laundering policies have been in place for almost 30 years. But in his view, that assumption is wrong: "cash is probably still one of the most important mechanisms for laundering the proceeds of crime."[51] He added that while cash is perhaps more common in low-value crimes,

> even very recently, even in jurisdictions that have had anti–money laundering laws for 30 years, there are still cases of drug dealers coming to banks with bags of millions of dollars in cash and being able to deposit that over the counter repeatedly and not being detected through this most unsubtle and unsophisticated style of money laundering.[52]

In other words, money launderers "don't innovate when they don't have to. If old ways still work, then there's not much incentive to go with new ways."[53] As cash is still effective for many forms of criminality, it continues to be used.[54]

Most suspicious transaction reports in Europe relate to cash or cash smuggling.[55] Suspicious cash is also a problem in Canada, as indicated in a 2018 report prepared by the federal Department of Finance:

48 Ibid, p 36.

49 Exhibit 64, *Europol Cash Report,* pp 6, 11–16.

50 Evidence of S. Lord, Transcript, May 29, 2020, p 5.

51 Evidence of J. Sharman, Transcript, May 6, 2021, p 15.

52 Ibid, pp 15–16.

53 Ibid, p 16.

54 Ibid, p 16.

55 Exhibit 24, M. Riccardi and M. Levi, "Cash, Crime and Anti–Money Laundering," p 135; Exhibit 64, *Europol Cash Report,* pp 7, 16.

> In Canada, there are criminal networks across the country that are responsible for the processing of hundreds of millions of proceeds of crime in cash. These transactions are often observed by law enforcement in public places as bags or boxes of cash are exchanged. Those who are providing cash in these situations have links to criminal organizations and criminal activity and do not otherwise have legitimate reasons for possessing these amounts in cash. However, the use of multiple cash transfers, the recourse to professional money movers, and the placement of cash in the financial system often make it difficult for law enforcement to establish the link between the cash and the commission of a specific criminal offence.[56]

Cash remains attractive for criminals today because it is relatively untraceable, readily exchangeable, and anonymous.[57] However, the FATF report notes that cash is only truly anonymous in smaller amounts; it is easier to justify small to medium amounts of cash, but harder to justify the possession or movement of large amounts of cash with no explanation of its origin or purpose.[58]

Cash plays a role at all three of the traditional "stages" of money laundering (see Chapter 2 for a discussion of the three-stage model and critiques of it). As the Europol report notes, "Although not all use of cash is criminal, all criminals use cash at some stage in the money laundering process."[59] Cash can be generated in any number of predicate offences, including drug trafficking, illegal trafficking of commodities (such as alcohol or tobacco), tax fraud, weapons and arms smuggling, organized immigration fraud, or the financing of terrorism. The FATF report concludes that there is seemingly no predicate offence that is more commonly associated with one method of cash smuggling.[60]

Cash smuggling often begins the money laundering cycle:

> Criminals who generate cash proceeds seek to aggregate and move these profits from their source, either to repatriate funds or to move them to locations where one has easier access to placement in the legal economy, perhaps due to the predominant use of cash in some jurisdictions'

56 Exhibit 960, Department of Finance, *Reviewing Canada's Anti–Money Laundering and Anti–Terrorist Financing Regime* (February 7, 2018), p 36.

57 Exhibit 33, Her Majesty's Treasury and Home Office, *UK National Risk Assessment of Money Laundering and Terrorist Financing* (October 2015), p 75, para 8.2; Exhibit 24, M. Riccardi and M. Levi, "Cash, Crime and Anti–Money Laundering," p 135; Exhibit 64, *Europol Cash Report*, p 9; Exhibit 4, Appendix LL, *FATF Bulk Cash Report*, p 27.

58 Exhibit 4, Appendix LL, *FATF Bulk Cash Report*, p 27.

59 Exhibit 64, *Europol Cash Report*, p 7.

60 Exhibit 4, Appendix LL, *FATF Bulk Cash Report*, pp 3, 30–31. Riccardi and Levi note that most European anti–money laundering units report drug trafficking as the predicate offence most closely linked to the use of cash in money laundering schemes; however, other crimes (such as extortion, sexual exploitation, and smuggling of migrants) are likely to generate cash proceeds as well. Corruption (e.g., through bribes) is the second predicate offence most frequently reported by law enforcement agencies: Exhibit 24, M. Riccardi and M. Levi, "Cash, Crime and Anti–Money Laundering," pp 141–42.

> economies, more lax supervision of the financial system or stronger banking secrecy regulations, or because they may have greater influence in the economic and political establishment.[61]

Cash smuggling can also occur at other stages of the money laundering cycle. Moreover, it is also used by non-cash generating offences: for example, criminals engaged in cybercrime such as phishing or hacking make use of money mules to receive and withdraw funds fraudulently obtained and then send the funds by wire transfer to other jurisdictions where they are then collected in cash, likely for onward transportation.[62]

Smuggling Cash Across Borders

A key finding of the FATF report was that the more countries impose restrictions on the use of cash, the more people start to smuggle it across borders.[63] Although there are no reliable estimates on the amount of cash laundered through smuggling cash across borders and then introducing it into the financial system in another country, the figure "would seem to be between hundreds of billions and a trillion US dollars per year."[64]

Other key findings in the FATF report include the following:

- Physical transportation of cash distances criminal proceeds from the predicate offence and breaks the audit trail.[65]
- The amounts of cash being concealed in cargo and adapted freight are in excess of what can be carried by a natural person.[66]
- The currencies most frequently encountered in consignments of criminal cash are those that are the most stable, widely used, and readily traded in the world.[67]
- While not universally seen, high-denomination notes are often used to reduce the bulk and weight of criminal cash when seeking to conceal it.[68]
- Criminals exploit cash declaration systems, including by:
    - using the fact that cash has been declared on entry as a way of legitimizing criminal cash paid into a bank account;

61 Exhibit 64, *Europol Cash Report,* p 18.
62 Ibid, p 18.
63 Evidence of S. Lord, Transcript, May 29, 2020, p 6; Exhibit 4, Appendix LL, *FATF Bulk Cash Report,* pp 27–29.
64 Exhibit 4, Appendix LL, *FATF Bulk Cash Report,* pp 3, 31–32.
65 Ibid, p 4.
66 Ibid.
67 Ibid.
68 Ibid.

  - reusing cash declarations several times for the same purpose; or
  - over-declaring cash on entry.[69]

- Although most countries seem to have reasonable knowledge and understanding of cash transported by natural persons (and measures in place to monitor and control this activity), much less attention is paid to money being moved by cargo.[70]

While a review of the entire FATF report is beyond the scope of this chapter, it is worth examining some of these findings in more detail.

Breaking the Audit Trail

A key driver of moving criminally derived cash from one jurisdiction to another is to break the audit trail – in other words, make it difficult for authorities in the second jurisdiction to establish that the cash is the proceeds of a crime in the first jurisdiction.[71] Relatedly, criminals may choose to move cash to a jurisdiction with less stringent anti–money laundering regulation, such that they can introduce large amounts of cash into the financial sector without attracting scrutiny.[72]

The Europol report notes that the most significant challenge reported by law enforcement in regard to cash is linking it to criminal activity. It explains that "[m]ost European law enforcement agencies are required to demonstrate the predicate offence in order to prosecute money laundering: given that cash is a bearer instrument, this is a challenging task, and successful investigations involving cash usually entail the use of traditional techniques."[73] Although difficulties in linking predicate offences to money laundering is not limited to cash, "the inability to trace physical cash money movements intensifies the problem when compared to other instruments for which records are kept."[74]

As I discuss in Chapter 40, the need to establish the predicate offence has also been identified as one of the barriers to effective law enforcement in this province.

Currencies and Denominations

As noted above, the currencies most frequently encountered in consignments of criminal cash are those that are the most stable, widely used, and readily traded.

69 Ibid, pp 16, 61–62. As Simon Lord, one of the authors of the FATF report, explained: "One of the things that we found, for example, is people were occasionally declaring cash that didn't actually exist so that they could then walk into a bank with a big pile of cash and say, look, this is entirely legitimate, here's the cash declaration form I filled in, so would you mind paying it into the bank account for me. And so that happens quite a lot. And it's the sort of adaptation you might expect actually when people are getting used to the way that regulatory systems work": Transcript, May 29, 2020, p 8.

70 Exhibit 4, Appendix LL, *FATF Bulk Cash Report,* pp 4–5.

71 Ibid, p 40.

72 Ibid, p 41.

73 Exhibit 64, *Europol Cash Report,* p 7.

74 Ibid, p 11.

These include the US dollar, euro, British pound, and Swiss franc. While less common than the foregoing currencies, the Canadian dollar is high on the list as well.[75]

The FATF report notes that high-denomination bills are more likely to be encountered when there is an element of concealment involved in the transportation of cash.[76] It explains:

> The reason for this is self evident … Taking the British pound as an example, measurements of the size and weight of the relevant banknotes shows that GBP 250 000 in "street cash", a mixture of GBP 10 and GBP 20 notes, weighs between 15–20 kg and is bulky enough to fill an average sports holdall [gym duffel bag]. The same value in EUR 500 notes would weigh about 0.6 kg and would fit in a fat envelope. High-denomination notes therefore facilitate the concealment of large values of cash.[77]

Authorities in the Netherlands believe that almost all 500-euro notes are used for criminal activity and have even noted that in some cases, a 500-euro note costs more than 500 euros because of demand.[78]

Despite the foregoing, the denominations most commonly held by criminals can vary depending on the country. For example, the UK and the Netherlands see many high-denomination bills, whereas Germany has made many more seizures of low to medium denominations.[79] The UK ultimately withdrew the 500-euro note from circulation after determining that there were few legitimate uses of it.[80]

As of April 27, 2019, the 500-euro note is no longer being issued.[81] However, ceasing to issue it will not eliminate the problem. The UK's 2015 national risk assessment notes that despite withdrawing the 500-euro note, "it is apparent that the €500 note is still being purchased from customers by the UK currency sector" and that it still frequently appears in suspicious activity reports.[82] Further, criminals may simply move to other high-denomination bills:

75 Exhibit 4, Appendix LL, *FATF Bulk Cash Report,* pp 4, 52.

76 Ibid, p 56.

77 Ibid, p 56. See also Exhibit 64, *Europol Cash Report,* p 20: "EUR 1 million in 500 notes equates to just 2000 notes weighing 2.2 kg, taking up a space of just under 3 litres (which, for instance, would easily fit inside a small laptop bag). Meanwhile, the same amount of money (EUR 1 million) in EUR 50 notes equates to 20,000 pieces weighing over 22 kg and taking up the space of a small suitcase."

78 Evidence of S. Lord, Transcript, May 29, 2020, pp 7–8.

79 Exhibit 4, Appendix LL, *FATF Bulk Cash Report,* pp 54, 55; Exhibit 33, Her Majesty's Treasury and Home Office, *UK National Risk Assessment of Money Laundering and Terrorist Financing* (October 2015), p 76, para 8.7.

80 Evidence of S. Lord, Transcript, May 29, 2020, p 7; Exhibit 33, Her Majesty's Treasury and Home Office, *UK National Risk Assessment of Money Laundering and Terrorist Financing* (October 2015), p 76, para 8.8.

81 European Central Bank, "Banknotes," online: https://www.ecb.europa.eu/euro/banknotes/html/index.en.html.

82 Exhibit 33, Her Majesty's Treasury and Home Office, *UK National Risk Assessment of Money Laundering and Terrorist Financing* (October 2015), p 76, para 8.9.

> The effect of [withdrawing the 500-euro bill] was [that] people moved almost immediately into purchasing the 200-euro notes instead, because it was the next highest note value and the best way of packing a lot of value into a small … space.[83]

Purposes of Cash Smuggling

The FATF report explains that the method used to transfer cash depends on a decision-making process by the criminal, which ultimately depends on the *purpose* of the cash movement:

> This process begins with the criminal deciding what the purpose of the cash movement is (for example, to break the audit trail, to pay a supplier, to bank it in another jurisdiction etc.). This will dictate the ultimate destination, which will in turn inform the method used, and ultimately the route chosen. At all stages, influences such as risk, familiarity, simplicity and the demands of partners will affect the decisions made.[84]

Simon Lord testified that transporting small amounts of cash can be accomplished by having someone hide the cash on their person, whereas when moving cash "on an industrial scale" – for example, in quantities possessed by Colombian drug trafficking cartels – would require transportation by freight, given the size, weight, and bulkiness of such quantities of cash.[85]

There are a number of reasons why criminals may seek to move cash. As noted above, a key one is to break the audit trail. Others include:

- **Demand:** cash may be needed in another jurisdiction to pay for further consignment of illicit goods or purchase an asset.
- **Avoiding regulatory oversight:** it may be easier to bank funds or otherwise use them in another jurisdiction due to less stringent anti–money laundering controls.
- **Familiarity:** criminals may move cash across borders where they were successful in doing so before.[86]

Depending on the purpose of moving the cash, criminals may engage in transactions that have no obvious business purpose. For example, criminals may withdraw cash from a bank account in one country and pay it into a bank in another.[87] Simon Lord explained that a colleague from the Tunisian financial intelligence unit has observed such activity:

83 Evidence of S. Lord, Transcript, May 29, 2020, p 7.
84 Exhibit 4, Appendix LL, *FATF Bulk Cash Report*, p 3.
85 Evidence of S. Lord, Transcript, May 29, 2020, pp 6–7.
86 Exhibit 4, Appendix LL, *FATF Bulk Cash Report*, pp 37–44.
87 Ibid, pp 35–36.

> [Criminals] had gotten money in the financial system in Tunisia and they had managed to withdraw the money in large amounts of cash. And obviously that's something that you can do in Tunisia, but you may not be able to do in somewhere like Canada or the UK. And the guy had then taken the cash and just moved it across a couple of midland boundaries to another country in Africa and paid it back into the bank in that location. And it was simply to break the audit trail … it was moving the cash across an international boundary, because he knew that even though they were only … maybe 500 kilometres apart, the authorities in country B wouldn't be talking to the authorities in country A, and equally, didn't consider the cash to be suspicious. And so, there was no way you would be able to know that that person in location A also had a bank account in location B and he just moved the cash from one place to another.[88]

Methods and Routes of Cash Smuggling

There are a number of ways in which cash can be smuggled across borders. Again, the technique chosen will depend on the purpose of moving the cash. Some methods include:

- **Cash couriers:** cash may be moved by a person who has been recruited by a criminal organization to transport criminally derived cash across an international border on their person – for example, concealed in clothing, in a money belt, in their luggage, or even internally.[89]
- **Concealed within a method of transport:** cash may be concealed in cars, trucks, or maritime craft, with or without the knowledge of the carrier.[90]
- **In containerized or other forms of cargo:** this method is popular for very large amounts of cash, given that individuals can only carry so much with them.[91]
- **Concealed in mail or post parcels:** significant amounts of cash can be concealed in this way if using large denomination bills.[92]
- **Hidden in plain sight:** this might be done by taking advantage of limited requirements for declaring cash.[93]

Closely related to methods of smuggling is the route chosen, which again will depend on the purpose of moving the cash in the first place. For example, a criminal seeking to move 100,000 euros from the Netherlands to Spain may make different decisions that a criminal seeking to move 100,000 British pounds from the United

88 Evidence of S. Lord, Transcript, May 29, 2020, p 10.

89 Exhibit 4, Appendix LL, *FATF Bulk Cash Report,* p 28; Exhibit 64, *Europol Cash Report,* p 19.

90 Exhibit 4, Appendix LL, *FATF Bulk Cash Report,* p 28; Exhibit 64, *Europol Cash Report,* p 19.

91 Exhibit 4, Appendix LL, *FATF Bulk Cash Report,* p 28.

92 Ibid, p 28.

93 Ibid, p 28.

Kingdom to Spain. The first criminal may choose to move cash from the Netherlands to Spain by car because (a) 100,000 euros would be very heavy, (b) they would likely be detected by authorities if moved by air, and (c) the Schengen agreement means that there are no restrictions on movement in the European Union.[94] In contrast, moving cash between the United Kingdom and Spain raises other considerations, including that (a) the United Kingdom has a different currency than Spain, meaning currency exchange would be necessary; and (b) concealment will be more important to avoid scrutiny by border agents, which may lead to increased use of high-denomination notes to reduce bulk and weight. Further, if the risk of detection is deemed too high, the criminal may choose to transport the funds by car through the Channel Tunnel to France before moving to Spain – while this would normally not be a sound business choice, it may achieve the criminal's purpose in moving the cash.[95]

Difficulties in Detecting Cash Smuggling

A number of difficulties arise in detecting cash smuggling across borders. The FATF report identifies a number of challenges that countries face domestically, including:

- a lack of training for customs officers specifically relating to cash-based money laundering;
- inefficient coordination between customs and other agencies (mainly law enforcement);
- insufficient information being communicated to the financial intelligence unit;
- limited resources;
- lack of access to tools such as X-ray facilities, body scanners, and cash detection dogs; and
- lack of knowledge by financial institutions' staff about how cash declaration forms can be misused.[96]

Given the necessarily international dimension of cash smuggling, it is also important to have effective information and intelligence sharing between countries. The FATF report notes a number of difficulties in this regard.[97] Related to intelligence sharing is the exchange of evidence: the report notes issues relating to ineffective use of mutual legal assistance.[98]

94 Ibid, p 49.

95 Ibid, p 49.

96 Exhibit 4, Appendix LL, *FATF Bulk Cash Report,* pp 94–96. See also Exhibit 64, *Europol Cash Report,* pp 7, 21.

97 Exhibit 4, Appendix LL, *FATF Bulk Cash Report,* pp 96–97.

98 Ibid, pp 97–98.

The FATF report also notes a number of legislative barriers that countries face. Although some countries may have a comprehensive legal framework in place to address cash smuggling by natural persons, they may lack the necessary legal tools to properly address cash in cargo and mail. For example, customs authorities may not have the legal authority to detain shipments for further information, to require the disclosure of further information, or to investigate appropriately.[99]

Simon Lord testified that cash, when being freighted, has its own commodity code that does not attract any duty or value-added tax (VAT). As a result, customs paperwork often does not refer to the *amount* in the shipment, and cash is sometimes deliberately misdeclared for security reasons. As a result,

> that makes actually understanding how much cash there is in transit from place A to place B extremely difficult, because what you might find, even if the cash is declared correctly, the … customs forms might just say "cash, two tons," and then give the value of the consignment as the value of the paper that it's printed on and the ink that's on it rather than the fact that it's 60 million francs.
>
> And so, it's actually quite difficult to work out how much cash is actually being moved around the world, and you have to dig into it quite a lot. And one of the things that we discovered was … that occasionally you might need to use … coercive powers on a financial institution to get them to tell you who the actual beneficial owner of the cash is, but you didn't have access to those powers because the cash had been declared entirely correctly according to customs procedures, and you have no other grounds for suspicion which might allow you to go for a court order.[100]

The difficulties in investigating crime involving large quantities of cash are unlikely to disappear in the near future, given that cash continues to be widely used in criminal activity. It is essential that law enforcement and policymakers continue to develop expertise in cash-based activity and have the necessary tools required to detect such activity. In Chapter 8, I recommend the creation of a new provincial AML Commissioner, a person and office that will develop significant expertise with money laundering typologies and vulnerabilities, as well as measures to combat money laundering. The AML Commissioner will be well-placed to engage in ongoing monitoring and research of bulk cash smuggling and to issue public reports that set out recommendations for improvement. I would also encourage the new provincial money laundering intelligence and investigation unit that I recommend in Chapter 41 to be alive the ways in which the movement of cash can be a component of a money laundering operation.

99 Ibid, pp 98–100.

100 Evidence of S. Lord, Transcript, May 29, 2020, pp 8–9.

Conclusion

Bulk cash smuggling, a practice that has existed for years and continues to occur, plays a key role in the underground economy. By its nature, bulk cash smuggling will always involve at least two countries, and thus has an inherently international dimension. Consequently, the activity calls for responses primarily at the federal level. It is my hope and expectation that the federal government will review the currency declaration regime under the *PCMLTFA* – particularly the continued appropriateness of the penalties therein – and pay close attention to reports by the FATF and Europol in order to strengthen the Canadian regime.

Chapter 37
Informal Value Transfer Systems

I have referred to informal value transfer systems (sometimes called "underground banks") at various points in this Report, including Chapters 2, 3, and 21. In basic terms, these systems allow people to move *value* from one location to another without transferring *funds* through the regulated financial system. This occurs through the use of "cash pools" in different locations that, in simple terms, enable someone to make a deposit in one location and access cash in another, with the cash pools ultimately being settled.

While, as I discuss below, informal value transfer systems can have legitimate uses, they also play a significant role in the underground money laundering economy. They exist around the world, and there is remarkable similarity between the various versions worldwide.[1] Informal value transfer systems internationally include *hawalas* (Middle East), *hundi* (India), *undiyal* (Sri Lanka), *fei qian* (China), and *saraf* (Iran).[2] In this province, one criminal operation employing the "Vancouver model," which I discuss in more detail in Chapter 3, made extensive use of informal value transfer to launder substantial sums of illicit cash over a number of years.

In what follows, I explain how these systems work and the money laundering vulnerabilities associated with them. Although this chapter focuses largely on illicit activity involving informal value transfer systems, I emphasize at the outset that such systems are often used for legitimate purposes as well, including by individuals who have difficulty accessing traditional banking services.

1 Evidence of S. Lord, Transcript, May 28, 2020, p 82.

2 Exhibit 445, FINTRAC, *Financial Intelligence Report: Criminal Informal Value Transfer Systems (IVTS)* (February 2016), para 2; Evidence of S. Lord, Transcript, May 28, 2020, p 75.

What Are Informal Value Transfer Systems?

Informal value transfer systems are essentially underground "banking" channels that allow users to move *value* between locations without actually transferring *funds*. While each system is slightly different, the operators typically have "pools" of cash available to them in different locations. When a client needs to transfer funds from one location to another, the money will be paid into the cash pool in the first location and paid out of the cash pool in the jurisdiction where the recipient needs the money. (Across borders, this may mean the use of different currencies, but for equivalent value.) The money paid into the first pool will be held in that location until another client needs to transfer funds into that jurisdiction. Over time, the operator may need to reconcile the cash pools to keep them in balance. However, there is no transfer of funds on an individual basis. In this way, individuals are not actually sending funds across borders – rather, the settling process enables funds to be deposited in one location and accessed in another.

Simon Lord described the operation of these systems as follows:

> Essentially, it's money transmission at its most basic. Quite a lot of the time these types of systems are tied to specific geographic regions, ethnic communities and what have you, and essentially what they do is they arrange for transfer and receipt of funds or equivalent value without the physical need to transfer the funds themselves. So you're transferring value but not necessarily the funds. So there won't be a straight line remittance from point A to point B through the banking system … [S]omeone will make a deposit of funds in one location and will receive an equivalent value in another location, less fees and commission, but without there actually being a physical connection between the two. And they generally involve a process which I generally refer to as "cash pooling." So, the people who are involved in these types of networks have available to them pools of funds in different locations, not always cash. Sometimes it's money in bank accounts, sometimes it's trade. But pools of funds in different locations and you receive the payment into one of those pools and make a payment out of another one. And then over time there will be a settlement arrangement between the pools to keep them in balance. Because obviously if all the money went one way, you would end up with lots of money in one place and not in another, and you would have to have some sort of settlement mechanism in place. So settlement can take place through trade, through cash, through net settlements over a long period of time, quite often through the banking system. They're often informal in so far as this type of stuff often happens outside of the formal financial system, but by no means all the time. They often interact with financial systems as well.[3]

3 Evidence of S. Lord, Transcript, May 28, 2020, pp 57–58.

Informal value transfer systems can be used to send money around the world. In a 2013 report, the Financial Action Task Force focused on what it termed "*hawalas* and other similar service providers."[4] The task force considers such services to be a subset of money or value transfer services and defines them as "money transmitters, particularly with ties to specific geographic regions or ethnic communities, which arrange for transfer and receipt of funds or equivalent value and settle through trade, cash, and net settlement over a long period of time."[5] However, the report differentiates informal value transfer systems from money transmitters as follows:

> While [*hawalas* and other similar service providers] often use banking channels to settle between receiving and pay-out agents, what makes them distinct from other money transmitters is their use of non-bank settlement methods, including settlement via trade and cash, as well as prolonged settlement time. There is also a general agreement as to what they are not: global money transfer networks (including agents) operated by large multinational money transmitters and money transfers carried out through new payment methods including money remittance services. This description is based on *services* provided by them and *not their legal status*. [Emphasis in original.][6]

The report divides *hawalas* and similar service providers into three categories: pure traditional (legitimate) ones, hybrid traditional (sometimes unwitting) ones, and criminal (complicit) ones.[7] Traditional, legitimate service providers – the first category – have existed for centuries in South Asia and the Middle East in largely unregulated environments.[8] They are used extensively for low-value remittances on behalf of individuals and tend to be popular among migrants because of familial, regional, or tribal affiliation, as well as inadequate access to regulated financial services.[9] If they are sufficiently regulated and supervised, these providers will present low or lower money laundering and terrorist financing risks because of the low value of average transactions.[10]

The second category – hybrid providers – are ones that may be used, intentionally or not, for illegitimate purposes such as the transmission of illicit money across borders. They are not primarily set up to move illicit money, but may become involved in illegal activities such as moving money generated from tax evasion or other crime, evading currency controls, or avoiding sanctions. They use similar methods to traditional providers and are not part of a criminal network.[11]

4 Exhibit 4, Overview Report: Financial Action Task Force, Appendix BB, FATF, *The Role of* Hawala *and Other Similar Service Providers in Money Laundering and Terrorist Financing* (October 2013) [FATF Hawala Report].

5 Ibid, pp 9, 12.

6 Ibid, p 9.

7 Ibid, p 14.

8 Ibid, p 14; Evidence of S. Schneider, Transcript, May 26, 2020, p 23.

9 Exhibit 4, Appendix BB, FATF Hawala Report, p 14.

10 Ibid.

11 Ibid, pp 14–15.

Finally, criminal providers are knowingly involved in criminal activity. The Financial Action Task Force report indicates that in some countries, informal value transfer service providers are increasingly being set up or expanded to service criminals. They are often controlled by criminals or criminal groups – particularly professional money launderers – and present high money laundering and terrorist financing risks.[12] Their networks often enable other crimes beyond money laundering, such as tax fraud, currency offences, and corruption.[13]

A 2016 report by the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) notes that although the Financial Action Task Force divides informal value transfer systems into three categories, "it is likely that even legitimate [systems] may, at times, facilitate transactions involving illicit funds. Similarly, criminal [systems] may facilitate transactions involving completely [lawful] funds."[14]

It is important to emphasize that there are many legitimate uses of informal value transfer services. Indeed, Professor Jason Sharman testified that "as far as we know, the overwhelming majority of those transfers are used for entirely legitimate and lawful purposes."[15] Informal value transfer services can be particularly useful in countries with underdeveloped financial systems. They have the ability to deliver money to distant countries where regulated channels do not exist; in some cases, they may be the only channel through which funds can be transmitted in conflict regions.[16] These systems are also frequently used by illegal foreign migrants residing in developed countries, whose illegal status precludes them from accessing banks and regulated financial services providers.[17] Further, in some countries, individuals may have a lack of confidence in banks; that is often the case in countries where bank failures have occurred and customers have lost deposits. Some users may also have limited understanding or familiarity with traditional financial services due to a lack of financial literacy or language barriers.[18] Some informal value transfer services also have some advantages over banks, offering cheaper or faster services or better exchange rates.[19]

How Does an Informal Value Transfer System Work?

The Financial Action Task Force's 2013 report outlines four different methods of settlements used by informal value transfer systems:

- simple reverse transactions;
- triangular settlement;

12 Ibid, p 15.

13 Ibid; Evidence of S. Schneider, Transcript, May 26, 2020, p 26.

14 Exhibit 445, FINTRAC, *Financial Intelligence Report: Criminal Informal Value Transfer Systems (IVTS)* (February 2016), para 3.

15 Evidence of J. Sharman, Transcript, May 6, 2021, p 23.

16 Exhibit 4, Appendix BB, FATF Hawala Report, pp 17–18.

17 Ibid, p 18; Evidence of J. Sharman, Transcript, May 6, 2021, p 26.

18 Exhibit 4, Appendix BB, FATF Hawala Report, p 18.

19 Ibid, p 17.

- settlement through value; and
- use of cash couriers.[20]

Simple reverse transactions are a classic form of transfer. For example, a customer may want to send money from the United States to India. The customer provides cash to the US service provider, who in turn asks his counterpart in India to make a payment to the beneficiary in India. The Indian service provider uses his local cash pool to make the payment – no transfer of funds actually occurs between the US and Indian providers. To settle the transaction, the US provider will make a future payment to a beneficiary in the US on behalf of a customer of the Indian service provider. Over a period of time, the overall net amount of transactions may balance, but if not, a settlement will take place, usually via wire transfer.[21]

Triangular settlement is a variation of the simple reverse transaction approach. It involves several service providers. In the above example, the US provider asks the Indian provider to provide cash to someone. At the same time, the Indian provider has a customer seeking to send money to Somalia. If the Indian provider does not have a counterpart in Somalia, he may seek assistance from the US service provider to identify a provider in Somalia that owes a debt to the US one. Once the Somalian service provider pays the beneficiary on behalf of the Indian one, all accounts are settled.[22]

Settlement through value is a common practice in Afghanistan, Iran, Pakistan, and Somalia. Operators use a surplus of cash or banked money to fund trade payments at the request of a business that in turn pays the individual recipients in the remittance destination region. Finally, settlement can occur through the **use of cash couriers** who physically transport cash, including across borders.[23]

Money laundering schemes involving informal value transfer systems can become very complex, involving multiple networks and countries and incorporating trade-based money laundering and other forms of criminality. Mr. Lord provided an example of a complex money laundering operation using informal value transfer, which I discuss in detail below.

Informal value transfer systems often involve multiple actors in several countries who may not know each other personally, and the amounts of money involved can be quite large. In order to ensure that the money is given to the right person, operators of informal value transfer systems often use a technique known as "token-based" exchange. As I explain further below, criminal informal value transfer systems typically involve a controller, collector, coordinator, and transmitter. The controller is in charge of the entire operation, and the collector actually meets with the criminal to receive the cash. When a

20 Exhibit 4, Appendix BB, FATF Hawala Report, pp 23–24.

21 Ibid, p 23.

22 Ibid.

23 Ibid.

controller asks a collector to meet a criminal to receive cash, the collector quotes the serial number of a small-denomination bill in his possession to the controller. The controller then transmits that number to the criminal by way of text message, WhatsApp, or another messaging system. When the criminal ultimately provides the cash to the collector, the collector produces the bill with its unique serial number, and the criminal is assured that the collector is the person meant to receive the cash – nobody else could have that bank note with its unique serial number. Further, when the collector hands over the bill, that bill acts as a kind of receipt: the criminal can show it to his boss in the event of a loss. Mr. Lord testified that token-based exchange is used all over the world, including in Canada.[24]

Money Laundering Risks

Informal value transfer systems entail a number of money laundering risks. In general, they can pose a money laundering vulnerability "simply because of the fact that they're off the books and that there's no official record of them [and] they're not part of the anti–money laundering surveillance system that covers formal banking."[25] Indeed, they may be attractive to money launderers precisely because they enable criminals to operate under the radar.[26]

In what follows, I review the "controller, collector, coordinator, transmitter" money laundering typology as well as the "Vancouver model." I then consider difficulties with anti–money laundering regulation of informal value transfer systems.

Controller, Collector, Coordinator, Transmitter Typology

Criminal informal value transfer systems often employ the controller, collector, coordinator, transmitter typology. The **controller** (also known as a money broker) is the individual who arranges for the collection of street money (such as drug proceeds) and arranges for the delivery of an equivalent value to its ultimate destination (for example, businesses controlled by a drug cartel). The Financial Action Task Force report calls the controller the "key to the success of the system," noting that the controller acts as a third-party money launderer and is normally responsible for the money from the time it is collected until the value is successfully delivered (and may bear the cost of funds that are lost or not effectively transferred). The **collector** is instructed by the controller to collect money from criminals and to dispose of it following the controller's instructions. He is the controller's trusted representative and faces the highest risk of arrest because

24 Evidence of S. Lord, Transcript, May 28, 2020, p 77–79. A receipt is important because the money laundering network assumes responsibility for the safe delivery of the funds to the remote location. As a result, the network will be responsible for paying out the funds even if, for example, a member of the network is arrested and the cash is seized. Further, this system avoids a situation where the networks would need to literally record the name of the criminal providing the funds, the amount of the funds, and the recipient – recording such info "would be suicide" for a criminal: ibid, p 78.

25 Evidence of J. Sharman, Transcript, May 6, 2021, p 24.

26 Evidence of S. Schneider, Transcript, May 26, 2020, p 48.

he actually meets the criminal customer to collect the cash.[27] The criminal customer using an informal value transfer system is typically charged a percentage of the amount sought to be transferred; this is a commission paid to the criminal network.[28] Some schemes involve a **coordinator**, who is an intermediary that manages parts of the money laundering process for one or more controllers. Finally, the **transmitter** receives and dispatches the money to the control of the controller.[29]

The diagram below (Figure 37.1; also included as Exhibit 11) was prepared by Mr. Lord and illustrates a fictitious example of a complex informal value transfer system and how it can be used to launder illicit funds. The diagram demonstrates that criminal informal value transfer systems can quickly become very complex, spanning multiple countries and using several money laundering techniques. Indeed, such systems can be used not only for money laundering but also for facilitating other crimes, including illegal currency trade, import and export fraud, sanctions evasion, tax evasion, and financing of terrorism.[30]

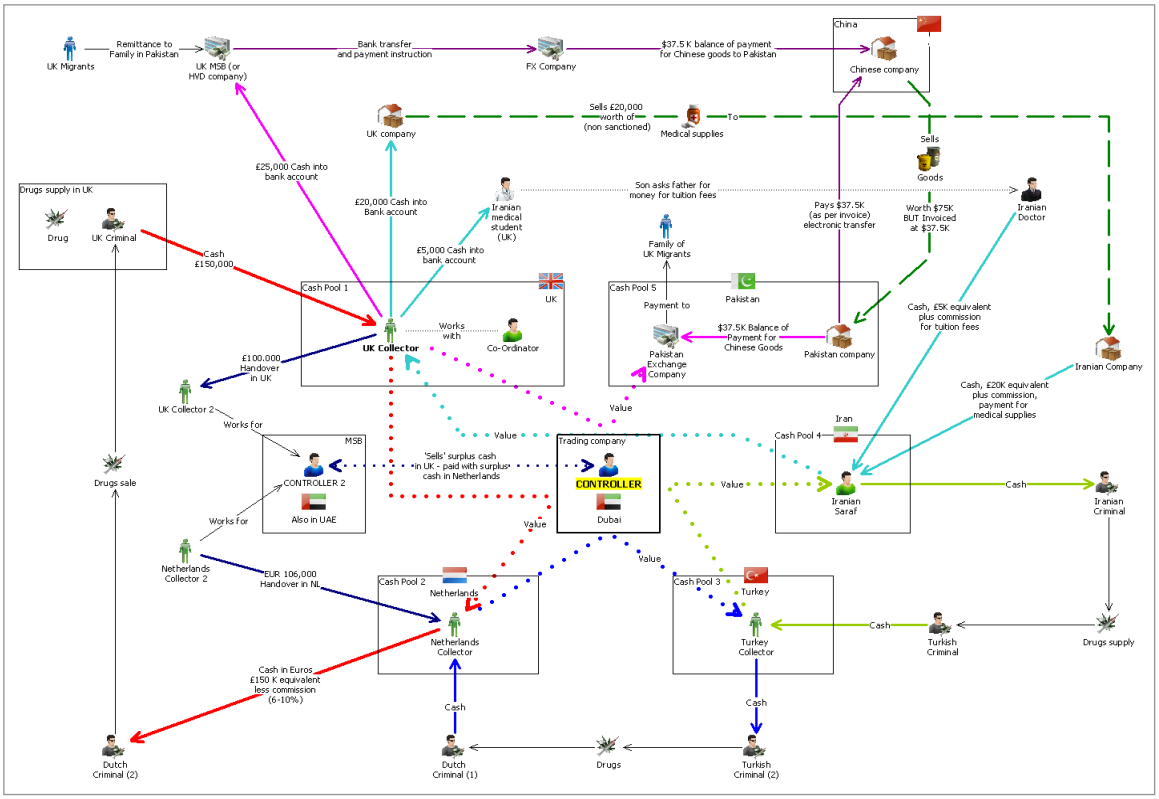


Figure 37.1: IVTS Network Map

Source: Exhibit 11, IVTS Network Map

27 Evidence of S. Lord, Transcript, May 28, 2020, pp 78–79.

28 Ibid, p 72.

29 Exhibit 4, Appendix BB, FATF Hawala Report, p 29.

30 Ibid, pp 9, 18, 33–44.

The diagram is nicknamed the "London Underground map" given the various colours and arrows.[31] What follows is a summary of Mr. Lord's explanation of the diagram. The controller at the centre of the picture (highlighted in yellow) is operating out of Dubai.[32] He has access to a number of cash pools: in this example, cash pools are located in the UK, the Netherlands, Turkey, Iran, and Pakistan. A collector is indicated in relation to each of these pools.

On the left side of the diagram, a UK criminal (in this example, a drug trafficker) is seeking to have £150,000 appear in the Netherlands. "Dutch criminal (2)" at the bottom left supplied the drugs, and the UK criminal is seeking to pay him.[33] The controller arranges for his UK collector to meet with the criminal and collect the cash.[34] The cost to the UK criminal to have his transaction pass through this network is around 6 to 8 percent of the amount he is seeking to pay Dutch criminal (2).[35]

The UK collector takes the cash from the UK criminal to a safe location, counts it, and reports to the controller on the amount received.[36] The controller then contacts the Dutch collector, who in turn has received cash from "Dutch criminal (1)" that the latter wants to appear in Turkey. The controller tells the Dutch collector to provide £150,000 to Dutch criminal (2).[37]

In most situations, the controller will pay out the criminal (in this example, Dutch criminal (2)) from the pool of cash he maintains in the Netherlands (here, Cash Pool 2). However, there may be situations in which that pool does not have enough cash for the payout. In such cases, the controller may work with other controllers conducting similar operations in order to facilitate the transfer.[38]

In this example, the Dutch collector is missing EUR 106,000. He informs the controller, who then contacts "Controller 2," who also happens to be located in the United Arab Emirates. The two controllers are technically in competition, but they will work together where it benefits them both. Here, Controller 2 agrees to provide EUR 106,000 (equivalent to £100,000) to the Dutch collector. In exchange, the controller agrees to provide £100,000 to Controller 2's network in the UK (recall that the UK cash pool has £150,000 in cash from the UK criminal). The controller instructs his UK collector to provide £100,000 to a collector working for Controller 2, and a reciprocal handover of EUR 106,000 occurs in the Netherlands.[39]

31 Evidence of S. Lord, Transcript, May 28, 2020, p 67.

32 Ibid, pp 67–68.

33 Ibid, p 69.

34 Ibid, pp 68–69. The scheme will often include a "coordinator" as well, who controls various collectors in an area.

35 Ibid, p 72.

36 Ibid, p 70.

37 Ibid. The Turkish collector has likewise received cash from "Turkish criminal (2)" that the latter wants to appear in Iran, and the cycle continues.

38 Ibid, pp 70–71.

39 Ibid, p 71.

At this point, the Dutch collector has sufficient funds to settle the transaction between the UK criminal and Dutch criminal (2). The collector pays Dutch criminal (2), and the transaction is settled (indicated by the red arrows on the diagram).[40]

Importantly, the UK collector still has £50,000 in the UK cash pool – the UK criminal had provided £150,000, and the UK collector transferred £100,000 to the collector working for Controller 2. The UK collector does not want the £50,000 to sit idle; he instead engages in trade-based money laundering.[41]

On the right side of the diagram, Cash Pool 5 is located in Pakistan. A Pakistani company is importing goods worth $75,000 from China. The Pakistani company wants to import these goods without paying the value-added tax (VAT), customs duties, and other charges. The Pakistani importer therefore arranges with the Chinese company to invoice for only half of the value of the goods – so, the paperwork indicates the value is $37,500 rather than $75,000.[42] At this point, the Pakistani company has received $75,000 worth of goods but has only paid $37,500. To compensate the Chinese company for the under-invoicing, the Pakistani company makes a payment of $37,500 to an exchange company in Pakistan that is complicit with the controller.[43]

At the same time, the controller contacts the UK collector to put £25,000 (of the £50,000 that remains from the UK criminal) into a bank account of a money services business located in the UK.[44] Meanwhile, some migrants want to send funds to their family in Pakistan for legitimate reasons. They send funds to the UK money services business, which transfers the funds to a foreign exchange (FX) trading company. That company is instructed to pay the $37,500 that the Chinese company is owed.[45] So, the Chinese company has been paid in full, and the Pakistani company has successfully evaded tax and fees.[46]

The result of all this is that a UK investigator, who sets off trying to follow the original £150,000, may not appreciate everything that has occurred:

> [T]he important thing to realize here is if you were following the old adage of "follow the money," what you would see is the UK criminal's money going to the UK collector, going into [a money services business] company, and going to China, and you'd be saying to yourself as a financial investigator, well, why does my guy want his money in China? And the fact is he doesn't, and his money hasn't gone to China. His money has actually popped out in the Netherlands, but the actual money that he put into the collector has been used for a different purpose, to settle a trade transaction in between two completely independent people.[47]

40 Ibid, p 72.

41 Ibid.

42 Ibid, pp 72–73.

43 Ibid, p 73.

44 Ibid. This is illustrated in the top left corner of the diagram.

45 Ibid, pp 73–74.

46 Ibid, p 74.

47 Ibid, p 74.

This is not the end of the matter, however. The UK collector still has £25,000 remaining from the original £150,000, and he uses those funds to facilitate two legitimate transactions.[48] First, he makes a £20,000 payment to a UK company that has exported medical supplies to a company in Iran. While the export of medical supplies is perfectly legal, it is virtually impossible for the company receiving those supplies to make a direct bank transfer to the UK company because of the international sanctions in place against Iran, so the Iranian company has paid the UK company through an Iranian *saraf* (essentially a money services business). The *saraf* settles with the controller, and the controller completes the transaction by making a cash payment to the UK company.[49]

Second, the UK collector allows an Iranian doctor to send £5,000 to his son, who is studying medicine in the UK. Like the Iranian company importing medical supplies, a direct bank transfer is impossible. Accordingly, the father provides an equivalent amount to the Iranian *saraf*, who transfers those funds to the controller, who instructs his UK collector to provide £5,000 to the son. While the use made of those funds is completely legitimate, it is important to note that the cash given to the son is the product of drug trafficking activity carried out by the UK criminal in the United Kingdom (something referred to as "cuckoo smurfing").[50]

Informal Value Transfer in British Columbia

The evidence before me revealed that informal value transfer systems have undoubtedly been used to launder significant amounts of money in British Columbia. Once such example was uncovered through the E-Pirate investigation, discussed further in Chapter 3, which revealed that a criminal organization engaged in a laundering operation utilizing a method that has been referred to as the "Vancouver model" made extensive use of informal value transfer to settle accounts between China, British Columbia, and other jurisdictions.

The Vancouver model is a method of money laundering that has figured prominently – as the name suggests – in British Columbia. The term appears to have been first used by an Australian professor, John Langdale, in a presentation about criminal alliances from China that posed a threat to Australia.[51] In this model, organized crime groups operating in British Columbia deposit the cash of their illegal activity with the operator of an informal value transfer system in the Lower Mainland and receive an equivalent value (less the commission earned by the operator) in countries such as Mexico and Colombia. The cash received by the operator is then repurposed and provided to wealthy Chinese nationals who are unable to move their wealth to British Columbia because of the currency export restrictions imposed by the Chinese government. Those individuals make payments to the operator of the

48 Ibid. This is illustrated on the far right of the diagram.

49 Ibid, pp 74–75.

50 Ibid, pp 75–76.

51 Evidence of S. Schneider, Transcript, May 26, 2020, pp 28–29.

informal value transfer system in China and receive the equivalent value in cash when they arrive in British Columbia.[52]

While a significant portion of that cash was used to make large cash buy-ins at Lower Mainland casinos (see Chapter 13), it is important to understand that the cash can be used for any legitimate or illegitimate purpose, including the purchase of real estate and luxury goods. I also emphasize that the individuals seeking to move their wealth from China to British Columbia are not necessarily involved in criminal activity; they may well have acquired that wealth through legitimate means. The problem is that most, if not all, of the actual cash provided to those individuals in British Columbia is derived from profit-oriented criminal activity and is being paid out by the operator of the informal value transfer system in furtherance of a money laundering scheme.

Elsewhere in this Report, I have concluded that the Vancouver model was used to launder significant sums of money through the British Columbia economy (see Chapter 13). That the model has been used to launder significant sums shows that informal value transfer systems have great potential to be misused — and indeed have been misused — by those intent on money laundering and other criminality. These systems are therefore a significant money laundering vulnerability in this province.

Indeed, the Criminal Intelligence Service British Columbia / Yukon Territory concludes in a 2018 report that there are professional money launderers in British Columbia who use informal value transfer systems to assist their organized crime clientele.[53] According to the report, organized crime relies on professional money launderers and their money services businesses and informal value transfer systems to handle illicit funds, convert currency, and move money internationally.[54] The report opines that criminal informal value transfer systems are of great concern in British Columbia because they provide organized crime with the ability to move illicit funds to other organized crime groups, including in other countries.[55]

FINTRAC has similarly concluded that professional money laundering in Canada takes place through money services businesses and informal value transfer systems, noting that professional money launderers may own or have connections to one or several money services businesses and informal value transfer systems.[56] A FINTRAC

52 Ibid, pp 29–31; Evidence of S. Schneider, Transcript, May 25, 2020, pp 27, 47–48, 59–61, 65. While the Vancouver model typically involves Chinese nationals seeking to move their wealth out of China, the same model could be used by any foreign national seeking to avoid the currency export restrictions imposed by the government in their home country and move significant sums of legitimate or illegitimate wealth to British Columbia.

53 Exhibit 438, Criminal Intelligence Service British Columbia / Yukon Territory, *Professional Money Launderers Who Own/Control Money Services Businesses* (November 2018), p 1.

54 Ibid, pp 1–2.

55 Ibid, p 4.

56 Exhibit 442, FINTRAC, *Financial Intelligence Report: Professional Money Laundering in Canada* (March 2019), p 6.

report notes that it has identified two professional money laundering networks that use both formal and informal value transfer systems and were, as of March 2019, under investigation by law enforcement.[57]

Difficulties with Regulation

Informal value transfer systems are not regulated in the same way as other sectors I have discussed in this Report. FINTRAC considers them to be a form of money services business and therefore expects them to comply with the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, SC 2000, c 17 (*PCMLTFA*) regime in the same way as a money services business would (see Chapter 21).[58] The requirements for money services businesses under the *PCMLTFA* notably include a requirement to register with FINTRAC.[59] However, I expect that the vast majority of these systems do not comply with the *PCMLTFA* regime, both because those that are involved in criminality would have no incentive to do so, and because those that seek to operate legally may be unaware of their obligations due to language or cultural barriers (this occurs with money services businesses, as I discuss in Chapter 21).

Indeed, a key challenge flagged by both the Financial Action Task Force and FINTRAC is the difficulty in identifying unregistered informal value transfer systems. A FINTRAC report notes that regulatory agencies, including FINTRAC, have difficulty identifying such systems because they rely on voluntary registration systems.[60] The Financial Action Task Force similarly observes that informal value transfer systems are difficult to detect because they are often trust-based, secretive, and unregistered; moreover, it is difficult to assess compliance of such services even when they operate legally.[61] It concludes that regulating and supervising informal value transfer service operators is one of the key challenges facing authorities.[62]

Some countries have attempted to regulate informal value transfer services, including by requiring that they be licensed or registered and report suspicious and other transactions. A 2010 Financial Action Task Force report notes that Denmark, Sweden, the United Kingdom, the United States, and Germany had done so.[63] As of 2013, a slight majority of countries had barred informal value transfer systems from operating legally. Those that allowed their operation (and required licensing/registration) believed

57 Ibid.

58 Exhibit 445, FINTRAC, *Financial Intelligence Report: Criminal Informal Value Transfer Systems (IVTS)* (February 2016), para 3; Exhibit 442, FINTRAC, *Financial Intelligence Report: Professional Money Laundering in Canada* (March 2019), p 6; FINTRAC, *Operational Alert: Laundering the Proceeds of Crime Through a Casino-Related Underground Banking Scheme* (December 2019), p 1, online: https://www.fintrac-canafe.gc.ca/intel/operation/casino-eng.pdf.

59 *PCMLTFA*, s 11.1.

60 Exhibit 445, FINTRAC, *Financial Intelligence Report: Criminal Informal Value Transfer Systems (IVTS)* (February 2016), para 4.

61 Exhibit 4, Overview Report: Financial Action Task Force, Appendix EE, *FATF Report: Money Laundering through Money Remittance and Currency Exchange Providers* (June 2010), para 82.

62 Exhibit 4, Appendix BB, FATF Hawala Report, p 26.

63 Exhibit 4, Overview Report: Financial Action Task Force, Exhibit EE, *FATF Report: Money Laundering Through Money Remittance and Currency Exchange Providers* (June 2010), para 82.

that legalization had helped expand remittances through legal channels; however, relatively few had actually registered or become registered.[64] Further, many countries had not yet devised effective mechanisms to identify, monitor, and take action against illegal operators.[65]

The difficulties with regulation increase the money laundering risk associated with informal value transfer systems. Operators that conduct their activities with no regulation are particularly vulnerable because they permit funds to be moved with little or no customer due diligence requirements – this allows criminals to freely send or receive funds with limited risk of being identified.[66] Relatedly, criminal informal value transfer service operators are difficult to prosecute: as the operators are typically far removed from the criminal activities that generate the illicit proceeds, it is difficult for law enforcement to demonstrate that they are handling proceeds of crime.[67]

In contrast to other members of the Financial Action Task Force, Canada and British Columbia have taken relatively few steps to regulate informal value transfer systems. As I noted above, FINTRAC takes the view that informal value transfer systems constitute money services businesses and are therefore subject to the requirements of the *PCMLTFA*, [68] including a requirement to register with FINTRAC. In a 2016 report, FINTRAC indicates that it has engaged with the eight largest financial institutions in Canada with the goal of enhancing suspicious transaction reporting on informal value transfer systems that are not complying with the *PCMLTFA*.[69]

As with the identification of unregistered money services businesses (see Chapter 21), outreach with other reporting entities may assist in identifying unregistered and non-compliant informal value transfer networks, particularly in instances where the problem is an operator's lack of knowledge or understanding of their obligations. However, such outreach is likely less useful when it comes to criminally run informal value transfer networks, the identification of which is properly a law enforcement issue. Some tools, such as surveillance and certain sources of intelligence, are available only to law enforcement, making it a key actor for the detection of such networks. Indeed, as I discuss in Chapter 39, it did not take long for law enforcement to make a link between Silver International and a criminal informal value transfer network. It is crucial that law enforcement be aware of the risks attaching to such networks and work toward identifying them using tools that only it possesses.

64 Exhibit 4, Appendix BB, FATF Hawala Report, p 11.

65 Ibid, p 55.

66 Ibid, p 26.

67 Exhibit 445, FINTRAC, *Financial Intelligence Report: Criminal Informal Value Transfer Systems (IVTS)* (February 2016), para 4.

68 Exhibit 445, FINTRAC, *Financial Intelligence Report: Criminal Informal Value Transfer Systems (IVTS)* (February 2016), para 3; Exhibit 442, FINTRAC, *Financial Intelligence Report: Professional Money Laundering in Canada* (March 2019), p 6; FINTRAC, *Operational Alert: Laundering the Proceeds of Crime Through a Casino-Related Underground Banking Scheme* (December 2019), p 1, online: https://www.fintrac-canafe.gc.ca/intel/operation/casino-eng.pdf.

69 Exhibit 445, FINTRAC, *Financial Intelligence Report: Criminal Informal Value Transfer Systems (IVTS)* (February 2016), para 15.

I have recommended elsewhere (Chapter 41) that the Province establish a new law enforcement unit within the Combined Forces Special Enforcement Unit focused on money laundering investigation and intelligence. It will be key that the new unit develop intelligence relating to underground informal value transfer networks, including those operating in the Lower Mainland whose aim is to navigate around foreign currency export restrictions. I emphasize that, despite the measures now in place in casinos that have greatly reduced the acceptance of cash (see Chapters 11, 12, and 14), other industries – such as real estate and luxury goods – may very well have become more vulnerable to money laundering through informal value transfer. The new unit will need to be aware of the potential displacement of this typology and actively seek to identify the criminal informal value transfer networks operating in the province.

Finally, it is important that government agencies and regulators are adequately informed of informal value transfer systems and related typologies of money laundering. In this regard, the AML Commissioner (recommended in Chapter 8) will be well placed to conduct ongoing study in this area and ensure that affected government agencies and regulators are aware of the risks and typologies associated with informal value transfer.

Conclusion

Informal value transfer systems are an important part of the underground economy. While they have legitimate uses for many customers, there are clear money laundering risks associated with those operators who are complicit with criminals. Money laundering using such systems has occurred in this province and will likely continue to occur. It is important that government, regulators, and law enforcement continue to develop their knowledge and awareness of this activity. Reporting entities have an important role to play in reporting activity that they suspect is liked to criminal informal value transfer systems. However, law enforcement – particularly the new investigation and intelligence unit I have recommended – must play a key role in disrupting this underground activity, which has had significant impacts on British Columbia's economy.

Chapter 38
Trade-Based Money Laundering

Trade-based money laundering is generally understood as the process of disguising illicit funds and moving value between jurisdictions through the use of international trade transactions, in an attempt to legitimize their illicit origins. At their most complex, these schemes can be a tangled web of transactions involving multiple criminal actors in various jurisdictions. When combined with other money laundering tools – such as shell companies, offshore accounts, nominees, legal trusts, and the use of cryptocurrency – it can be extremely difficult for investigators to analyze and unravel these complex schemes.

While there is general agreement that trade-based money laundering is a significant threat, and arguably one of the largest and most pervasive methodologies in the world, it is not well understood and there is good reason to think that a significant percentage of such activity goes undetected. Fortunately, however, there are a number of promising tools that can assist investigators in identifying suspicious transactions and deterring this type of conduct.

In this chapter, I provide an overview of trade-based money laundering and discuss some of the international trade transactions commonly used to launder illicit funds. I also examine the risks associated with trade-based money laundering in British Columbia and conclude with concrete proposals for reform.

The International Trade System

In order to understand how trade-based money laundering operates, it is important to have a basic understanding of the international trade system.

International trade is the buying and selling of goods and services between parties in different states, which allows countries to expand their markets and results in increased competition and competitive pricing. In the Canadian context, an **export** is a product sold to the global market, and an **import** is a product bought from the global market.

International trade is a matter of federal jurisdiction under section 91(2) of the *Constitution Act, 1867*. The federal government has the exclusive delegated jurisdiction to enter into international treaties and participates in a number of international agreements and memoranda of understanding with other governments.[1]

Trade accounts for a significant portion of Canada's gross domestic product and has, with few exceptions, continued to rise in recent years.[2] Exports have grown in British Columbia relatively consistently since 2010, with 2020 standing as an anomaly, likely due to the COVID-19 pandemic. BC exports the most (by value) to the United States, followed by China, Japan, and South Korea. Natural resource and energy products represent, by a large margin, the most significant export sector in British Columbia.[3]

Trade Finance

In many cases, those involved in international trade require financing to support their activities – something known as trade finance. Exporters, for example, may require working capital to process or manufacture products for export before receiving payment. Conversely, importers may require a line of credit to buy goods from overseas.

John Cassara, a former US law enforcement official and an internationally renowned expert on trade-based money laundering, explained trade finance in the following terms:

> [T]rade finance covers trade transactions in which a bank provides some form of financing to a party in the transaction. In the transactions, a party will present documents to the bank, and often a letter of credit, for example, is requested. And these are referred to as "documentary transactions." In these transactions, banks generally process documentation involved in the trade transactions, such as bill of lading, invoice, packing lists. This type of stuff. And the trade finance officer in the bank reviews the information underlying the transaction for soundness and compliance with anti–money laundering policies and procedures.[4]

1 See, for example, Exhibit 338, Overview Report: Canada's Customs Mutual Assistance Agreements, which contains examples of customs mutual assistance agreements and other international agreements and memoranda of understanding between Canada and its partners.

2 Detailed statistics breakdown at: https://www150.statcan.gc.ca/n1/en/subjects/international_trade. BC–specific reports related to trade at: https://www2.gov.bc.ca/gov/content/data/statistics/business-industry-trade/trade.

3 See https://www2.gov.bc.ca/assets/gov/data/statistics/business-industry-trade/trade/exp_annual_bc_exports.pdf.

4 Evidence of J. Cassara, Transcript, December 9, 2020, pp 74–75.

Some of the more common trade finance products include:

- **bills of exchange**, which bind a purchaser to pay a fixed sum to an exporter on demand or at a predetermined date, much like a promissory note;
- **countertrade**, where an exporter takes on a reciprocal obligation in lieu of a cash payment or settlement; and
- **documentary credit**, where a bank extends credit to its client (usually an importer) and assumes responsibility for payment of the imported goods.

International trades that do not rely on financing from a financial institution are known as **open account trade transactions**. By one estimate, open account trade constitutes 80 percent of international trade processed through financial institutions.[5]

While most open account trade transactions are processed through conventional electronic funds transfers, I heard evidence that mobile payments such as WeChat (a Chinese social media app used to transfer money) and cryptocurrencies are increasingly favoured by those involved in trade-based money laundering and other underground financial systems.[6]

Trade-Based Money Laundering

Trade-based money laundering is the process of disguising illicit funds and moving value through the use of trade transactions in an attempt to legitimize their illicit origins.[7] It typically occurs through the misrepresentation of price, quantity, or quality of imports or exports in order to transfer value between complicit sellers and complicit buyers in different jurisdictions (something known as **trade mispricing**).[8]

Trade-based money laundering involves varied and, in some cases, elaborate schemes to transfer value between countries. However, the basic techniques include

5 Ibid, p 76.

6 Ibid, p 81.

7 Exhibit 345: Canada, TBML Presentation (April 1, 2020), p 2; Exhibit 1020, Overview Report: Information Relating to the FATF & Egmont Group Trade-Based Money Laundering Report, Appendix A, pp 11–12; Exhibit 1017, Overview Report: NCIE ML / Fraud, Appendix A, p 14; Evidence of J. Cassara, Transcript, December 9, 2020, pp 41–42; Evidence of B. Gateley, Transcript, December 10, 2020, p 15; Evidence of J. Gibbons, Transcript, December 10, 2020, pp 19–20 (Mr. Gibbons testified that the use of "illicit financial flows," as opposed to "proceeds of crime," is intended to capture more conduct, including capital flight, proceeds of corruption, and sanctions evasion).

8 Exhibit 339, Overview Report: Trade-Based Money Laundering Reports and Records, p 61; Exhibit 347, CBSA, TBML (June 5, 2019), pp 11–13. See also Evidence of J. Gibbons, Transcript, December 10, 2020, p 27. Evidence of J. Zdanowicz, Transcript, December 11, 2020, p 122. (To move money out of a country, a party must undervalue its exports or overvalue its imports. Conversely, to move money into a country, a party must overvalue its exports and undervalue its imports.)

over- and under-invoicing, multiple invoicing, over- and under-shipments, and falsely described goods and commodities. I discuss each of these techniques below.[9]

Over- and Under-invoicing

Over- and under-invoicing occurs where the exporter issues an invoice for an amount greater or less than the true value of the goods in order to transfer value between countries. In an **under-invoicing** scenario, an exporter seeking to move value to another country might sell widgets worth two dollars per widget to a foreign importer for a price of one dollar per widget. When the foreign importer sells those widgets in its home country, it will receive one dollar more per widget than was paid for those products.[10]

In an **over-invoicing** scenario, an exporter seeking to transfer money into the country could sell widgets worth two dollars each to the foreign importer and invoice the importer for a higher price (for example, three dollars per widget). When the invoice is paid, the exporter will have received one dollar per widget more than the widgets were worth. If a thousand widgets were sold at this elevated price, one thousand dollars would be surreptitiously transferred to the exporter.

John Zdanowicz, a professor emeritus at Florida International University and a pioneer in the research of illicit financial flows through international trade, provided the following example of under-invoicing:

> Let me give you an example. If I am a drug dealer here in Miami and I have $1 million in cash that I want to move to a foreign country, let's say Colombia, I can go into downtown Miami in an afternoon and buy 200 gold watches for $5,000 each. So I've converted my million dollars in cash into a million dollars of a commodity, gold watches. I then export them to my colluding partner in the foreign country, but I invoice him $5 per watch. Therefore, I export the gold watches. He actually pays me $1,000 for those, which is just a transaction cost. Once the watches are in Colombia, they are sold in the open market for $5,000 each. Actually a few years back in Miami there were drug dealers buying Corvettes for $40,000 cash [and] exporting them to Latin American countries, and they were invoiced at $500 an automobile. And when they got into the Latin American countries, they were sold for $50,000. So not only do they launder $40,000, they made a $10,000 profit doing it.[11]

9 Evidence of J. Cassara, Transcript, December 9, 2020, p 51; Exhibit 341, Final Statement by John A. Cassara [Cassara Report], pp 14–15. Over- / Under-invoicing explained: Evidence of J. Gibbons, Transcript, December 10, 2020, pp 24–25. Multiple invoicing explained: Evidence of J. Gibbons, Transcript, December 10, 2020, pp 26–27. Phantom shipping explained: Evidence of J. Gibbons, Transcript, December 10, 2020, pp 26, 82. Misdescription explained: Evidence of J. Gibbons, Transcript, December 10, 2020, p 25. Although there is some debate over whether trade-based money laundering is distinct from trade fraud, the aim of trade-based money laundering is the concealment or legitimization of value through trade, whereas the aim of other trade-related predicate offences is the evasion of duties, tariff quotas, or other controls on goods.

10 It will also receive one dollar more per widget than what was reflected on the invoice and shipping documents, which helps to obscure the transfer of illicit funds.

11 Transcript, December 11, 2020, pp 122–123.

He also provided a number of extraordinary examples of trade mispricing, including plastic buckets imported to the United States from the Czech Republic with a declared price of $972 per bucket, toilet tissue from China imported at a price of over $4,000 per kilogram, and bulldozers shipped from the United States to Colombia at a price of $1.74 per bulldozer.[12]

Multiple Invoicing

Multiple invoicing occurs where the exporter issues multiple invoices for the same shipment of goods. The second invoice is completely fictitious. However, it creates a pretext for the transfer of money from a foreign importer to the domestic exporter.[13]

Over- and Under-shipping

Over- and under-shipping is similar to over- and under-invoicing, except that the exporter sells widgets to the foreign importer for the correct price (two dollars per widget) but includes more widgets than indicated on the shipping documents to transfer value to the foreign importer, or fewer widgets than indicated to transfer value into its home country.[14]

The common feature of these methods is that value (though not actual dollars) is secretively moved from one country to another, in a manner that obscures the real transaction. Such a process may also provide an explanation for certain funds (that they resulted from a particular transaction) and hide the real amount of value involved.

Falsely Described Goods and Commodities

In some cases, the importers and exporters involved in trade-based money laundering will falsely describe the goods and commodities being shipped in order to transfer value into or out of the country. The shipment of more valuable goods will result in a transfer of value to the foreign importer while the shipment of less valuable goods will result in a transfer of value to the domestic exporter when the invoice is paid.

New and Emerging Methodologies

While the export of goods through marine-containerized shipping remains the key driver of trade-based money laundering activity, it is important to note that there are a number of emerging methodologies. **Service-based money laundering** seeks

12 Exhibit 341, Cassara Report, p 17. Although these prices could be the result of input or classification errors in the database used in Professor Zdanowicz's study, they could also represent attempts to transfer value into or out of the United States.

13 Evidence of J. Gibbons, Transcript, December 10, 2020, pp 26–27.

14 As I understand it, **over- and under-shipping** refers to a situation where the price of the goods as set out on the trade documents is correct but the exporter ships a different number of goods than indicated. **Over- and under-invoicing** refers to a situation where the correct number of goods is shipped but the exporter manipulates the price of those goods to surreptitiously transfer value between countries.

to obscure the transfer of illicit funds through the trade of services as opposed to commodities. It presents difficulties for law enforcement because of the challenge in establishing market prices for specialized professional services.[15] It is particularly difficult to detect, given the absence of a database of services comparable to that for imports and exports.[16]

Phantom shipments, where money is transferred between importers and exporters through the financial system in order to settle a purely fictitious invoice without any physical movement of goods, have also emerged as a new typology.[17] Because the bank is not extending any kind of financing to the Canadian exporter or the foreign importer, it has a limited stake in the transaction and will not perform any real due diligence unless it sees other red flags associated with the transaction. Moreover, there are no customs declarations or shipping documents to fill out, with the result that the Canada Border Services Agency (CBSA) may not know about the trade unless the information comes to its attention through other sources.

I return to some of the unique challenges faced by CBSA and law enforcement agencies investigating trade-based money laundering later in this chapter.

Nature and Magnitude of the Threat

While the nature and prevalence of trade-based money laundering has never been systematically examined, there can be little doubt it poses a significant risk to Canada and Canadian institutions.

Bryanna Gateley, an intelligence analyst supervisor with the RCMP's Federal Serious and Organized Crime Border Integrity Unit and a former intelligence analyst with FINTRAC, testified that trade-based money laundering causes four types of harm to Canada:

- First, it has national security implications insofar as it gives criminals – including terrorists, extremists, and transnational organized crime groups – a relatively risk-free mechanism to repatriate illicit funds and continue their unlawful activities.
- Second, it leads to the perception that Canada is a jurisdiction of concern from a money laundering perspective (thereby leading to reputational harm).
- Third, it has the potential to cause harm to the economic security of the country, including the integrity of financial institutions and legitimate markets for goods and commodities. It also has the potential to undermine the foundation of macroeconomic policy decisions made by the federal government, insofar as it distorts the trade data that forms the basis of those decisions.

15 Evidence of J. Cassara, Transcript, December 9, 2020, pp 79–80.

16 Evidence of J. Zdanowicz, Transcript, December 11, 2020, p 195; see also Evidence of B. Gateley, Transcript, December 10, 2020, p 30.

17 Evidence of J. Gibbons, Transcript, December 10, 2020, pp 82–88; and Evidence of B. Gateley, Transcript, December 10, 2020, p 26.

- Fourth, the misdescription of goods and commodities on customs forms could result in less tax revenue being collected by the federal government (although the magnitude of that loss is unknown and there are some trade-based money laundering schemes that could theoretically result in more revenue being collected).[18]

While the magnitude of these harms or potential harms cannot be ascertained without further study, I agree with Ms. Gateley that trade-based money laundering poses a serious risk to Canadian and BC institutions and requires a meaningful response.[19]

A June 8, 2020, assessment by CBSA suggests that, *at a minimum*, hundreds of millions of dollars are being laundered through the trade in goods "to and through Canada each year." Moreover, it appears that a significant percentage of trade-based money laundering activity is carried out by professional money laundering organizations and networks.

A 2018 operational alert issued by FINTRAC warns that professional money launderers are using traditional trade-based money laundering techniques such as multiple invoicing to transfer illicit funds to complicit parties in other jurisdictions.[20] It also raises the spectre of Canadian businesses participating in underground currency exchanges such as the **black market peso exchange** (which is one of the best-known examples of trade-based money laundering).

In basic terms, the black market peso exchange and other similar exchanges allow transnational organized crime groups such as Mexican and Colombian cartels to move US drug-trafficking proceeds back to their home countries. From the perspective of the transnational organized crime group, the US drug money is "sold" to the black market peso dealer at a discount, with the cartel receiving "clean" money in its home country. However, the peso dealer must undertake a complex series of transactions in order to produce "clean" money for the transnational organized crime group in Mexico or Colombia. In a simple version of the scheme, the black market peso dealer may contact business owners in Mexico who want to buy goods or services from US vendors but need US dollars to purchase those goods. The peso dealer will arrange for the US drug money to be transferred to the US vendor to pay for the goods ordered by the business owner in Mexico. In return, it receives "clean" funds from the Mexican business owner, which are provided to the transnational organized crime group.[21]

Joel Gibbons, a senior analyst at CBSA and a senior program advisor to the Trade Fraud and TBML Centre of Expertise, testified that these schemes range from the simple

18 Evidence of B. Gateley, Transcript, December 10, 2020, pp 42–45.

19 A Government of Canada PowerPoint presentation dated April 28, 2018, suggests that the lack of reliable information with respect to the magnitude of the problem is the result of a "circular policy trap" whereby "resources are required to prove resources are needed"; see Exhibit 339, Overview Report: Trade-Based Money Laundering Publications and Records, Appendix CC, p 1063.

20 A copy of the FINTRAC alert that includes these risk factors is included as Appendix 38A.

21 Online: https://www.fintrac-canafe.gc.ca/intel/operation/oai-ml-eng. See also Evidence of J. Gibbons, Transcript, December 10, 2020, pp 63–69, and December 11, 2020, pp 35–36. Of course, there are many other versions of the scheme, some of which have a high level of complexity.

to the exceedingly complex and, more often than not, involve the shipment of goods through multiple jurisdictions in an attempt to obfuscate the audit trail. He stated:

> More often than not, goods are routed through multiple different countries all around the world, even in often-times nonsensical trading routes, before they ultimately arrive back at the jurisdiction where the criminal proceeds are destined. And so Canada, for example, can be used as just one node in a very complex international black market peso exchange scheme where the US could be involved – Canada, and imagine any number of countries around the world. And shipments are broken up at specific locations around the world to further obfuscate the trail of those goods. And so a customs service like mine may only be able to see just one leg in the international routing of goods that are involved in black market peso exchange schemes, and criminal actors are well aware of that, and they exploit it to their advantage. So, by breaking up one of these schemes into multiple jurisdictions where Canada or the United States don't really have any knowledge of how those goods are being declared in those foreign jurisdictions, the trail goes cold, and it's one of the many reasons that black market peso exchange schemes are such a concern and used to the extent that we believe they are by criminal actors.[22]

British Columbia may be particularly vulnerable to trade-based money laundering because of its international shipping ports; its large volume of international trade; and its stable, accessible financial system. For example, intelligence reports produced by the Criminal Intelligence Service British Columbia / Yukon Territory indicate that:

- There are organized crime groups in British Columbia that have the capability, knowledge, and transnational relationships to orchestrate trade-based money laundering schemes.
- These organized crime groups have the knowledge, skills, and relationships to manipulate trade chains and conduct complex foreign exchange transactions to commingle proceeds of crime with legitimate funds.
- Two BC-based organized crime groups were known to be involved in trade-based money laundering as of 2018 (though that is believed to be an under-representation, with the true scope of trade-based money laundering in British Columbia being a significant "intelligence gap").[23]

22 Evidence of J. Gibbons, Transcript, December 10, 2020, pp 68–69. The FINTRAC alert notes that the two variants of the scheme that FINTRAC observes most often involve (a) brokers sending suspected illicit funds held in Latin America or the United States to Canadian trading companies, wholesalers, dealers, and brokers via electronic funds transfer and, to a limited extent, cash couriers with these entities subsequently sending the funds to entities in places such as China, Hong Kong, and the United States to pay for the goods; and (b) brokers sending suspected illicit funds held in Latin America to US–based entities, as well as Chinese- or Hong Kong–based trading companies, through electronic funds transfer via a Canadian financial institution acting as a correspondent bank.

23 See Exhibits 352, 353, 354, 355, 356.

Staff Sergeant Sushile Sharma, a senior RCMP investigator with significant experience investigating trade-based money laundering schemes, gave an example of an investigation that involved the export of used vehicles and furniture from individuals in Vancouver to areas of Africa, including Tanzania and Nigeria. These goods were sold at a considerable profit, with the proceeds being used to purchase heroin at cheaper prices than in North America.[24] Female drug mules then transported the heroin back to North America on commercial flights, where it was sold at a profit. In some cases, the proceeds of those sales were used to purchase additional vehicles and furniture to continue the loop.[25]

After receiving information from an international partner, the RCMP determined that the individuals involved in that scheme were also involved in a "very, very, very sophisticated and far-reaching mass-marketing fraud ring operation extending … from Los Angeles to the Midwest as well as the eastern seaboard of America."[26] The proceeds of that fraud were making their way into the hands of their target and used to accumulate more goods, vehicles, and furniture to sustain the cycle.

Overall, I am satisfied that trade-based money laundering is a significant (and perhaps the most significant) money laundering threat facing this province. I am also satisfied that this problem is deserving of serious attention by law enforcement agencies, particularly at the federal level. I return to the law enforcement response to trade-based money laundering later in this chapter.

Goods Typically Used in Trade-Based Money Laundering Schemes

Trade-based money laundering schemes can involve a wide range of commodities ranging from high-value, low-volume goods (such as precious metals) to low-value, high-volume sectors (such as textiles). Generally speaking, preferable goods have the following qualities:

- they are easy to sell;
- they have wide pricing margins;
- they have extended trade cycles, meaning that they are shipped through multiple jurisdictions; and
- they are difficult for customs authorities to examine.

Mr. Gibbons testified that electronics and mobile phones are an attractive commodity for trade-based money laundering in Canada: these commodities are portable, easy to ship,

24 Evidence of S. Sharma, Transcript, December 10, 2020, p 109–11. Kilo-level heroin purchased off the east coast of Africa can run anywhere from $15,000 to $18,000 per kilo, whereas the kilo-level price of heroin in North America would be anywhere from $55,000 to $70,000 and sometimes even $80,000 per kilo.

25 Evidence of S. Sharma, Transcript, December 10, 2020, p 118.

26 Evidence of S. Sharma, Transcript, December 10, 2020, p 119.

easy to sell, and have a high value. Moreover, their descriptions can be easily manipulated and their values adjusted.[27] Other commodities vulnerable to trade-based money laundering include fresh and frozen food products, clothing, textiles, lumber and paper-based products, scrap metal, scrap plastic, precious metals and stones, and used vehicles.[28]

Mr. Cassara raised particular concerns about the international gold trade. He testified that, in his experience, some of the largest money laundering cases have involved misuse of the international gold trade. Gold, he said, is attractive to money launderers because it is both a commodity and a de facto bearer instrument that offers stability as well as anonymity to money launderers:

> Gold is a readily acceptable medium of exchange. It's accepted anywhere in the world. In times of uncertainty, gold offers stability. Gold offers easy anonymity to money launderers. Depending on the need … the form of gold can be easily changed or altered. It can be melted, smelted down. There's a worldwide market in cultural demand. Gold transactions can easily be layered or hidden. It's perfect for placement, layering, and integration. Old and varied forms can be easily smuggled. And by weight, it represents much more value than cash.[29]

Mr. Cassara went on to state that the countermeasures for the misuse of gold as a money laundering tool are known but have not been implemented in many jurisdictions:

> While there have been major investigations around the world involving the misuse of gold, precious metals, diamonds, and gems, it is not clear if cases have been made in Canada. Certainly, Canada is vulnerable. Canada has all the factors that would enable gold and precious gems to be used as a money laundering mechanism. Countermeasures are known. Gold in all its many forms should be an automatic red flag for customs, law enforcement, intelligence agencies, and bank compliance officers – particularly when the sourcing, destination, or routing is problematic. Trade data for gold in almost all its forms should be collected and analyzed. Anomalies should be identified and the results disseminated. Money laundering via the misuse of the international gold trade should be prioritized simply because gold represents one of the prime risks for laundering large amounts of money or transferring large amounts of value. Also, we know that gold manufacturers and dealers should set up [anti–money laundering / combatting the financing of terrorism] compliance programs. The challenge is that these common sense countermeasures are not sufficiently implemented.[30]

27 Evidence of J. Gibbons, Transcript, December 10, 2020, pp 94–98; Evidence of J. Gibbons, Transcript, December 11, 2020, pp 81–84; Exhibit 359, CBSA, *Electronics and Canadian Goods Returned / The Abuse of Tariff Codes 9813 and 9814 in TBML* (October 1, 2020).

28 Evidence of B. Gateley, Transcript, December 10, 2020, pp 35–37, 101–3; December 11, 2020, pp 51–52.

29 Transcript, December 9, 2020, p 110.

30 Exhibit 341, Cassara Report, p 34.

I agree with Mr. Cassara that gold is particularly vulnerable to trade-based money laundering. I also agree that there are a number of common sense countermeasures that could be put in place to deter the use of gold in trade-based money laundering schemes, and I would urge further study of this issue at the federal and provincial levels.

Another commodity frequently used in trade-based money laundering schemes is used vehicles.[31] Such vehicles may not hold their value long in the North American market, but they continue to hold their value in other parts of the world because of their scarcity.

Staff Sergeant Sharma testified that the US Drug Enforcement Administration has recently exposed a massive money laundering scheme involving the purchase of used cars by traders in West Africa (see Figure 38.1). His evidence with respect to that scheme illustrates the extreme complexity of many trade-based money laundering schemes as well as the manner in which other money laundering tools, such as informal value transfer systems, are used in conjunction with these schemes:

> So this graphic [on display] really is part of the United States Drug Enforcement, DEA's exposure of a massive money laundering scheme operated by Hezbollah for major drug cartels in South America. The scheme involved Lebanese banks wiring money to the United States for the purchase of used cars. These were transported to West Africa, which is known as a springboard location for the delivery of European-bound drug shipments and sold for cash. The cash from the used cars was mixed with drug proceeds and laundered using … Hezbollah-controlled hawalas.
>
> …
>
> From here the money was deposited into accounts at Lebanese Canadian banks, the branches in Lebanon, which [have] strong links with the Hezbollah. A portion of the funds that were deposited into these bank accounts were then wired back to the US to continue the trade of used cars to West Africa, and this all sustained the convoluted money laundering loop. So as you can see, there's a number of things happening here from this graphic, this slide. We're talking about drug trade. We're talking about the movement of vehicles from North America to Africa. We're then talking about the purchase of drugs on the continent of Africa and then the movement of those drugs into Europe.[32]

31 Exhibit 345, Canada, TBML Presentation (April 1, 2020), pp 19–21; Evidence of J. Gibbons, B. Gateley, S. Sharma, Transcript, December 10, 2020, pp 104–20; Exhibit 842, Luxury Vehicle – Case Scenario (redacted); Exhibit 843, Luxury Vehicle Sub Group (undated); Evidence of M. Paddon and B. Robinson, Transcript, April 14, 2021, pp 87–97. See also Exhibit 833, Peter M. German and Peter German & Associates Inc. *Dirty Money, Part 2: Turning the Tide – An Independent Review of Money Laundering in B.C. Real Estate, Luxury Vehicle Sales & Horse Racing*, March 31, 2019, pp 194–201.

32 Evidence of S. Sharma, Transcript, December 10, 2020, pp 105–6.

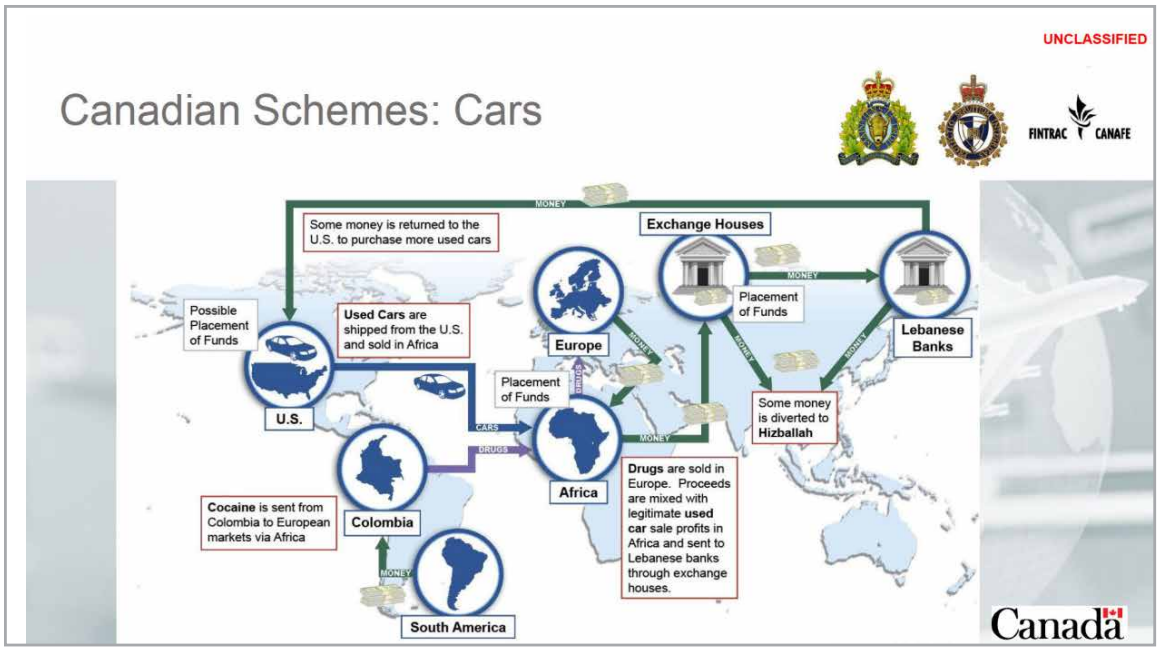


Figure 38.1: "Canadian Schemes: Cars"

Source: Exhibit 345, Government of Canada, Trade Based-Money Laundering Overview (April 1, 2020), p 19.

While the evidence before me is not such that I can make express findings with respect to this scheme, the evidence given by Staff Sergeant Sharma and others underscores the magnitude of the problem and the need to address this type of money laundering.

Types of Businesses Used in Trade-Based Money Laundering Schemes

Trade-based money laundering schemes can be carried out by a wide range of business types, including shell companies, freight forwarders, and customs brokers. Risk factors indicating that a particular business could be involved in trade-based money laundering include:

- rapid growth of a newly formed company into existing markets;
- evidence of consistent and significant cash payments, including those directed toward unrelated third parties;
- receipt of unexplained third-party payments;
- unnecessarily complicated and complex supply chains;
- unexpected pivots into an entirely unrelated sector (e.g., an information technology company becoming involved in the acquisition and distribution of bulk pharmaceuticals); and
- simultaneous involvement in more than one unrelated sector.

A 2018 FINTRAC alert contains a list of factors that may indicate a particular entity is part of a professional money laundering network. It states:

> **Indicators of trade-based money laundering by professional money laundering networks**
>
> - An entity is a Canadian small or medium-size import / export company, wholesaler, dealer or broker operating in a sector dealing in high-volume, high-demand commodities with variable price ranges, including agri-food, textiles, electronics, toys, lumber and paper, and automotive or heavy equipment.
> - The entity has business activities or a business model that is outside the norm for its sector, or conducts no business activities in Canada. It may also be difficult to confirm the exact nature of the business.
> - The entity transacts with a large number of entities that have activities in the above-noted sectors or have names that suggest activities in a wide range of unrelated sectors, and also does some or all of the following:
>   - receives a sudden inflow of large-value electronic funds transfers;
>   - orders electronic funds transfers to the benefit of China- or Hong Kong–based trading companies or individuals, and receives electronic funds transfers from the U.S. and Latin American countries;
>   - orders electronic funds transfers to the benefit of entities or individuals in the U.S., Mexico or Latin American countries, and receives such transfers from the U.S.;
>   - orders or receives electronic funds transfers to / from entities holding a bank account in Latvia or Cyprus, and are registered to addresses in the U.K., Cyprus, the British Virgin Islands, Panama, the Seychelles, Belize, the Marshall Islands or other offshore financial centers; and
>   - orders or receives payments for goods in round figures or in increments of approximately US$50,000.
> - A trading company based in the United Arab Emirates orders electronic funds transfers to the benefit of individuals or entities in Canada.
> - An entity's U.S. dollar business accounts held in Canada exhibit flow-through activity – that is, money is taken or transferred out of the account as quickly as it flows in.

- An entity imports currency (predominantly U.S. dollars) from Latin American countries.
- An entity makes large business purchases by credit card, funded by overpayments.
- An individual issues cheques, purchases drafts or orders electronic funds transfers through the account of a legal professional for trade-related payments.[33]

A 2020 CBSA report indicates that freight forwarders are particularly well-placed to control and direct trade-based money laundering schemes while disguising their role from law enforcement.[34] Freight forwarders occupy a pivotal place in most international supply chains. They are neither the seller nor the buyer of goods. Rather, they expedite the shipment of goods by helping buyers and sellers navigate complex shipping routes and customs processes. In one ongoing investigation, Canadian and foreign freight forwarders were believed to be manipulating the exporter and consignee information on both the Canadian export and overseas import declarations, in order to conceal the true identities of the originator and recipients of the goods on either side of the transaction.[35]

Many money laundering schemes also make use of third parties (i.e., parties with no apparent connection to the international trade transaction) to make payment on the invoices issued by the exporter, in order to reduce scrutiny on the transaction.[36]

Key Challenges Faced by Investigators

Trade-based money laundering schemes pose a number of unique challenges for customs authorities and law enforcement officials. The sheer volume of international trade and the impossibility of checking every transaction and shipment mean it is easy for trade-based money laundering to "hide in plain sight."[37]

Some estimates suggest that, globally, less than 2 percent of shipping containers are physically examined and that criminals "routinely" take advantage of customs processes by intentionally misstating the value, quantity, quality, weight, and descriptions of commercial goods in order to evade duty and regulatory requirements.[38]

33 A copy of the FINTRAC alert that includes these risk factors is included as Appendix 38A.

34 Exhibit 339, Overview Report: Trade-Based Money Laundering Publications and Records, Appendix Z, CBSA, Trade-Based Money Laundering Overview (June 8, 2020), p 1035.

35 Ibid, p 1035; ibid, Appendix T, CBSA, Knowledge Pool on Trade-Based Money Laundering (April 2020), pp 960–61.

36 Ibid, Appendix Z, CBSA, Trade-Based Money Laundering Overview (June 8, 2020), p 1034.

37 Evidence of J. Gibbons, Transcript, December 10, 2020, p 134. See also Evidence of J. Cassara, Transcript, December 9, 2020, pp 75–76; Exhibit 339, Overview Report: Trade-Based Money Laundering Reports and Records, p 60. A general discussion of the challenges faced by investigators in the investigation of money laundering is set out in Chapter 40.

38 Exhibit 357, CBSA – COVID-19 Implications for Trade Fraud, p 2.

Even if an examination takes place, it can be extremely challenging for border agents to value the commodities being shipped. For example, it is very difficult for a front-line customs agent to tell whether a particular shipment of gold is 18 or 24 carats (which has a substantial impact on value). Moreover, there is often no way for border agents to cross-reference the price that is actually paid for the product against the amount claimed on the shipping documents.

Mr. Gibbons provided an example of a trade-based money laundering scheme where the export declaration indicated that the value of the goods was $80,000, but $100,000 was transferred from the foreign importer to the Canadian exporter in order to transfer value into Canada. He testified that the commodity chosen was very difficult to value and examine. However, even if customs agents had examined the shipment, it would have been very difficult to uncover the fraud for various reasons, including the fact that CBSA does not have a systematic way to determine how much money was actually wired.[39]

While trade data may be collected by customs agencies, that information is often paper-based or buried within multiple databases such that it cannot be readily accessed by investigators. In some cases, the software used to aggregate data may not be compatible between agencies, a problem that leads to "information silos" and undermines the effective investigation of trade-based money laundering. Ms. Gateley summarized these challenges as follows:

> Additional challenges are that, as you would expect, the trade system is very opaque. It's often paper based. There [are] very long supply chains where you see various documents, including manifests, bills of lading, invoices moving around with the shipment and being processed by various entities, including ports, customs authorities, banks. Though trade data might be collected, the information needed can be buried within multiple databases that [are] really not readily available to analyze or it's not in a format that can be analyzed, especially if it's paper based. Or the trade data arrives just before or even after the product has been delivered, so … as my colleague Staff Sergeant Sushile [Sharma] has mentioned, it's kind of a day late and a dollar short. It's difficult to ascertain what actually happened after the fact and [to] verify what happened … [A]dditional challenges are software to analyze aggregate data [that] might not be compatible between agencies, so it's a puzzle piece that we have that needs to be shared amongst agencies so that we can build this larger puzzle of what the scheme is and who's involved. But if our basic software systems aren't compatible to be able to analyze that across various platforms [that] various agencies have, that creates a bit of an issue and an information silo. So essentially the upshot here is that we're missing a lot of these foundational pieces that are really needed to build the picture of what our [trade-based money laundering]

39 Evidence of J. Gibbons, Transcript, December 10, 2020, pp 71–74; Evidence of B. Gateley, Transcript, December 10, 2020, pp 134–36. Indeed, it may be only when goods or documents are examined in conjunction with other data that an otherwise innocuous shipment will appear suspicious.

> scheme is and who the threat actor is involved, in that information sharing at the domestic and international level is typically very ad hoc, case by case based, very target specific and very manual. So this can make it very difficult to take a macro look or step back as an analyst and extrapolate broader trends, indicators or determine the scope or the true scope of the issue.[40]

When trade-based money laundering is combined with other money laundering tools – such as the use of shell companies, offshore accounts, nominees, legal trusts, third-party payment methods, and cryptocurrencies[41] – it becomes exponentially more difficult for investigators to unravel these complicated schemes and to prove that each person involved in a scheme has the requisite degree of knowledge and control needed to secure a criminal conviction. Moreover, the investigation of trade-based money laundering offences often requires Canadian authorities to work with international partners in order to gather relevant information.

With a co-operative partner it can sometimes take months, if not years, to obtain relevant information through the mutual legal assistance treaty process. However, there are also cases where corruption, ambivalence, or even blind ignorance among foreign police departments makes the investigation of trade-based money laundering even more difficult. For example, Staff Sergeant Sharma gave evidence that his investigators had to be extraordinarily careful about the information they provided to a foreign police agency in one of his investigations because of concerns about corruption within that agency.

In light of these complexities, investigative agencies often focus on the predicate offence and leave the trade-based money laundering scheme unaddressed. This is highly problematic, given the volume of illicit funds that can be laundered through trade-based money laundering schemes and the impact of that activity on government institutions.

Measures Currently in Place

Investigating trade-based money laundering is largely a federal responsibility. Not only does it involve the manipulation of international trade transactions – an area of exclusive federal responsibility – but it is perpetrated by transnational organized crime groups and requires the co-operation of international partners to investigate.[42]

At present, four key players are involved in the federal response to trade-based money laundering in the province of British Columbia: FINTRAC, CBSA, the RCMP, and the Canada Revenue Agency.

40 Evidence of B. Gateley, Transcript, December 10, 2020, pp 135–36.

41 Evidence of J. Gibbons, Transcript, December 10, 2020, pp 28–29. By way of example, illicit funds can be commingled with funds from legitimate businesses, routed through uncooperative jurisdictions, or moved through the use of informal value transfer systems, a process that makes it difficult for investigators to follow the audit trail and prove that each person involved in the scheme has the requisite degree of knowledge and control.

42 At the same time, there may be a role for the Province in the investigation of trade-based money laundering schemes to the extent that part of the scheme occurs in British Columbia or involves BC companies. There may also be a role for the BC Civil Forfeiture Office in pursuing illicit assets located in British Columbia.

FINTRAC

FINTRAC plays a central role in the identification of trade-based money laundering through the receipt and analysis of suspicious transaction reports. While FINTRAC has received some reports concerning trade-based money laundering activity, there are a number of gaps in the current reporting regime that allow many trade-based money laundering schemes to go undetected.

Importers, exporters, customs brokers, freight forwarders, and other similar entities are not designated as reporting entities under the *PCMLTFA* and have no obligation to file suspicious transaction reports with FINTRAC. These businesses are on the front lines of trade-based money laundering and would undoubtedly be in a position to identify and report at least some suspicious activity.

Financial institutions have an obligation to file suspicious transaction reports concerning electronic funds transfers (sometimes referred to as wire transfers). However, these institutions do not have the opportunity to review sales documents, shipping invoices, or customs forms at the time they process these transfers. As a result, many suspicious transactions are not identified and reported, through no fault of the financial institution.

While financial institutions are better able to identify and report transactions that are processed using the trade finance tools reviewed earlier in this chapter, these transactions make up only about 20 percent of international trade transactions, and, in any event, the evidence suggests that trade-based money laundering may be hidden by a lack of access to financial information and a low degree of awareness of the problem within the capital markets divisions of many financial institutions.

Another complication is that lawyers, who often negotiate trade finance contracts, are exempt from anti–money laundering reporting requirements.

For these reasons, there is good reason to think that a significant percentage of trade-based money laundering activity in this country goes undetected by FINTRAC, and that law enforcement entities engaged in the investigation of trade-based money laundering must develop new ways of identifying and detecting such activity (see below).

Canada Border Services Agency

CBSA is primarily responsible for managing the flow of goods and people into and out of Canada. It manages all of Canada's ports of entry and has staff at the three major international mail-processing centres in Canada. It is important to understand that CBSA is not responsible for the investigation of money laundering and terrorist financing activity. Such investigations remain within the purview of the RCMP. However, CBSA has a role in the investigation of trade-based money laundering because of its role as a trade gatekeeper responsible for the identification of trade transactions indicative of trade fraud.

In identifying trade fraud and trade-based money laundering, CBSA is largely reliant on external sources of information. Financial disclosures from FINTRAC, which are received on a proactive basis and in response to voluntary information requests submitted by CBSA, provide the agency with one of its largest sources of information and will often be the starting point for further exploration of suspicious transactions.[43] Other sources of information include law enforcement bodies at the federal, provincial, and municipal levels, as well as requests from international partners, which often lead to a closer examination of Canadian companies believed to be engaged in trade fraud or trade-based money laundering activity.

CBSA also has border services officers at all of Canada's ports of entry, who are responsible for processing the importation and exportation of goods into or out of Canada. Where these officers have grounds to suspect that a particular transaction has indicators of trade fraud (e.g., where the description does not seem to match the goods they have examined, or where an exporter who is in one line of business presents customs documents for goods that are in a completely different sector), these transactions will be flagged in the system.

A separate program, described as the "trade" program, is responsible for the final accounting of goods once they have arrived in Canada, to ensure that all appropriate duties and taxes have been paid on the shipment. If investigators in that program develop grounds to suspect that any potential non-compliance is wilful, they can make referrals to CBSA's Intelligence and Enforcement Branch for further analysis.

Mr. Gibbons testified that CBSA is on the cusp of implementing a new information technology system known as the CBSA Assessment and Revenue Management (CARM) Project. The system will allow for advanced data analysis of imported goods and search for potential indicators of trade fraud and trade-based money laundering.

One example is **anomalous unit pricing**, where the individual unit price for a good being declared is inconsistent with the aggregate pricing ranges for previous importations of that same commodity. While these anomalies may be indicative of trade fraud or trade-based money laundering, it would be extremely difficult for a CBSA agent to detect pricing anomalies in shipments of similar goods without access to that software.

While the CARM system may provide some assistance in identifying suspicious transactions, the primary purpose of that software is to ensure compliance with revenue requirements such as duties and tax payments, and it has a number of important limitations for the investigation of trade-based money laundering, including the fact that it focuses on imports and does not compare Canadian prices with commodity prices in other countries. I return to this issue later in this chapter.

43 Evidence of J. Gibbons, Transcript, December 10, 2020, p 50.

RCMP

The RCMP has primary responsibility for the investigation of money laundering offences, including trade-based money laundering. While it has recently increased the number of investigators examining money laundering issues (see below), it is an "information consumer" in the sense that it largely relies on information and intelligence provided by other federal agencies in making operational decisions involving the investigation of money laundering offences. Moreover, I am unaware of any successful trade-based money laundering investigations or prosecutions in recent years.

In an expert report prepared for the Commission, John Cassara, a senior American money laundering expert, recommended the creation of a specialized unit within the RCMP to investigate trade-based money laundering.[44] Mr. Cassara testified that such a unit would reassure the public that trade-based money laundering is being taken seriously, and would pay for itself through the collection of increased taxes, duties, and forfeitures.[45] He also argued that it would allow for the development of specialized expertise in trade-based money laundering.

Staff Sergeant Sharma disagreed, and shared his view that trade-based money laundering does not need to be investigated as an "alien entity."[46] In his view, there are already money laundering investigators within the RCMP and trade-based money laundering is "just a more specialized manner of layering that investigators now need to be alive to."[47] He did agree, however, that more training is required, not just for law enforcement officials but also for all federal partners.

I agree with Staff Sergeant Sharma that the creation of a specialized unit to address trade-based money laundering may not be necessary, provided sufficient resources are dedicated to existing money laundering units and information pathways are created to ensure that the RCMP receives as much information as possible with respect to trade-based money laundering. I return to this topic in Chapter 39.

Canada Revenue Agency

The Canada Revenue Agency has a mandate to investigate criminal violations of the legislation it administers, including organized tax schemes and international tax evasion. It also works jointly with law enforcement on money laundering files, including those involving trade-based money laundering.

Recent Federal Initiatives

In the past few years, the federal government has announced two new initiatives aimed at addressing trade-based money laundering: the TBML Working Group and the Trade Fraud and TBML Centre of Expertise.

44 Exhibit 341, Cassara Report, p 35.

45 Ibid, p 36.

46 Evidence of S. Sharma, December 10, 2020, p 150.

47 Ibid.

TBML Working Group

In the summer of 2018, the officer-in-charge of the RCMP's Federal Serious and Organized Crime Financial Integrity Unit created the Interagency TBML Working Group. The intention was to bring together directors from various agencies, including the RCMP, CBSA, the Canadian Security Intelligence Service, and the Canada Revenue Agency to explore opportunities for these agencies to work together on trade-based money laundering. Unfortunately, however, the individual who spearheaded that project is no longer with the RCMP, and it is unclear whether the working group is still in existence or whether it has produced any tangible results.

Trade Fraud and TBML Centre of Expertise

In its 2019 budget, the federal government announced a number of initiatives aimed at strengthening Canada's anti–money laundering and anti–terrorist financing regime. One of those initiatives was the creation of a multidisciplinary Trade Fraud and Trade-Based Money Laundering Centre of Expertise.[48] Mr. Gibbons testified that the primary thrust of the initiative is to develop more institutional knowledge about trade-based money laundering, including the scope and scale of the problem, and to better position CBSA to leverage its capabilities under the *Customs Act,* RSC 1985, c 1 (2nd Supp.) and to work beside the RCMP in combatting trade-based money laundering activity.

CBSA officers are able to refer suspected money laundering files to the Trade Fraud and TBML Centre of Expertise, and these referrals may result in criminal investigations for trade fraud or trade-based money laundering. At the time of writing, the centre has received a number of potential leads, but no referrals have been made to criminal investigators. It remains to be seen whether the centre will continue to receive support from the federal government[49] and whether it will lead to any tangible law enforcement results.

Additional Measures

I heard evidence from a number of leading trade-based money laundering experts on steps that could be taken to address the problem. While many of these steps fall within areas of federal responsibility, I outline three of the most promising recommendations below.

48 More specifically, the federal government announced the investment of $28.6 million over four years beginning in 2020–21, with $10.5 million per year on an ongoing basis to fund 21 full-time-equivalent employees (FTEs): Exhibit 339, Overview Report: Trade-Based Money Laundering Reports and Records, p 556.

49 A PowerPoint presentation prepared by CBSA with respect to this initiative states that "incremental funding starting in 2022–23 is frozen" and that a report to the president of the Treasury Board is required by March 2022 to unlock funding for an additional 27 FTEs; Exhibit 339, Overview Report: Trade-Based Money Laundering Reports and Records, p 912.

Trade Transparency Units

One of the most promising recommendations is the creation of a trade transparency unit to collect customs and trade data and share that data with similar units in other countries in order to identify anomalies that might demonstrate over- and under-invoicing. The United States has had a trade transparency unit since 2004, and approximately 17 to 20 units are currently established worldwide.[50] As of 2015, the unit's network had seized over $1 billion in assets.[51] To help analyze that trade data, US Homeland Security investigations developed specialized software called the Data Analysis and Research for Trade Transparency System (DARTTS). DARTTS incorporates trade, customs, financial, and other data from across US agencies as well as customs services in partner countries.[52] Mr. Gibbons explained the operation of the system as follows:

> An example I often give when talking about trade transparency units are banana [exports] from Colombia. So think of a marine container that has bananas in it that's destined for the United States, it's destined for the port of Miami. The Colombian government gathers export information on the bananas that are departing Colombia and that are outbound for the United States, and on the US side the US government gathers import data for that same transaction. And … DARTTS … is able to cross-compare those two data points … the Colombian export transaction and the US import transaction … and it will cross-compare the elements of the customs declarations – the Colombian export, the US import – to see if they match. That's a relatively simple and simplistic explanation, but that's the fundamental underpinnings of the trade transparency unit concept.
>
> So if the bananas were declared as being valued at the equivalent of $100,000 US in Colombia but on the US side on import they're being declared to the US authorities as $2 million worth of bananas, you can see that you've now enabled the movement of the difference, so 1.9 equivalent US dollars, out of Colombia and into the United States. And the DARTTS system … is designed to detect those anomalies, so it's a form of proactive lead generation really for Homeland Security investigations to try to uncover trade fraud, including possibly trade-based money laundering.[53]

Mr. Gibbons testified that a trade transparency unit could, in principle, be an effective tool in the fight against money laundering. However, a 1987 memorandum of

50 Evidence of J. Cassara, Transcript, December 9, 2020, p 91; Exhibit 341, Cassara Report, Appendix 2; Evidence of J. Gibbons, Transcript, December 10, 2020, p 76.

51 Evidence of J. Cassara, Transcript, December 9, 2020, p 89.

52 There have, however, been implementation challenges. Mr. Cassara opined that those challenges stemmed primarily from insufficient financial and human resources: Evidence of J. Cassara, Transcript, December 9, 2020, pp 87–91.

53 Evidence of J. Gibbons, Transcript, December 10, 2020, pp 76–77.

understanding between Canada and the United States makes the implementation of that concept difficult in practice. Under the terms of that memorandum, Canada and the United States only collect data involving the *import* of goods into the two countries.[54] Export data – such as the value of goods when they leave the country – is not collected by either party, with the result that there is no useful way to compare the price of goods when they leave Canada against the price of goods when they enter the United States (and vice versa).[55] Accordingly, the creation of an effective trade transparency unit would likely require the renegotiation of the 1987 memorandum of understanding.

Canada could also create a trade transparency unit and enter into bilateral or multilateral agreements with other countries to identify anomalies that could demonstrate over- and under-invoicing. It is important to note, however, that the identification of anomalous transactions is only the first step in the investigation of trade-based money laundering and that significant human effort would be required to follow up on those red flags and determine whether they are, in fact, the result of mispricing or money laundering activity. There is little benefit to creating a trade transparency unit unless the federal government is willing to properly resource these follow-up efforts.

Advanced Data Analytics

Another solution is to use advanced data analytics to identify anomalies in the Canadian trade data. Such an initiative could assist in detecting and measuring the flow of illicit funds without the need to examine every shipment of goods into and out of the country.

While the CARM Project, discussed above, is one example of software that could allow for advanced data analysis of imported goods, that software appears to be more focused on compliance issues, such as tax and duty evasion, than on trade-based money laundering. For example, it only analyzes data from Canada and does not compare imports with commodity prices in other parts of the world.

Moreover, it focuses only on *imports* and does not analyze any export data, despite the fact that the Canadian export environment is more susceptible to trade-based money laundering than the Canadian import environment because of the significant volume of illicit funds moving from Canada to countries such as Mexico and Colombia.[56]

By contrast, Professor Zdanowicz has developed a methodology that involves examining US trade data purchased from the US Department of Commerce, Bureau of the Census, to identify anomalies that might assist in detecting and measuring the

54 Ibid p 79–80. Importantly, the memorandum of understanding applies to the import and export of goods only to and from the United States.

55 Ibid, pp 75–81. Export data is collected in the aggregate but no specific information is collected with respect to the declared value of goods when they leave Canada.

56 Evidence of J. Gibbons, Transcript, December 10, 2020, pp 55–59; Exhibit 993, Affidavit of Joel Rank, paras 17–18, 28, 40. In fairness, there is a separate reporting system for exports that was launched by CBSA in June 2020. However, there remains somewhat of an imbalance between border controls on exports and controls on the import side of the equation.

flow of illicit funds.[57] Examples of those anomalies include razor blades imported from Colombia at $34.81 per blade when the world average price was nine cents (a markup of about 38,000 percent) and emeralds imported from Panama at $974.58 per carat when the world average price was $43.63 (a markup of more than 2,000 percent).[58] While not all these transactions will be indicative of money laundering,[59] the anomalies identified through his analysis are, at the very least, worthy of investigation.

Professor Zdanowicz testified that anyone in the United States can purchase the trade data for the sum of $4,800 per year and that he routinely gets retained by organizations such as the World Bank, as well as financial institutions involved in trade finance, to perform his analysis. He also testified that the US trade data is updated monthly and that the analysis can be performed in real time.[60]

Professor Zdanowicz was asked to undertake a similar analysis of Canadian import and export data and generated five macro reports for the Commission that show the amount of money being moved into and out of Canada (and each of its provinces) from 2015 to 2019. In 2019, for example, $45 billion was moved out of Canada in undervalued exports, and $44 billion moved out of the country in overvalued imports, for a total of $90 billion. In British Columbia, there were more than $4.3 billion in undervalued exports and $4.1 billion in overvalued imports, for a total of $8.4 billion.

In terms of money moved *into* Canada, there were $20.34 billion in overvalued exports and more than $124 billion in undervalued imports, for a total of $144.44 billion, of which $16.5 billion was moved into British Columbia.

Professor Zdanowicz also produced four micro reports for British Columbia. These reports identified approximately 10,000 suspicious transactions, including:

- undervalued exports of digital cameras, resulting in the movement of a $5.4 million value from British Columbia to Australia;
- undervalued exports of smart cards, resulting in the movement of more than $148 million out of British Columbia;

57 In order to understand the technique used by Professor Zdanowicz, it is extremely helpful to watch the livestream of his testimony on December 11, 2020, which can be found here: https://www.youtube.com/watch?v=i5LjoNex9cY. The US trade data covers 239 countries and includes 9,084 unique commodity codes for exports and 18,243 unique commodity codes for imports to the United States.

58 Professor Zdanowicz's analysis also allows for the possibility of country-specific prices (as opposed to worldwide prices) to take into account the heterogeneity in goods imported from different countries. For example, clothing imported from France may be valued differently from clothing imported from Haiti.

59 For example, the anomalies could be caused by a data entry error or there could be a good reason for the increased price (such as the import or export of prototypes); see Evidence of J. Zdanowicz, Transcript, December 11, 2020, p 161.

60 Using updated data is critically important in conducting an effective analysis because commodity prices change over time: Evidence of J. Zdanowicz, Transcript, December 11, 2020, p 153. While Professor Zdanowicz's methodology is based on pricing data, he suggested that there are other ways of identifying anomalous transactions, including the weight of the imported goods. For example, he was able to identify briefcases imported from Malaysia at 98 kg per briefcase: Evidence of J. Zdanowicz, Transcript, December 11, 2020, p 142.

- undervalued exports of prefabricated wood buildings, resulting in the movement of a $4.2 million value out of British Columbia;
- overvalued imports of pistols, resulting in the movement of a $3 million value out of British Columbia;
- overvalued imports of beer, resulting in the movement of a $1.9 million value from British Columbia to Mexico; and
- undervalued imports of dishwashing machines from the United States, resulting in the movement of a $64.9 million value into British Columbia.

In producing these micro reports, Professor Zdanowicz reviewed every import and export transaction into and out of British Columbia in 2019 and used the statistical analysis outlined above to identify these, and other, anomalous transactions. While the data provided to Professor Zdanowicz does not include identifying information about the importer or exporter, that information is available and could be provided to law enforcement agencies once a suspicious transaction is identified.

Professor Zdanowicz was retained by the federal government in 2004 to make a presentation about his data analysis to FINTRAC and other government agencies. Unfortunately, however, it appears that no one followed up with him with a view to implementing this kind of analysis in Canada.[61] I consider his technique to be an extremely valuable tool insofar as it allows for the identification of anomalous transactions in real time without the need to examine every shipment into and out of the country. Moreover, it is noteworthy that Canada already has the data that would allow for the generation of a list of suspicious companies and individuals.

All law enforcement agencies with involvement in the identification and investigation of trade-based money laundering would do well to examine how Professor Zdanowicz's software (or other software with the same capability) could assist in the investigation and prosecution of trade-based money laundering activity. Indeed, his software would be useful not only in identifying trade-based money laundering activity but also in identifying professional money laundering organizations and networks operating in the province.

I therefore recommend that the dedicated provincial money laundering intelligence and investigation unit recommended in Chapter 41 take steps to implement and make use of that software as part of its intelligence functions.

Recommendation 88: I recommend that the dedicated provincial money laundering intelligence and investigation unit implement and make use of the software developed by Professor John Zdanowicz, or other software with the same capability, as part of its intelligence functions.

61 Evidence of J. Zdanowicz, Transcript, December 11, 2020, pp 108, 190.

Financial institutions involved in trade financing may also benefit from Professor Zdanowicz's software in order to ensure that they do not inadvertently facilitate the transfer of illicit funds into or out of the country.

Professor Zdanowicz also identified six red flags that may assist law enforcement agencies, financial institutions, and others to identify individuals and groups involved in trade-based money laundering activity:

- conducting business in high-risk jurisdictions;
- shipping products through high-risk jurisdictions;
- conducting transactions involving high-risk products (with high-risk products defined as products likely to give rise to anomalous transactions);
- misrepresentation of the quantity and type of products on customs documents;
- invoices that are inconsistent with customs documents; and
- obvious over- and underpricing of commodities (such as bulldozers shipped from the United States to Colombia at $1.74 per bulldozer).

Finally, I heard evidence that **distributed ledger technology** has promise in detecting and preventing trade mis-invoicing. I understand that the United States has applied such technology at cargo entry on a pilot basis,[62] and I would encourage all levels of government to explore the use of this technology as a tool in the fight against this form of money laundering.

Information Sharing

A repeated theme in the evidence on trade-based money laundering was the need for better information sharing among relevant stakeholders. At present, information sharing at the national and international level is typically ad hoc, targeted, and manual, which makes it difficult to get a macro analysis of trends or indicators in order to understand the scope of the issues.[63] For example, the software currently used to analyze aggregate data might not be compatible among agencies even within Canada (let alone internationally).[64] Mr. Gibbons explained that one reason that Canada does not have an integrated system is to ensure that each agency has access to information only when there are grounds to suspect that there is money laundering or non-compliance occurring within its sphere of authority. In other words, incompatibility between systems is a safeguard built into the system to protect privacy and *Charter* rights.[65]

62 Evidence of J. Cassara, Transcript, December 9, 2020, pp 100–1.

63 Evidence of B. Gateley, Transcript, December 10, 2020, p 136.

64 Ibid, pp 135–38.

65 Evidence of J. Gibbons, Transcript, December 10, 2020, p 140.

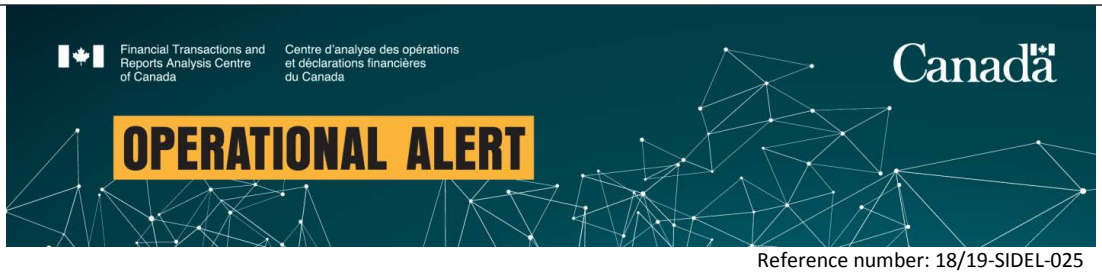
While I do not wish to diminish the importance of those rights, it may be that a more effective system would include compatible software with access limitations that could be overcome in appropriate instances. Ms. Gateley opined that the use of IT systems that are capable of sharing and analyzing big data sets and can "speak interagency" would be a structural improvement.[66] She also addressed the need to engage the private sector through public / private partnerships such as Project Athena (see Chapter 39) and to leverage non-traditional public sector partners such as Global Affairs Canada, Export Development Canada, and Industry Canada, which hold information that may be relevant to trade-based money laundering.

While information sharing is an important piece of any anti–money laundering regime, the collection and analysis of trade data is particularly important in addressing trade-based money laundering. All efforts should be made to ensure that government systems are at least capable of sharing relevant information when legally permissible, and that CBSA engages all relevant stakeholders in both the public and the private sectors. I would also note that improved trade data analysis and information sharing will only contribute to the identification and disruption of trade-based money laundering if sufficient resources are allocated to the agencies charged with investigating and prosecuting such activity.

In light of the fundamental importance of information sharing in addressing trade-based money laundering, I would urge British Columbia to work with the federal government to encourage improvements to trade data analysis and information sharing capabilities, as well as the resourcing of appropriate agencies to such a level that they can make meaningful use of this information.

66 Evidence of B. Gateley, Transcript, December 11, 2020, p 8.

Appendix 38A: FINTRAC – Operational Alert



Reference number: 18/19-SIDEL-025

July 18, 2018

Professional money laundering through trade and money services businesses

Professional money launderers are sophisticated actors who engage in large-scale money laundering on behalf of transnational organized crime groups such as drug cartels, motorcycle gangs and traditional organized crime organizations. Professional money launderers sell their services to these groups and are involved in the majority of sophisticated money laundering schemes; they are not members nor are they involved in the predicate offences that generate illicit proceeds. As such, they present unique identification challenges.

While professional money launderers may be accountants, bankers or lawyers, current financial intelligence suggests that they often are owners of, or associated with, trading companies or money-services businesses. Professional money launderers use their occupation and knowledge, as well as the infrastructure associated with their line of work and their networks, to facilitate money laundering, providing a veneer of legitimacy to criminals and criminal organizations.

This operational alert provides indicators for money laundering carried out through trade and money services businesses. Entities required to report to FINTRAC should use these indicators on their own and in combination to identify potential professional money laundering activities. Reporting entities should also use these indicators in conjunction with a risk-based approach and other money laundering indicators. Financial institutions are especially well positioned to recognize and report on suspicious financial transactions that may be connected to professional money laundering. FINTRAC uses these indicators, along with other sources of information, to assess reporting entities' compliance with their reporting obligations.

Trade-based money laundering

Professional money launderers use trade transactions to legitimize proceeds of crime and move them between jurisdictions and between currencies. FINTRAC has observed two main schemes of this type.

- Schemes involving falsified customs, shipping and trade finance documents, including the following:
  - Phantom shipments: Transferring funds to buy goods that are never shipped, received or documented.
  - Falsely described goods and services: Misrepresenting the quality, quantity, or type of goods or services traded.
  - Multiple invoicing: Issuing a single invoice but receiving multiple payments.
  - Over/under invoicing: Invoicing goods or services at a price above or below market value in order to move money or value from the exporter to the importer or vice-versa.
- The Black Market Peso Exchange, which typically works as follows:
  - Transnational organized crime groups, such as Colombian or Mexican drug cartels, place proceeds of crime into the U.S. financial system through structured cash deposits (deposits that are organized to avoid record-keeping or reporting requirements) of U.S. dollars.

1

- A Colombian or Mexican importer buys those dollars from complicit brokers, paying for them in pesos.
- The importer uses the U.S. funds to purchase goods that are then shipped to Colombia or Mexico.
- The brokers return the pesos they received from the importer to the cartel.

There are many variations on the Black Market Peso Exchange—which is essentially a form of unregistered foreign currency exchange—involving locations other than Latin America, other criminal groups and other world currencies (although the U.S. dollar is the most common). The two versions FINTRAC observes most often are the following:

- Brokers send suspected illicit funds held in Latin America or the U.S. to Canadian trading companies, wholesalers, dealers and brokers via electronic funds transfer and, to a limited extent, cash courier. These entities subsequently send the funds to entities in multiple jurisdictions, including China, Hong Kong and the U.S., to pay for goods.
- Brokers send suspected illicit funds held in Latin America to U.S.-based entities of varying types, as well as to China- or Hong Kong-based trading companies, through electronic funds transfer via a Canadian financial institution acting as a correspondent bank.

Indicators of trade-based money laundering by professional money laundering networks

- An entity is a Canadian small or medium-size import/export company, wholesaler, dealer or broker operating in a sector dealing in high-volume, high-demand commodities with variable price ranges, including agri-food, textiles, electronics, toys, lumber and paper, and automotive or heavy equipment.
- The entity has business activities or a business model that is outside the norm for its sector, or conducts no business activities in Canada. It may also be difficult to confirm the exact nature of the business.
- The entity transacts with a large number of entities that have activities in the above-noted sectors or have names that suggest activities in a wide range of unrelated sectors, and also does some or all of the following:
  - receives a sudden inflow of large-value electronic funds transfers;
  - orders electronic funds transfers to the benefit of China- or Hong Kong-based trading companies or individuals, and receives electronic funds transfers from the U.S. and Latin American countries;
  - orders electronic funds transfers to the benefit of entities or individuals in the U.S., Mexico or Latin American countries, and receives such transfers from the U.S.;
  - orders or receives electronic funds transfers to/from entities holding a bank account in Latvia or Cyprus, and are registered to addresses in the U.K., Cyprus, the British Virgin Islands, Panama, the Seychelles, Belize, the Marshall Islands or other offshore financial centers; and
  - orders or receives payments for goods in round figures or in increments of approximately US$50,000.
- A trading company based in the United Arab Emirates orders electronic funds transfers to the benefit of individuals or entities in Canada.
- An entity's U.S. dollar business accounts held in Canada exhibit flow-through activity—that is, money is taken or transferred out of the account as quickly as it flows in.
- An entity imports currency (predominantly U.S. dollars) from Latin American countries.
- An entity makes large business purchases by credit card, funded by overpayments.
- An individual issues cheques, purchases drafts or orders electronic funds transfers through the account of a legal professional for trade-related payments.

2

Money services businesses

Money services businesses provide a wide range of unique and valuable financial services to Canadians and international customers; however, the sector has unique challenges and risks with respect to money laundering. Most money services businesses engage in legitimate activities but some allow professional money launderers to exploit their services with their full cooperation. Others turn a blind eye to the fact that they are serving criminals. Professional money launderers who own or are connected to money services businesses use these entities to place and transfer illicit funds.

Indicators of professional money laundering through money services businesses

- A Canadian money services business does some or all of the following:
  - receives a sudden inflow of large electronic funds transfers and cash deposits; this is followed by an increased outflow of electronic funds transfers, cheques and bank drafts made out to multiple unrelated third parties for loans or investments, or to the individual conducting the transaction;
  - undertakes numerous currency exchanges involving Canadian and U.S. dollars and/or Euros;
  - carries out business largely with or through Iran or other countries subject to sanctions, the United Arab Emirates, Kuwait, Hong Kong, and China or countries with internal capital controls; and
  - receives electronic funds transfers from foreign exchange and trading companies based in the above-noted countries for real estate transactions, loans or investments.
- A money services business owner, associate or employee does some or all of the following:
  - maintains personal account activity similar to that of a money services business;
  - attempts to avoid reporting obligations when exchanging currency on behalf of another money services business;
  - lists multiple occupations, addresses and/or telephone numbers with financial institutions or online;
  - lists occupation as immigration consultant, student, homemaker or unemployed;
  - lives outside of their reasonable means (i.e., buys real estate beyond what they could reasonably afford on their claimed income);
  - attempts to close an account(s) to avoid due diligence questioning;
  - receives wires and transfers from multiple sources in accounts at numerous banks and credit unions; the individual then depletes these amounts through drafts payable to self or for real estate purchases;
  - places large structured cash deposits into the same account at multiple locations on the same day; and
  - is a customer at many banks and credit unions, and negotiates many self-addressed bank drafts from various financial institutions.
- A Canadian import/export company has account activity similar to that of a money services business, including the following:
  - receives one or two large electronic funds transfers and then orders multiple outgoing cheques and drafts to multiple third-party individuals and companies; and
  - receives large incoming electronic funds transfers from Iran, the United Arab Emirates, Kuwait, Hong Kong and China for living costs, expenses or spare parts.

3

Reporting to FINTRAC

To facilitate FINTRAC's disclosure process, please include the term **#pml** in Part G—Description of suspicious activity on the Suspicious Transaction Report. (See also, STR guidance.)

Contact FINTRAC

- **Email:** guidelines-lignesdirectrices@fintrac-canafe.gc.ca (include Operational Alert 18/19-SIDEL-025) in the subject line)
- **Telephone:** 1-866-346-8722 (toll free)
- **Facsimile:** 613-943-7931
- **Mail:** FINTRAC, 24th Floor, 234 Laurier Avenue West, Ottawa ON, K1P 1H7, Canada

Cat. No. FD4-16/2018E-PDF
ISBN 978-0-660-27307-5

FINTRAC Operational Alerts provide up-to-date indicators of suspicious financial transactions and high-risk factors related to new, re-emerging or particularly topical methods of money laundering and terrorist activity financing.