Part IX
Other Sectors

Chapter 34
Luxury Goods

Section 4 of the Commission's Terms of Reference directs me to make findings and recommendations with respect to the extent, growth, evolution, and methods of money laundering in the luxury goods sector.

This chapter sets out my findings and recommendations with respect to this sector. I begin by discussing the meaning of the phrase "luxury goods" in this context and the process undertaken by the Commission to examine money laundering in this aspect of the province's economy. As I discuss below, I propose an expansive approach to determining what a luxury good is, based on four features that such goods possess. While the bulk of this chapter is devoted to luxury *goods*, I note at the outset that some *services* also present money laundering risks; I return to this topic later and include services in the recommendations I make at the end of this chapter.

After reviewing the nature of luxury goods, I discuss the risk of money laundering and evidence that money laundering is actually occurring in luxury goods markets, as well as the implications of the manner in which these markets are organized and regulated. I then set out a general model for addressing money laundering risks in luxury goods markets and the role that may be played by a permanent AML Commissioner, the creation of which is recommended in Chapter 8.[1] The flexible model I propose in relation to luxury goods is centred on principles that can be adapted to the nature of different luxury goods markets and the varying risk levels they present. I conclude this chapter by addressing money laundering in the motor vehicle market and by briefly discussing recent steps taken by the Insurance Council of British Columbia to address money laundering in the insurance industry.

1 As I explain in Chapter 8, I expect that the AML Commissioner will require a team to assist him or her with the various duties I am proposing. As such, my references to the AML Commissioner should be taken to include the commissioner's office.

While I am not in a position to identify with precision the extent to which money laundering is occurring in the luxury goods sector, it is evident from the evidence before me that this sector is at a high risk of being exploited for money laundering or spending of criminal proceeds and that, to some degree, this risk has been realized in the form of actual money laundering activity. The risk of money laundering associated with this sector arises, in part, from the inherent features of luxury goods and the markets in which they are traded. In this province, however, it is clear that this risk has been exacerbated by a near-complete absence of visibility into and scrutiny of what is taking place within this sector of the economy. In my view, it is essential that the Province take immediate action to drastically reduce this risk and ensure that the luxury goods sector is not exploited for money laundering moving forward.

What Are "Luxury Goods"?

My Terms of Reference do not define the phrase "luxury goods," and the parameters of this sector are more ambiguous than those of some other listed economic sectors, such as real estate or gaming. Given this ambiguity, it is necessary to comment briefly on the meaning of the phrase, how it has been used in previous study and analysis of money laundering in this sector, and how it is used in this Report.

The notion that money laundering may occur through luxury goods markets is not new. To the extent that the luxury goods sector has been a focus of anti–money laundering scholarship and analysis in the past, this work has tended to focus on specific luxury goods markets. As examples, Dr. Peter German was directed to focus on luxury vehicles in his second report,[2] the Financial Action Task Force has released separate reports focused on the markets for gold[3] and diamonds,[4] and several academic publications have examined the risk of money laundering in the fine arts market.[5] A 2017 report prepared by Transparency International addressed the risk of money laundering in several luxury goods markets, including those for fine art, precious stones and jewels, super-yachts, and "personal luxury items" (which encompass accessories, apparel, watches and jewellery, and perfume and cosmetics).[6] While the Transparency International report considers several different luxury

2 Exhibit 833, Peter M. German, *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 [*Dirty Money 2*], p 167.

3 Exhibit 4, Overview Report: Financial Action Task Force, Appendix WW: FATF, *Money Laundering / Terrorist Financing Risks and Vulnerabilities Associated with Gold* (Paris: FATF, 2015) [*FATF Report: Gold*].

4 Exhibit 4, Overview Report: Financial Action Task Force, Appendix XX, FATF, *Money Laundering / Terrorist Financing Through Trade in Diamonds* (Paris: FATF, 2013) [*FATF Report: Diamonds*].

5 Saskia Hufnagel and Colin King, "Anti-Money Laundering Regulation and the Art Market" (2019) 40(1) *Legal Studies* (Society of Legal Scholars); Hannah Purkey, "The Art of Money Laundering" (2010) 22(1) *Florida International Law Journal*; Katie L. Steiner, "Dealing with Laundering in the Swiss Art Market: New Legislation and its Threats" (2017) 49(1–2) *Case Western Reserve Journal of International Trade Law*; Fausto Martin De Sanctis, *Money Laundering Through Art: A Criminal Justice Perspective* (Cham, Switzerland: Springer, 2013).

6 Exhibit 774, Overview Report: Luxury Goods, Appendix A, Transparency International, *Tainted Treasures: Money Laundering in Luxury Markets 2017* [*TI Tainted Treasures 2017*], pp 34, 49.

goods markets, it largely treats them as separate markets rather than a single economic sector.

These past efforts to examine money laundering in luxury goods markets offer examples of the types of items that may qualify as luxury goods but provide little insight into how this category ought to be defined, or how to determine what is *excluded* from it. While it may not be difficult to identify examples of products that intuitively qualify as luxury goods, in my view, defining "luxury goods" only by way of example is of little value for the purpose of understanding and addressing the risk of money laundering in this sector.

Rather, I believe that, for this purpose, the category of "luxury goods" should be understood to be a broad and open one defined by the nature of the money laundering risk presented by the markets and products in question. As I discuss in more detail below, the money laundering risk posed by luxury goods markets is derived in large part from four features: their high value, their capacity to retain value, their transferability, and their portability.

While the unique features of individual luxury goods markets – such as the traditions of confidentiality and discretion in the fine art world,[7] or the capacity of precious metals and stones to serve as mediums of exchange[8] – may further contribute to the money laundering risk in these markets, any market at risk of money laundering because of the four features I have just identified should be considered a luxury goods market for anti–money laundering purposes. This definition, which should be understood to apply to the use of the phrase "luxury goods" throughout this Report, encompasses conventional luxury goods such as yachts, jewellery, and fine art, but also includes products that may not immediately come to mind as falling within this category, such as electronics, vintage wine, event tickets, or sports and entertainment memorabilia. One might reasonably argue that a more inclusive phrase such as "high-value goods" may more accurately capture this category, but in the interest of consistency with my terms of reference, I will continue to use the phrase "luxury goods" throughout this Report.

In my view, this broad and open definition is preferable to a fixed list of examples of luxury goods for two reasons. First, it recognizes that the products and markets that may fall within this category are numerous and constantly evolving, underscoring the need to continually search for additional markets that bear a similar risk and that should be subjected to anti–money laundering scrutiny. A closed list of existing markets risks creating the incorrect impression that if the money laundering risk associated with the goods sold in those particular markets can be addressed, money laundering through luxury goods would cease to be a cause for concern. In reality, however, even in the

7 Exhibit 774, Overview Report: Luxury Goods, paras 2, 57, 60; Appendix D, Responsible Art Market Initiative, *Guidelines on Combatting Money Laundering and Terrorist Financing* (2017) [*Art Trade Guidelines*], p 103; Appendix F, United States Senate, Permanent Subcommittee on Investigations: Committee on Homeland Security and Governmental Affairs, *The Art Industry and U.S. Policies that Undermine Sanctions* (2020) [*Art Industry and Undermining Sanctions*], p 121.

8 Exhibit 774, Overview Report: Luxury Goods, paras 35–38.

unlikely event that a comprehensive list of such markets could be compiled, this list would quickly become obsolete as markets for new products emerge. I note as examples the growth in consumer electronic goods in recent years, including the introduction of many new products to the marketplace, and the very recent advent of "non-fungible tokens," which clearly fall into this category but would likely not have been included on a list of luxury goods markets even at the time that this Commission was established in 2019.

The second reason why a broad, open definition is preferable is that it encourages those engaged in the fight against money laundering to think of these diverse markets as a unified economic sector for the purpose of preventing money laundering. Because the money laundering risks associated with these markets are similar, they may be viewed by those intent on laundering the proceeds of crime as largely interchangeable. Accordingly, addressing money laundering in one luxury goods market may be of little use to the province as a whole if the effect is simply to displace this illicit activity to another sector of the province's economy. This risk of displacement has important implications both for the type of anti–money laundering measures to be implemented and for the sorts of bodies or agencies best able to implement those measures. For example, providing new resources and authorities to regulators responsible for single markets – or even the creation of new regulators – may be a sensible approach if the objective is to eliminate money laundering in the market for a single luxury good, but may be of little utility in addressing money laundering *throughout* this sector. Defining luxury goods as a broad category rather than as a list of individual markets maintains a focus on this economic sector broadly, rather than on the loose collection of individual markets that may be commonly thought to comprise it.

The Commission's Process

The Commission undertook extensive efforts to examine money laundering in various luxury goods markets in British Columbia. These efforts included consultation with experts in Canada and internationally, review of relevant literature, and obtaining records from and interviewing representatives of trade associations, regulatory bodies, and businesses operating in various luxury goods markets within the province. Through these efforts, the Commission developed an in-depth understanding of the risk of money laundering in this sector and identified indicators of actual money laundering in the markets that it comprises.

Despite these efforts, Commission counsel elected not to devote significant hearing time to the luxury goods sector. This should not be taken as an indication that the Commission assessed the luxury goods sector as an area of low priority or low risk. Rather, the nature of this sector was such that it was not necessary for the Commission to devote as much hearing time as it did to others.

While the information obtained by the Commission is sufficient to allow me to draw conclusions regarding the risk of money laundering in luxury goods markets in this

province and identify indicators that this activity is actually occurring, it is necessary to acknowledge two factors that limited the Commission's efforts in this sector.

The first of these factors is the COVID-19 pandemic. While the pandemic had an impact on all aspects of the Commission's work, few areas were as significantly affected as its inquiries into the luxury goods sector. The Commission's intended approach to this sector included the engagement of private investigators to seek out information by attending luxury goods retailers, identifying and cultivating sources of information about these businesses and industries, and gaining insight into whether and where activity that may be associated with money laundering is taking place in these industries. These investigative efforts commenced in early 2020 but came to a halt almost immediately following the onset of the COVID-19 pandemic. Due to the initial closure of many retailers, changes in their operations, and concern for the safety of Commission and retailer staff and the broader public, it was not possible to pursue these investigations as initially planned. The Commission quickly adjusted its approach and made contact with a number of luxury goods retailers, obtaining relevant documents and conducting remote interviews. While this process yielded valuable information, it is impossible to say how it compares to what the Commission would have learned had it been able to execute its original plan.

The second limitation faced by the Commission in its investigations into money laundering in the luxury goods sector was legal restrictions on the extent to which the Commission was able to collect information. In particular, despite the summons power set out in the *Public Inquiry Act*, SBC 2007, c 9, the Commission faced limits in its ability to obtain information related to provincial sales tax rebates for vehicles exported from the province and to records held by the Vehicle Sales Authority, which regulates motor vehicle dealers and salespeople. These comments are in no way meant to suggest that these records and information were improperly withheld from the Commission. To the contrary, I am satisfied that those in possession of those records were properly complying with the governing legislation. However, the reality is that the Commission's ability to inquire into money laundering in the luxury goods sector was, to some degree, hampered by these limitations.

I do not believe that these limitations significantly affected the Commission's ability to fulfill its mandate with respect to this sector. Rather, I consider it necessary to identify them for two reasons. First, as this is a public inquiry, I believe that, to the extent possible, it is important that I explain to the public the steps the Commission did and did not take and, where the Commission did not take what may seem to be logical steps, the reason why those steps were not taken. Second, the above-noted limits on the Commission's ability to obtain information are likely to inhibit future efforts to obtain the same information by others concerned with combatting money laundering in the province, including the AML Commissioner. By identifying these limits here, my hope is that steps can be taken to ensure that these barriers do not restrict future efforts to address money laundering in British Columbia.

Money Laundering Risk in Luxury Goods Markets

While the luxury goods sector is comprised of a diverse set of markets for a broad range of products, these markets are unified by the money laundering risk that they face. Broadly speaking, the luxury goods sector is at risk of money laundering in three forms:

1. **Luxury goods as a means of laundering money:** The first form of money laundering through luxury goods – a more traditional one – involves using luxury goods as a means of storing the value of the proceeds of crime so that they can be dealt with in a manner that would be difficult or impossible if the illicit funds remained in the form in which they were originally obtained and give the funds a façade of legitimacy when the goods are sold. In this form, luxury goods are a means to an end, acquired *for the purpose of* laundering money.
2. **Use of proceeds of crime to purchase luxury goods for use and enjoyment:** The second form of money laundering risk facing the luxury goods sector involves the use of proceeds of crime to acquire luxury goods, such as luxury automobiles or yachts, for the purpose of using and enjoying those goods. In this form, the acquisition of luxury goods is an end in itself. The goods are not acquired solely for the purpose of laundering money; however, they ultimately serve the purpose of storing value and giving the proceeds a façade of legitimacy when sold.
3. **Use of luxury goods in the "Vancouver model":** As I expand below and in Chapter 2, the "Vancouver model" involves lending proceeds of crime to individuals who were not directly involved in the criminal activity that generated those proceeds (and who may not be aware of their illicit origins), with the expectation that the loan will be repaid in another form and/or location. It seems highly likely that money laundering has occurred through the Vancouver model in the luxury goods sector, with those receiving the illicit funds using them to purchase luxury goods.

In what follows, I review these three forms of money laundering in more detail.

My focus in this chapter is primarily on luxury *goods*, as stipulated in my Terms of Reference. However, I note that there are at least two ways that *services* can be used to launder money. First, an individual may ostensibly pay for services, but those services are not in fact performed. This allows for the movement of illicit funds and an appearance of legitimacy of the funds in the hands of the purported service provider. Second, individuals who receive illicit funds as part of the Vancouver model can spend those funds on services. As the model ultimately requires repayment from the individual who was loaned the funds, the use to which those funds are put by the borrower is immaterial to the successful laundering of the illicit funds. As such, their use to purchase services furthers the aims of the money laundering scheme as effectively as their use to gamble, purchase luxury goods, or for any other purpose. The two methods of money laundering through services raise significant risks and concerns; I have therefore included services in the recommendations I make at the end of this chapter.

Luxury Goods as a Means of Laundering Money

The first money laundering risk arises from the possibility that proceeds of crime can be used to acquire goods, which can then be held, transferred, sold, and/or transported. This is done in order to store value, convert value, or transfer it to another location, jurisdiction, or person. This in turn obscures the source of funds initially used to acquire the luxury good and/or the movement of the value stored in that good.

The nature of this risk was captured in a 2015 report prepared by the Europol Financial Intelligence Group titled *Why Is Cash Still King?* (which uses the phrase "high value goods" in place of "luxury goods"):

> Typically, the reason for using high value goods (such as watches, art works, luxury vehicles, precious metals and jewels) or real estate is that they offer criminals an easy way to integrate funds into the legal economy, converting criminal cash into another class of asset which retains its value and may even hold opportunities for capital growth.
>
> ...
>
> Another reason that attracts criminals to the purchase of high value goods is that certain items, such as gold or precious stones, are readily liquid and moveable asset classes which can be traded globally. As these items have a very high value, just like high denomination notes, they offer criminals the opportunity to shrink bulky cash holdings into discrete and portable holdings of gold or diamonds, for example. These items can be smuggled across borders and thereafter sold ... [T]hese items are not captured under European cash control regulations and as such have an added advantage in that they need not be declared.[9]

The risk that luxury goods may be used to launder money in this way arises primarily from the four features common to luxury goods that I identified above: their high value, capacity to hold value, transferability, and portability. There are, of course, additional features of specific luxury goods markets that may exacerbate or attenuate these risks for specific markets. In my view, however, these four features are the primary sources of the risk of this form of money laundering that afflicts the sector as a whole, and they are useful in defining what should qualify as a luxury good for the purpose of combatting money laundering in British Columbia.

High Value

The first, and most obvious, feature of luxury goods that contributes to the risk of money laundering is their high value. The value of luxury goods is relevant to money laundering risk because the more expensive a good, the greater the volume

9 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* (2015) [*Europol Cash Report*], p 36.

of illicit funds that can be converted into that good. This enables the laundering of proceeds of crime because it permits the more efficient conversion, transfer, or transportation of illicit funds. Where, for example, a substantial volume of illicit cash is used to purchase a single piece of jewellery or work of art, the cash is converted into a different form in a single transaction, and the value of that cash can be much more easily stored or transported than could the cash itself or a larger volume of less expensive goods. Moreover, the luxury good can be converted back into cash or another monetary instrument in a single transaction, rather than a series of transactions, which would be required to convert a large quantity of less expensive goods. This should not be taken to suggest that money laundering cannot be accomplished through the purchase of lower-value goods – particularly if purchased in high volumes – or that lower-value goods should not be the subject of anti–money laundering scrutiny; rather, in my view, the risk associated with particular markets will typically increase with the value of the goods sold in that market.

Capacity to Retain Value

A second feature of luxury goods that gives rise to an elevated risk of money laundering is their capacity to retain value. Goods like vehicles, yachts, jewellery, and fine art are not perishable and do not typically become valueless following purchase, as evidenced by the robust markets for used or pre-owned goods in each of these categories. While some of these items may decline in value, if purchased with the proceeds of crime, these items can be relied on to retain at least a portion of the value of those illicit funds while offering relief from the burden and inconvenience of storing and concealing large quantities of cash – as well as the suspicion that large amounts of cash may attract.

Transferability

The utility of luxury goods in efforts to launder money is further enhanced by the relative ease with which these goods can be transferred to others.[10] As noted above, because luxury goods tend to retain their value following purchase, there are relatively robust markets for used or pre-owned goods in many of these categories. This facilitates money laundering by ensuring that a bad actor can reasonably expect to be able to transfer the good to another person and, in doing so, extract the value retained by the good after it was acquired with the proceeds of crime. This feature of these goods may also facilitate the transfer of value for criminal purposes other than through the exchange of cash by permitting that value to be transferred through the delivery of a good, rather than cash itself.

The transferability of these goods is also useful to those intent on laundering money, as it enables the creation of a legitimate explanation for criminally derived property. Where a luxury good acquired with the proceeds of crime is resold, the funds obtained through the resale can be explained as the proceeds of the sale of the luxury good, obscuring the criminal origins of the funds initially used to acquire the item.

10 Exhibit 774, Overview Report: Luxury Goods, paras 37–38.

Portability

A further common feature of luxury goods that contributes to the risk of money laundering posed by this sector is the portability of these goods.[11] Goods like jewellery, electronics, and works of fine art are often relatively compact and easily transported. Some items within this category, such as vehicles and yachts, are themselves modes of transportation. The portability of these goods allows the value of the proceeds of crime stored in these items to be moved between locations – and potentially jurisdictions – easily and without attracting the scrutiny often directed at large volumes of cash.

Additional Features of Specific Luxury Goods

There are, of course, other features of certain luxury goods markets that may further contribute to a risk of money laundering. The risk of money laundering through fine art, for example, is elevated by the industry's traditions of confidentiality and discretion,[12] while the risk of money laundering through jewellery and precious metals and stones is exacerbated by their capacity for use as a medium of exchange, obviating the need to convert them to currency before they can be spent.[13] These additional features do not apply to all luxury goods, but illustrate how the features listed above, which are of more general application and unify the luxury goods sector, may be exacerbated by other characteristics.

Using Risk to Define the Sector

In my view, and for the reasons outlined in detail above, the foregoing four characteristics are a useful means of defining this otherwise amorphous sector of the economy. Efforts to combat money laundering through luxury goods should be focused on any market that satisfies this description – including those that arise following the conclusion of the Commission's work – regardless of whether those markets sell goods that would typically be considered "luxuries." The proposed regulatory model for combatting money laundering in this sector, set out later in this chapter, is intended to apply to all such markets and, in my view, will be most effective if implemented in a way that permits it to do so.

Using Proceeds of Crime to Purchase Luxury Goods for Use and Enjoyment

The second, broader form of money laundering connected to the luxury goods sector involves the use of proceeds of crime to purchase luxury goods with the intention of using or enjoying those goods.

11 Ibid, paras 2, 35, 57, 60.

12 Ibid, paras 2, 57, 60; Appendix D, *Art Trade Guidelines,* p 103; Appendix F, *Art Industry and Undermining Sanctions,* p 121.

13 Ibid, paras 35, 37–38, 49.

Witnesses during the Commission's hearings referred to the affinity of criminals for high-value, luxury goods.[14] Simon Lord, one of the world's leading experts on money laundering, described how the purchase of luxury goods by those who commit crimes may not be attempts to launder money, but rather the ultimate purpose motivating their criminal endeavours:

> People like to buy luxury goods, and one of the things that you tend to find with criminals is that they go for things like expensive cars. They go for … expensive watches and things like that. And there's always an argument as to the extent to which the purchase of an expensive item is a method of laundering funds or whether it's just a way of realizing your ill-gotten gains … [T]he whole purpose of committing most types of crime is the acquisition of a large amount of money … [W]henever I talk about money laundering, I say that actually all crimes, a million crimes, are actually money laundering, but just with a predicate offence bolted on that generates the money that you're going to launder. And so … in a lot of cases, if you want to buy a flash car or you want to buy a decent watch, it is simply the way you enjoy your ill-gotten gains. But the other side of that is … that you're essentially getting into a type or form of trade-based money laundering.[15]

Similar observations were made by Dr. German in the "luxury vehicles" section of *Dirty Money 2*, where he suggested that criminality motivated by a desire to live a luxurious lifestyle may be particularly prevalent in this province:

> Gangsters in B.C. have often been associated, for good reason, with living a fast life of upscale restaurants, designer clothes, expensive jewellery, and luxury cars, funded and fuelled by drug trafficking and other crimes. Through their ostentatious lifestyle, they seek to portray power and wealth. One expert on gangs internationally wrote, "In none of the places that I visited did I see the same level of wealth on display by gang members that I have observed in B.C."
>
> British Columbia gangs are unlike territorial street gangs in other cities in the world that are a product of economic necessity or oppression; rather, they are motivated by the "ability to make quick money and enjoy a lifestyle of hedonism and decadence," and their girlfriends have "a desire to live in the upper echelon of society – fast cars, fast drugs and fast parties."[16]

I am not in a position to assess whether those engaged in a life of crime do indeed have a greater fondness for luxury goods than law-abiding people, or whether crime in British Columbia is disproportionately motivated by a desire for conspicuous consumption. I do accept, however, that the purchase of luxury goods with the proceeds

14 Evidence of S. Lord, Transcript, May 29, 2020, p 21; Evidence of S. Schneider, Transcript, May 26, 2020, pp 10–11.

15 Transcript, May 29, 2020, p 21.

16 Exhibit 833, *Dirty Money 2*, p 181.

of crime is likely often motivated simply by a desire to own and use those goods and not always part of a premeditated money laundering scheme.

The likelihood that criminals may use the proceeds of crime to purchase luxury goods for the same reason that anyone else might purchase an expensive car, piece of jewellery, or painting does not, in my view, exclude these purchases from being categorized as money laundering – nor does it in any way diminish the need to eliminate this kind of activity. The ultimate goal of money laundering is to convert the proceeds of crime into a form that can be used in the legitimate economy. If illicit funds can be used to purchase luxury goods directly – without distinct, intervening steps to make the funds appear legitimate – the goal of laundering has been accomplished, just as it would if those funds had been routed through a series of offshore bank accounts and numbered companies in secrecy jurisdictions. That this type of complex laundering process was not required before the funds could be spent only simplifies the criminal operation and lowers its costs of business. Further, that a luxury good was not acquired for the *purpose* of laundering money does not mean that it will not ultimately be used to launder money. A vehicle purchased for personal use with the proceeds of crime will, in most instances, eventually be sold. When it is, the value derived from the sale will appear legitimate in the same way that it would if the vehicle was purchased with the intent of laundering the illicit funds originally used to purchase it. In my view, as there is ultimately no difference in outcome, the purchase of luxury goods for personal use with illicit funds should be viewed as no less concerning than their purchase for the purpose of laundering.

Vancouver Model

The third way in which luxury goods can be used to launder money is through the "Vancouver model." This model, discussed in more detail in Chapter 2, involves the lending of cash or other instruments of illicit origin to individuals not directly involved in the criminal activity that generated those proceeds, with the expectation that the loan will be repaid in another form and/or location. The borrower may or may not have knowledge of the illicit source of the funds.

The evidence before me does not definitively prove that there is widespread systematic use of the Vancouver model of money laundering through luxury goods in the same way as in casinos. However, there is a sufficient basis to be concerned about criminal proceeds being loaned to fund the purchase of luxury goods in this province. As I discuss in Chapter 13, it is clear that, due in part to barriers to the removal of money from China, patrons of BC casinos gambled substantial amounts of illicit funds acquired as part of the Vancouver model. It seems obvious that the barriers these individuals faced in obtaining legitimate funds with which to gamble would have also impacted their ability to obtain legitimate funds to finance other aspects of their lives. In this context, it seems highly likely that some of these patrons – if in need of funds with which to purchase a vehicle, jewellery, artwork, electronics, or any number of

other luxury goods – would have resorted to the same source of illicit cash that they used to gamble.

As such, it is clear, in my view, that the risks of money laundering in the luxury goods sector include a high risk of money laundering through the Vancouver model. In my view, using proceeds of crime in this way can certainly be considered money laundering and should be cause for concern – just as it is cause for concern when those who engage in illicit activity themselves purchase goods with illicit funds (as discussed above).

Use of Proceeds of Crime by Criminals and the Vancouver Model Beyond Luxury Goods Markets

I pause here to note that there is no credible basis to believe that the use of proceeds of crime by criminals themselves or by third parties is limited to luxury goods markets or, in the case of the Vancouver model, the gaming sector. On the contrary, it would seem that these typologies can appear in virtually any aspect of the economy, including (as noted above) payment for services. Absent measures that would prevent the use of proceeds of crime in certain sectors, it seems entirely likely that an individual with access to criminal proceeds – whether through the Vancouver model or their own criminal activity – would use those proceeds to fund any and all aspects of their lives. While the use of illicit funds to gamble or purchase luxury vehicles may lead to more compelling headlines, it is just as likely that these funds are also used for more mundane purposes, such as groceries, entertainment, and payment for services. However, despite the capacity of criminal proceeds to be spent on virtually anything, I remain of the view that there is good reason to focus efforts to detect and combat money laundering in the "luxury goods" sector, with reference to the four characteristics I have identified above – high value, capacity to retain value, transferability, and portability.

While the risk of money laundering through the Vancouver model and the direct use of proceeds of crime by criminals are not restricted to the luxury goods (or gaming) sectors, I believe that their use in the luxury goods sector is worthy of particular attention for two reasons. First, these typologies are likely to be much more detectable in this sector than in other parts of the economy. Second, the use of proceeds of crime to purchase luxury goods is more likely to have a greater impact on society than is their use in other types of transactions.

The use of proceeds of crime in the form of cash to purchase luxury goods is likely to be more detectable than in other transactions because of the high value of luxury goods. The use of illicit cash to make small purchases such as groceries, restaurant meals, or movie tickets is unlikely to stand out from similar transactions made using legitimate funds because the value of those purchases is such that it would not be at all unusual for any member of the public to use cash. This is not the case where the item purchased is a luxury car, yacht, work of fine art, or piece of jewellery costing tens or even hundreds of thousands of dollars. As such, the relevance of these

typologies to the luxury goods sector – and the reason, in part, for their inclusion in this chapter – is not the exclusivity of their use in this sector, but rather the opportunity for detection. Accordingly, the model for addressing money laundering in this sector that is developed later in this chapter is designed to address all three forms of money laundering outlined above – the purchase of luxury goods with the intention of laundering money, by criminals themselves to purchase items they desire, or by others through the Vancouver model.

The second reason why the use of proceeds of crime to purchase luxury goods is deserving of particular attention is the elevated impact this activity may have on society because of its potential to motivate criminal activity and to distort local economies. The profit motivation that drives revenue-generating criminal activity is dependent on the ability of those engaged in those crimes to spend their ill-gotten gains. As discussed previously in this Report, the purpose of any money laundering endeavour is to ensure that the proceeds of crime can be spent. While in an ideal world it would not be possible to spend illicit funds at all, it seems obvious that some types of spending will provide a stronger incentive for criminal activity than others and that profit-driven crime would be much less attractive in this province if those who make money through crime were limited to using that money to purchase the necessities of life rather than the luxury vehicles, expensive jewellery, and super-yachts often associated with a stereotypical criminal lifestyle.

In addition, limiting the spending of illicit funds to the purchase of the same kind of day-to-day necessities that all law-abiding British Columbians purchase – if this were possible – would be less likely to distort local economies. In his evidence, journalist Oliver Bullough described how the unfettered use of the proceeds of crime and corruption to purchase luxury goods can distort the mix of businesses and "hollow out" a local economy:

> [I]t inflates asset prices enormously – I mean house prices enormously – and it skews the economy towards particular sectors … the luxury watch sector, the sports car sector … the high-end boutique sector … the kind of things that are purchased by oligarchs and the relatives of oligarchs, but not by the rest of us … [I]t skews the economy towards what Ajay Kapur called plutonomy rather than the kind of things that the rest of us buy.[17]

In my view, because of the greater likelihood that proceeds of crime in the form of cash will stand out when used to purchase luxury goods and the potential that these transactions hold to motivate criminal activity and impact local economies, it is important that efforts to combat money laundering in luxury goods markets include a focus on preventing the use of illicit funds to purchase luxury goods, even where those purchases are for the purpose of consumption and not part of a deliberate money laundering scheme.

17 Evidence of O. Bullough, Transcript, June 2, 2020, p 57.

Money Laundering Risk in Luxury Goods Markets Realized

The evidence before me establishes that the risk of money laundering in luxury goods markets described above is not merely a hypothetical concern. To the contrary, the evidence indicates that this risk has been realized and that substantial amounts of proceeds of crime and corruption have been laundered through luxury goods markets in jurisdictions around the world, including in Canada. While I am unable to determine precisely how much money is being laundered through luxury goods markets in British Columbia specifically, the record before me offers strong indications that this form of money laundering is present in this province.

Money Laundering Through Luxury Goods Globally

Money laundering through luxury goods markets is clearly a source of concern to those working to combat money laundering internationally. This issue has been addressed in reports prepared by organizations including Transparency International,[18] the Financial Action Task Force,[19] Europol,[20] the Basel Institute on Governance,[21] the United Kingdom's National Crime Agency,[22] and the United States Senate Permanent Subcommittee on Investigations.[23] Money laundering in this sector globally has also been addressed in academic commentary[24] and was referred to by a number of international experts who gave evidence during the Commission's hearings.[25]

Much of this evidence included references to concrete examples of money laundering through luxury goods markets. These examples offer valuable insight into how money laundering through luxury goods markets actually occurs and demonstrate that it is much more than a theoretical risk. A sampling of these examples from various sources is set out below.

Europol's 2015 report *Why Is Cash Still King?* offered the following example of a money laundering scheme uncovered in France involving the purchase, transportation, and sale of gold:

18 Exhibit 774, Appendix A, TI *Tainted Treasures 2017*, online: https://images.transparencycdn.org/images/2014_PolicyBrief4_RegulatingLuxuryInvestments_EN.pdf.

19 Exhibit 4, Appendix WW, *FATF Report: Gold*, and Appendix XX, *FATF Report: Diamonds*.

20 Exhibit 64, *Europol Cash Report*, p 13.

21 Exhibit 774, Appendix D, *Art Trade Guidelines*.

22 Exhibit 13, National Crime Agency, *Chinese Underground Banking and "Daigou"* (NAC/NECC v.1.0) (2019).

23 Exhibit 774, Appendix F, *Art Industry and Undermining Sanctions*.

24 F.M. De Sanctis, *Money Laundering Through Art: A Criminal Justice Perspective*, p 56; S. Hufnagel and C. King, "Anti-Money Laundering Regulation and the Art Market," p 4; H. Purkey, "The Art of Money Laundering," p 112.

25 Evidence of R. Wainwright, Transcript, June 15, 2020, pp 24–25; Evidence of O. Bullough, Transcript, June 2, 2020, pp 2–3; Evidence of S. Lord, Transcript, May 29, 2020, pp 20–22; Evidence of G. Hughes, Transcript, May 3, 2021, pp 30, 79; Evidence of S. Cassella, Transcript, May 10, 2021, p 15.

> A recent investigation by French authorities into a drug trafficking network led to several arrests relating to the laundering of the group's profits. Money from the sale of cannabis was collected in France and its laundering was orchestrated through the movement of cash from Paris to Belgium, where it was used to buy gold. Thereafter, couriers (often Belgian students) acted as mules, transporting the gold to Dubai. In Dubai the gold was then made into jewellery and sent to India to be sold on the gold market. The profits were finally shared between the [organized crime groups] and money launderers with the assistance of bankers with access to the financial system. A key organiser admitted laundering EUR 36 million since 2010 and sending 200 kg of gold from Belgium to India. The network collected about EUR 170 million per year.[26]

Simon Lord spoke of money laundering schemes involving gold observed in the United Kingdom in strikingly similar terms:

> [O]ne of the things that we have seen is people using ... bullion dealers, paying cash into the accounts of a bullion dealer, the bullion dealer supplying them with fine gold bars, and then people ... moving the gold bars across an international boundary instead of moving cash. Now, the advantage that they had of doing that in the UK up until relatively recently was that gold and precious metals, stones, and things like that didn't count as cash, and so you couldn't seize it in the same way that you could cash. That has actually changed recently. There has been something ... called the "listed asset" provisions which have been introduced into our primary money laundering legislation ... [They] effectively enabl[e] us to seize ... gold, precious metals, items like that, in the same way that we would do in cash. But ... it is something we've seen, and it's a useful method of money laundering, when you're moving gold to ... a gold processing centre or [somewhere], the demand is very high. So, in places like India, for example, and in places like the [United Arab Emirates] ... which processes a lot of gold [and] turns it into jewellery. And India, the price of gold actually tends to go above the gold fix a lot of the time because the demand is so great, they can't get enough gold to meet the demand. So if you're going to move money and you're going to move it to somewhere like India, then doing it through gold is quite an effective way of dealing with it.[27]

A 2013 Financial Action Task Force report identified a money laundering scheme involving the purchase of vehicles in the United States with funds originating in Lebanon, and the export of those vehicles to West Africa:

> An investigation by the Drug Enforcement Administration (DEA) and other federal law enforcement agencies discovered a scheme to launder money

26 Exhibit 64, *Europol Cash Report,* p 37.

27 Transcript, May 29, 2020, p 22.

> through the United States financial system and the United States used car market. As part of the scheme, funds are transferred from Lebanon to the United States in order to purchase used cars, which were are [*sic*] shipped to West Africa and sold for cash. Cash proceeds of these car sales are then transferred, along with the proceeds of narcotics trafficking and other crimes, to Lebanon. The cash is often moved through bulk cash smuggling. In 2012, the US District Court–Southern District of New York (SDNY) issued a civil ML complaint and "in rem" forfeiture action involving a number of Lebanese financial institutions and exchange houses.[28]

Other examples found in these sources describe the identification of luxury goods including luxury cars, fine art, yachts, and jewellery purchased with the proceeds of crime or corruption; the use of various luxury goods to convert, store, transport, and/or transfer value acquired through illicit activity; and efforts to launder luxury goods that are themselves the proceeds of crimes such as theft or smuggling.[29] In my view, this evidence clearly establishes not only that it is possible to launder money through luxury goods markets, but that this type of activity is a reality in jurisdictions across the globe.

Money Laundering Through Luxury Goods in Canada

The evidence before me also establishes that Canada's luxury goods markets are not immune to this form of money laundering.[30] Of the 38 case examples set out in the Financial Action Task Force report referred to above, six were drawn from Canada.[31] The methodology used in compiling the Financial Action Task Force report[32] was clearly not intended to produce a representative sample, and no conclusions should be drawn as to the prevalence of this typology from the apparent disproportionate number of cases in this report emanating from Canada. However, these examples, set out below, clearly demonstrate that luxury goods markets are being used to launder money in Canada:

a. **Case Study #1:** This case involved an organised criminal group that distributed drugs and controlled several low-level (street-level) drug dealers. The higher-placed distributor would distribute drugs to the street-level dealer and receive diamonds, gemstones, and jewellery as payment, as well as cash. Likewise, the street-level drug dealer traded drugs for diamond jewellery and then traded up to the higher placed drug dealer for more drugs and debt payments. The higher placed drug distributor would then sell the diamonds and jewellery at small

28 Exhibit 4, Appendix XX, *FATF Report: Diamonds*, p 125.

29 Exhibit 774, Overview Report: Luxury Goods, p 42; Exhibit 4, Appendix XX, *FATF Report: Diamonds*, pp 86-127; Evidence of S. Lord, Transcript, May 29, 2020, pp 20–22.

30 Evidence of D. LePard, Transcript, April 7, 2021 (Session 1), pp 59–61; Evidence of C. Leuprecht, G. Clement, A. Cockfield, J. Simser, Transcript, April 9, 2021, pp 38–39; Evidence of M. Paddon, Transcript, April 14, 2021 pp 90–95; Evidence of R. Gilchrist, Transcript, June 9, 2020, pp 59–60; Transcript, May 26, 2020, p 17.

31 Exhibit 4, Appendix XX, *FATF Report: Diamonds*, pp 87, 90, 92–93, 99, 123.

32 Exhibit 4, Appendix XX, *FATF Report: Diamonds*, p 84.

incremental amounts (CAD $3,000–$8,000) to the jewellery market (jewellers) and in return would receive payment by way of cheque. The drug distributor also received high-end jewellery (watches) instead of payment for the illicit jewellery.[33]

b. **Case Study #4:** This case involved a drug dealer/producer who sold drugs and traded drugs for collectively over US $1 million in stolen and purchased jewellery. The drug dealer – who had strong industry, commodity, and market knowledge – sold the least valuable (scrap) jewellery as scrap to jewellery stores and bullion dealers. Jewellery that had some aesthetic or residual market value above the component parts was sold as estate jewellery to jewellers. In return, the drug dealer received cash, gold and silver bars, and coins and diamond jewellery. The drug dealer used some of the proceeds of crime from the sale of drugs and sale of jewellery obtained through trade for drugs to purchase specific diamond jewellery and gemstones items (jade) as a mean[s] to store wealth. The drug dealer used appraisals to define the value of jewellery that was stored as wealth and to help negotiate fair prices for the resale of the jewellery to the market.[34]

c. **Case Study #13:** This is a case where fraud was the predicate offence. The criminals had jewellery industry contacts at the wholesale level. To launder the proceeds of crime, they purchased over CAD $1 million worth of diamonds that were then re-sold back to the jewellery market and also to the general public through the Internet. They did not mark up the value of the diamonds for retail purposes; instead, they sold them to retail customers at wholesale prices and therefore moved them quickly. The diamonds were all in a size and quality class that are the most desirable and resulted a quick turnover of the diamonds. The money received from the sale of the diamonds was wired direct to their bank from the various sales locations.[35]

In addition to these examples, evidence from witnesses who testified before me also supports the conclusions that proceeds of crime are being used to purchase luxury goods in Canada and that the markets for these goods are being used to launder money in this country. Garry Clement, an anti–money laundering expert and former RCMP member who was heavily involved in the early days of the RCMP's proceeds of crime section, described the frequency with which proceeds-of-crime investigations undertaken by the units he led involved luxury goods:

> I can tell you in just about every investigation that I was involved in or had my units investigate, we came across all kinds of safety deposit boxes full

33 Exhibit 774, Overview Report: Luxury Goods, para 44.

34 Ibid.

35 Ibid.

> of high-value jewellery, Rolex watches, not so much of interest today, but they were quite popular in the ’80s and ’90s. We all know that paintings from renowned artists are worth [a] tremendous amount of money, but … high-valued goods [haven’t] been something that Canada in the past has looked at, and yet it’s a great investment because we’ve gone into lots of fairly sophisticated criminals and found their house[s] full of art. So it was a great way to launder money and at that time, and still for the most part, a lot of these high-end jewellers have not had to report. So it’s … a vehicle for money laundering very much like the high-end car industry was. And so what we had to look at and we’ve looked at for years is that … anything that can … hide your cash, a vehicle to hide your cash, definitely is used by sophisticated criminals, and I think it’s an area that we are tightening up in some areas in Canada, but it’s an area that we really need to take a serious look at, whether it’s done provincially or otherwise … I started a program in the ’90s out of Ottawa called Merchants Against Money Laundering, and I really believe that all merchants need to get on side here. It’s both a moral and ethical responsibility because we are sadly losing the fight in this arena.[36]

Similarly, Chief Superintendent Robert Gilchrist, director general of Criminal Intelligence Service Canada, gave evidence of an investigation into a casino-focused money laundering scheme resulting in the seizure of property including luxury vehicles presumably believed to have been purchased with the proceeds of crime:

> A recent example of the use of casinos by organized crime is actually an example out of the Province of Ontario. It’s a York Regional Police investigation that has been publicly reported on and therefore I can comment. It’s an investigation into an organized crime group based in Ontario. During that investigation, group members collectively gambled in Ontario casinos and are believed to have laundered over $70 million Canadian inside legal casinos. It’s reported members of their group went to casinos nightly with $30 to 50,000 Canadian funds, lost a fraction of their cash, and allegedly pocketed the rest as legitimate wins. In July of 2018, this investigation resulted in numerous arrests in Canada and Italy, and approximately $35 million in seizures, including homes and luxury vehicles.[37]

While it is not possible based on this evidence to gain a sense of the prevalence of this method of money laundering in Canada generally, it makes clear that the risk of money laundering through luxury goods markets in this country is not simply theoretical. It also demonstrates that, as is the case elsewhere in the world, proceeds of crime are actually being used to purchase luxury goods, including as part of deliberate efforts to launder those illicit funds.

36 Evidence of G. Clement, Transcript, April 9, 2021, pp 38–40.

37 Evidence of R. Gilchrist, Transcript, June 9, 2020, pp 59–60.

Money Laundering Through Luxury Goods in British Columbia

The foregoing examples of money laundering through luxury goods markets in Canada are not identified as occurring within British Columbia specifically. The example drawn from Mr. Gilchrist's evidence occurred in Ontario, while the remainder do not specify the province in which they occurred. While I am unable to determine whether any of these specific incidents occurred in British Columbia, it would be naïve, in my view, to believe that the proceeds of crime were being laundered through luxury goods markets globally and elsewhere in Canada, but not in this province. This is particularly so in light of the near-complete absence of regulatory efforts to deter or prevent this form of money laundering in this province, as I discuss later in this chapter.

While the evidence described above offers, in itself, ample basis to infer that this method of money laundering must also be in practice in this province, evidence before the Commission – including testimony of criminologist Stephen Schneider, Dr. German's second report (*Dirty Money 2*), and evidence of efforts relating to luxury vehicles undertaken as part of Project Athena – provides additional support for this inference.

Dr. Schneider gave evidence before the Commission for three days and produced a report titled *Money Laundering in British Columbia: A Review of the Literature*.[38] As part of this literature review, Dr. Schneider identified both "Motor Vehicles" and "Precious Metals and Gems" as methods of money laundering in the province, offering examples of the use of proceeds of crime to purchase jewellery and motor vehicles, including the following two case studies:

> **Case Study #1:** In August 2018, a multi-agency police task force investigation into gang activity in Greater Vancouver arrested members of the "Kang/Latimer Group," charging 14 people with 92 criminal offences. As part of the bust, police seized 93 firearms, an improvised explosive device, 59 prohibited devices, 9.5 kilograms of fentanyl, almost 40 kilograms of other illicit drugs, $833,000 in cash, $800,000 in jewellery, and $350,000 in collector cars, all of which became the subject of civil forfeiture proceedings. The next week, the Delta Police Department announced additional drug trafficking and weapons charges against seven men linked to the Red Scorpion gang. Among the assets seized as proceeds of crime from Latimer were $82,000 in cash and four luxury vehicles.[39]
>
> **Case Study #2:** In November 2014, the B.C. Civil Forfeiture Office successfully pursued a civil claim to force the forfeiture of more than CAD $200,000 worth of jewellery from an individual who was, at the time, a member of the Renegades MC, a Hell's Angels affiliate in Prince George. The individual was found guilty in May 2014 of weapons offences, although the Civil Forfeiture Office alleged that he and his girlfriend derived

38 Exhibit 6, Stephen Schneider, *Money Laundering in British Columbia: A Review of the Literature* (May 11, 2020).

39 Ibid, p 76.

> their income from drug trafficking. Among the items (and their worth) ordered to be forfeited by the courts were a man's yellow 10-karat gold diamond pendant (CAD $42,610.40), a man's Breitling watch ($37,916.00), a man's 12-karat yellow gold chain ($30,284.80), a man's 14-karat white gold diamond ring ($26,073.60), a man's 18-karat white gold diamond ring ($22,797.60), a yellow and white gold diamond cross pendant ($15,444.80), a man's 12-karat yellow gold diamond ring ($12,331.20), a man's yellow gold demon garnet ring ($3,472.00), and a yellow gold chain ($3,225.60). The girlfriend allegedly stored some of the jewelry in a safety deposit box to prevent its seizure by the RCMP.[40]

Dirty Money 2 provides further support for the contention that money laundering through the luxury goods market is actually occurring in British Columbia. Focusing specifically on luxury vehicles, Dr. German identified significant cause for concern regarding possible money laundering in the motor vehicle market, setting out information obtained from motor vehicle dealers about suspicious transactions and activity suggestive of money laundering.[41] Dr. German[42] and Doug LePard, who worked with Dr. German on his second report, gave evidence as to the efforts undertaken with respect to the motor vehicle industry in preparation of the report. Mr. LePard, a policing and criminal justice consultant and former deputy chief with the Vancouver Police Department, explained the process by which they examined this industry and the ease with which he was able to identify activity he believed to be connected to money laundering:

> I did a lot of reading to orient myself to what the situation was and looked at investigations into money laundering in other jurisdictions that had been occurring through vehicles. There was really a wealth of information about that. I applied my police experience too in terms of, well, how does a criminal with no legal source of income buy an expensive car? Well, they are going to need to buy it with cash because they're not going to be getting bank loans and that sort of thing.
>
> So again, to put it in a nutshell, I approached it from a number of different angles. And one of those was to cold call dealerships – sometimes with information that I had received confidentially, either through tips that we received when we were working on the project or through police officers who were expert at these kinds of investigations – about where I might want to look and found it wasn't hard at all to find that there was money laundering going on through luxury cars in a number of different ways, either directly purchasing very expensive cars with the proceeds of crime to engaging in various scams to legitimize proceeds of crime.[43]

40 Ibid, pp 99–100.

41 Exhibit 833, *Dirty Money 2*, pp 184–89.

42 Evidence of P. German, Transcript, April 12, 2021, pp 67–70.

43 Transcript, April 7, 2021 (Session 1), pp 60–61.

Similarly, Melanie Paddon, a retired RCMP sergeant with 27 years of experience investigating the proceeds of crime, gave evidence regarding the efforts undertaken with respect to luxury vehicles, undertaken as part of Project Athena (described in detail in Chapter 39).[44] Sergeant Paddon described her own efforts to examine the practices of motor vehicle dealers in British Columbia, identifying a number of indicators of possible money laundering activity observed at motor vehicle dealerships in this province.[45] Given her experience and qualifications, Sergeant Paddon's evidence offers some further support for the conclusion that money laundering through luxury goods markets is a reality in British Columbia.

It is therefore clear, in my view, that money laundering is occurring in British Columbia's luxury goods markets. There is no credible basis to believe that this province would be immune to this phenomenon, observed in multiple international jurisdictions and in Canada generally. The work of Dr. German and Dr. Schneider, as well as the efforts of Sergeant Paddon as part of Project Athena, are sufficient to put to rest any lingering doubts that British Columbia may be an outlier in this regard and satisfies me not only that the province faces a significant risk of money laundering through luxury goods markets, but that activity of this sort is actually occurring.

Organization and Regulation of Luxury Goods Markets

The significant risk of money laundering in the luxury goods sector – and the inescapable conclusion that this risk has been realized – call for a forceful regulatory response to mitigate risk and eliminate this activity through the prevention and detection of money laundering in this sector. Unfortunately, no such response has materialized to date, and to whatever extent the proceeds of crime are being laundered in luxury goods markets in British Columbia, they are being laundered largely without interference. In fact, efforts to combat money laundering in the luxury goods sector in this province are so anemic that they inhibited the Commission's efforts to examine money laundering in the sector simply because, in many markets, there are no records, no information about suspicious activity is gathered, and there is no one with relevant responsibilities to speak to.

This absence of anti–money laundering regulation is one of three features of the luxury goods sector that exacerbate the inherent money laundering risk associated with these types of goods, discussed above. The other two features – the diversity of the sector and diffusion of the markets that comprise the sector – are contextual features that add to the money laundering risk in luxury goods markets. In what follows, I discuss these two features and their impact on the risk associated with the sector, before addressing the absence of regulation in greater depth.

44 Transcript, April 14, 2021, pp 90–95; Exhibit 842, Luxury Vehicle Sub Group (undated).

45 Transcript, April 14, 2021, pp 91–95; Exhibit 842, Luxury Vehicle Sub Group (undated).

The Nature of British Columbia's Luxury Goods Sector: Diversity and Diffusion

In order to understand the money laundering challenge facing British Columbia's luxury goods sector, it is necessary to appreciate the significance of the two features of the sector identified above: diversity and diffusion. These features add to the risk of money laundering in the sector, while also complicating efforts to regulate it.

The sector is **diverse** in the sense that it is comprised of a broad range of different markets, selling products ranging from motor vehicles to jewellery to electronics. Even as the risk of money laundering faced by these markets is shared, they are, in other ways, distinct, each with their own unique cultures, traditions, and practices. While, in my view, it is useful to view these markets as one sector for anti–money laundering purposes, this does not change the fact that it is a sector comprised of a loose collection of very different markets that may have little in common beyond the elevated value of the goods that they sell and the nature of the money laundering risk that they face.

The diversity of the sector exacerbates money laundering risk and complicates anti–money laundering efforts. In particular, it creates a complex tapestry of distinct markets, the idiosyncrasies of which can be exploited by those intent on laundering money. Meanwhile, efforts to regulate these markets in a coordinated way are forced to grapple with how each operates and consider how to distinguish the normal functioning of unique markets from genuinely suspicious activity. For example, the tradition of confidentiality and discretion in the market for fine art[46] creates money laundering risk, but also a possible legitimate explanation for an interest in maintaining a level of secrecy over transactions that would be difficult to justify in other markets. Effective anti–money laundering regulation of this sector in a unified way requires an in-depth knowledge of how each of these markets functions sufficient to distinguish normal behaviour consistent with the cultures and traditions of each from genuinely suspicious activity.

Money laundering risk and the complexity of regulation is also elevated by the **diffusion** of the luxury goods sector. The sector is diffuse in the sense that the markets that comprise the sector typically consist of a large number of separate, often small, retailers. For example, by the end of 2021, there were 1,535 separate licensed motor vehicle dealers in British Columbia,[47] while in 2018 a representative of the Canadian Jewellers Association estimated in testimony before the House of Commons Standing Committee on Finance that there were approximately 5,000 jewellers in Canada.[48] Add to these all of the art dealers and galleries, yacht brokers, electronics retailers, and other businesses dealing in luxury goods in British Columbia and it is clear that the number of

46 Exhibit 774, Overview Report: Luxury Goods, paras 2, 57, 60; Appendix D, *Art Trade Guidelines*, pp 103, 121.

47 Vehicle Sales Authority of British Columbia, *Annual Report 2020/2021*, p 7, online: https://www.mvsabc.com/about-the-vsa/corporate-documents/annual-report-2020-2021.pdf.

48 Exhibit 776, Affidavit No. 1 of Beatrice Sturtevant, March 22, 2021 [Sturtevant #1], p 23.

distinct businesses operating in this sector creates an industry very different in character from, for example, the gaming industry, which is overseen by a single Crown corporation.

The diffusion of the sector presents a money laundering challenge and complicates regulation by creating a vast number of distinct locations at which money laundering could occur. Whereas the gaming industry offers a limited number of casinos – all under the control of single Crown corporation – that can be targeted for money laundering, the luxury goods sector presents a virtually limitless number of distinct businesses, any one of which could be used to launder money. The challenge this presents for regulation is obvious. Given the realities of finite time and resources, the task of maintaining effective oversight over activities within one such market is daunting. When multiplied by the number of distinct markets that comprise the sector, the challenge only grows.

The Absence of Anti–Money Laundering Regulation in the Luxury Goods Sector

While the foregoing features of the luxury goods sector offer insight into why it may be difficult to address the risk of money laundering in this sector in British Columbia, they offer no excuse for the near-complete absence of any efforts to combat or even detect the use of illicit funds in this area of the province's economy. In most instances, the absence of anti–money laundering regulation is likely a function of the absence of any kind of significant regulatory regime. Most luxury goods markets – for example, art dealers and galleries, jewellers, yacht brokers, and luxury clothing and apparel retailers – are largely unregulated industries, save for the reporting and other obligations of jewellers under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, SC 2000, c 17 (*PCMLTFA*) and routine obligations for requirements such as business licenses.[49]

However, even heavily regulated markets in this sector – particularly the motor vehicle industry – suffer from a dearth of anti–money laundering regulation. The sale of motor vehicles in British Columbia is governed by the *Motor Dealer Act*, RSBC 1996, c 316, and the regulations to that Act.[50] The Act and regulations set out a comprehensive scheme for regulating motor vehicle dealerships and salespeople, which is administered in part by the Vehicle Sales Authority of British Columbia.[51] Among the regulatory requirements set out in the Act are requirements that motor vehicle dealers be registered with the authority[52] and that motor vehicle salespersons be licensed by it.[53] The Act provides for a complaints process[54] and authorizes the

49 Exhibit 774, Overview Report: Luxury Goods.

50 Ibid, para 7.

51 Ibid, para 7.

52 Ibid, para 10.

53 Ibid, paras 12–14.

54 Ibid, paras 18–26.

authority to take various investigative steps and impose disciplinary measures in response to complaints.[55] The authority also has the power to refuse, cancel, or suspend a registration and to refuse, revoke, or suspend a license if the registration or license is not in the public interest.[56]

Despite these stringent regulatory requirements, motor vehicle dealers are not subject to any anti–money laundering requirements: neither the Act nor the mandate of the Vehicle Sales Authority extends to money laundering, and motor vehicle dealers are not subject to the *PCMLTFA*.[57] The primary function of the Vehicle Sales Authority is consumer protection.[58] Accordingly, while it has the power to conduct inspections and compel dealers to produce information, it cannot do so for the purpose of identifying indicators of money laundering.[59] Further, although the authority can produce rules and regulations binding motor vehicle dealers and salespeople, it has no such rules or regulations requiring basic anti–money laundering practices such as customer due diligence requirements or regulations governing cash payments.[60]

Impact of Diversity, Diffusion, and Absence of Regulation on Perceptions of Money Laundering in the Luxury Goods Sector

In addition to the above challenges, the absence of centralization and regulation in luxury goods industries may contribute to an underestimation of the severity of money laundering activity in this sector. Because no one is responsible for monitoring possible money laundering activity in these markets, and because no one is collecting the information necessary to do so, it may appear as though there is no money laundering concern in these markets simply because signs of such activity go unnoticed. As such, it may be that the greater public concern about money laundering in the gaming industry (a centralized, regulated sector), compared to the luxury goods sector, is *not* a reflection of limited money laundering activity in luxury goods markets, but rather the result of greater scrutiny of the gaming industry, which brings those issues that do exist to light. In other words, it may be that the reason the public has not been alarmed by surveillance footage of bags of cash accepted at car dealerships, jewellers, art dealers, and yacht brokerages is not because there are no bags of cash, but because there is no surveillance footage. This possibility underscores the need for further efforts to examine money laundering in this sector as well as the need to structure the sector to ensure that effective anti–money laundering scrutiny is possible.

55 Ibid, paras 18–26.

56 Ibid, paras 11–16.

57 Exhibit 775, Overview Report: Motor Vehicle Sales Authority of British Columbia, para 6.

58 Exhibit 774, Overview Report: Luxury Goods, para 31.

59 Exhibit 775, Overview Report: Motor Vehicle Sales Authority of British Columbia, para 7.

60 Ibid, para 10.

Industry-Driven Anti–Money Laundering Efforts

The near-complete absence of any kind of meaningful anti–money laundering regulation in British Columbia's luxury goods sector does not mean that there is no cause for optimism that steps are being taken to address the elevated risk faced by this sector. While regulators and other public authorities are, for the most part, not taking meaningful action, there are examples of industry itself working to mitigate the risks of money laundering in luxury goods markets. In particular, the jewellery and precious metals and stones industry, as well as the yacht brokerage industry, have taken action to prevent money laundering within their markets. As I discuss below, however, there are inherent limitations on the impact of this kind of voluntary, industry-led action, and it cannot be relied upon as a complete solution to this problem.

Jewellery and Precious Metals and Stones

In contrast to the motor vehicle sales industry, where heavy regulation has not resulted in meaningful anti–money laundering action, the market for jewellery and precious metals and stones offers an example of how limited regulation can spur an industry to take additional action on its own initiative where that industry is well-organized and where that regulation is focused on the risk of money laundering.

The jewellery and precious metals and stones industry is largely unregulated. While the industry is the subject of some federal legislation such as the *Export and Import of Rough Diamonds Act*, SC 2002, c 25, and the *Precious Metals Marking Act*, RSC 1985, c P-19, there is no legislation at the federal or provincial level establishing a comprehensive regulatory regime for the industry. Accordingly, in contrast to the motor vehicle sales industry, there is no requirement that jewellery and precious metals and stones retailers register with a regulator, or that salespeople working in the industry be licensed. Nor is there a regulator equivalent to the Vehicle Sales Authority, which is empowered to receive complaints, conduct inspections, impose discipline, or exclude bad actors from the industry.[61]

Where the regulation of this industry exceeds that of the motor vehicle sales industry, however, is with respect to regulations specifically targeted at money laundering. Unlike motor vehicle dealers (and most luxury goods retailers), dealers in precious metals and stones are subject to the *PCMLTFA* and have been since 2008.[62] Accordingly, dealers in precious metals and stones are required to comply with the obligations of that regime, including reporting suspicious and other transactions to the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) and implementing a compliance program.[63]

While the requirements of the *PCMLTFA* may well assist in the identification and prevention of money laundering in the industry, perhaps of greater interest in understanding the impact of regulation is the response of the industry itself to this regulation, organized by the Canadian Jewellers Association.

61 Exhibit 774, Overview Report: Luxury Goods, paras 39–40.

62 Ibid, para 39; Exhibit 776, Sturtevant #1, pp 32, 67.

63 Exhibit 776, Sturtevant #1, para 25. See Chapter 7 for a more detailed explanation of the *PCMLTFA* regime.

The Canadian Jewellers Association is a national trade association for the Canadian jewellery industry,[64] founded in 1918[65] and comprises retailers, suppliers, appraisers, designers, and providers of goods and services.[66] Membership in the Canadian Jewellers Association is voluntary.[67] In 2020, the association had 444 members across Canada, including 57 in British Columbia.[68] I note that this membership seems to be a small proportion of the total number of jewellers operating in Canada, given the association's 2018 estimate that there were 5,000 jewellers operating in Canada.[69]

Since the incorporation of dealers in precious metals and stones into the *PCMLTFA*, the Canadian Jewellers Association has taken a number of actions to assist its members and the industry more broadly to comply with their obligations under the regime and to reduce the risk of money laundering in the market for jewellery, precious metals and stones. These actions include:

- producing training and professional development materials for the association's members, available in person and online;[70]
- publishing anti–money laundering articles and resources, including in the association's monthly newsletter and in trade publications;[71] and
- developing resources in conjunction with a consulting firm to assist in implementation of compliance programs, including the creation of an online tool to assist in risk assessment and identification of necessary components of a compliance program.[72]

It does not appear that any data have been collected that would allow the Commission to draw any conclusions as to the impact these measures have had on the prevalence of money laundering in the jewellery and precious metals and stones industry. However, experience in other sectors has taught us that anti–money laundering education and resources can go some way toward addressing risk. These efforts on the part of the industry were clearly prompted by the increased regulation introduced when the *PCMLTFA* was extended to dealers in precious metals and stones. Yet, there was no obligation for the Canadian Jewellers Association to take the action that it took, and I applaud the association and, by extension, the industry, for the steps it has taken.

The activity by the Canadian Jewellers Association demonstrates not only that enhanced regulation can have positive ancillary effects that go beyond basic legal

64 Exhibit 774, Overview Report: Luxury Goods, para 51.
65 Exhibit 776, Sturtevant #1, para 6.
66 Ibid, para 2, 5.
67 Exhibit 774, Overview Report: Luxury Goods, para 51.
68 Exhibit 776, Sturtevant #1, para 8.
69 Ibid, exhibit A, p 23.
70 Ibid, paras 17–21 and exhibit C.
71 Ibid, paras 21–24 and exhibits D, E, F.
72 Ibid, paras 25–29 and exhibits G, H.

requirements, but also that voluntary industry action may be a viable means of enhancing the province's response to money laundering. It also shows that there may be value in government working with industry groups such as the Canadian Jewellers Association in the hope of inspiring such action.

Yacht Brokerages

The example of the yacht brokerage industry in British Columbia suggests that it may be possible to prompt this kind of voluntary action by industry even in the absence of binding regulations. Like many luxury goods retailers, yacht brokers are not subject to the *PCMLTFA*.[73] The industry is also largely unregulated, with no licensing or registration requirements in the same way as the motor vehicle sales industry.

While largely unregulated, the industry in this province is organized through the British Columbia Yacht Brokers Association. The association is a society incorporated under the *Societies Act*, SBC 2015, c 18,[74] and has the following purposes:

a. To unite those engaged in the yacht brokerage business for the purpose of promoting cooperation and professionalism through its members.

b. To promote and maintain a high standard of conduct in the transacting of the yacht brokerage business.

c. To instill in the boating public a greater confidence in yacht brokers.

d. To encourage a greater interest in the welfare and safety of the boating public.[75]

In June 2020, the BC Yacht Brokers Association introduced its "Anti–Money Laundering Practice Policy"[76] and amended its Code of Ethics to require compliance with the policy.[77] The policy requires members to implement certain anti–money laundering practices, including those related to client identification, ascertaining beneficial ownership, and handling cash transactions.[78] It also assigns brokers responsibility for establishing a "comprehensive and effective program" for complying with the policy and provides tips for identifying possible money laundering activity.[79]

As with the actions taken by the Canadian Jewellers Association, I am unable to evaluate the precise impact the actions taken by the BC Yacht Brokers Association have had on money laundering in the industry. However, this is clearly a positive development from

73 Exhibit 774, Overview Report: Luxury Goods, para 72(i).

74 Exhibit 774, Overview Report: Luxury Goods, para 73.

75 Exhibit 774, Overview Report: Luxury Goods, para 73.

76 Exhibit 774, Overview Report: Luxury Goods, para 74, Appendix I, British Columbia Yacht Brokers Association, "Anti–Money Laundering Practice Policy" [Yacht Brokers AML Policies].

77 Exhibit 774, Overview Report: Luxury Goods, para 74; see also Appendix J, British Columbia Yacht Brokers Association, Code of Ethics, para 14.

78 Exhibit 774, Appendix I, Yacht Brokers AML Policies.

79 Ibid.

an anti–money laundering perspective and further demonstrates that voluntary action on the part of industry may realistically contribute to the province's anti–money laundering efforts. Moreover, the actions of the BC Yacht Brokers Association indicate that this kind of industry-led action may be possible even without binding regulation like that applicable to dealers of precious metals and stones. Based on documents produced by the BC Yacht Brokers Association, I understand that it was contact from the Commission itself that may have spurred the development of this practice policy. This suggests that it may be possible for authorities to inspire meaningful action to address money laundering in luxury goods markets simply by reaching out to industry and raising awareness of the risk of illicit activity.

The Limits of Industry-Driven Action

The examples of voluntary industry action noted above are encouraging. I commend the Canadian Jewellers Association and the BC Yacht Brokers Association for their efforts to protect their own industries from criminal activity, and I encourage other industries to take similar action. In my view, however, while industry-led action may be part of the solution to the elevated money laundering risk faced by the luxury goods sector, it cannot be relied upon to resolve the problem in the absence of meaningful action from government.

This is so in part because both of these examples involve voluntary industry action *prompted by action on the part of government or public authorities.* The efforts of the Canadian Jewellers Association are clearly a response to the inclusion of dealers in precious metals and stones in the *PCMLTFA*, while I understand the actions of the BC Yacht Brokers Association to have been a response to contact by the Commission. It is possible that these industries may have eventually taken action on their own initiative, but it seems likely that in both cases the "nudge" provided by a public authority was a necessary precondition to the voluntary action. This illustrates the importance of government engaging at least to the point of encouraging voluntary action by industry. Further, as I noted above, the Canadian Jewellers Association represents approximately 10 percent of the total number of jewellers in Canada; while I understand that their anti–money laundering activities are not strictly limited to their own membership, they likely leave unaddressed a large proportion of the industry.

More fundamentally, voluntary industry action cannot be relied on as a complete solution to the risk of money laundering precisely *because* it is voluntary. There will inevitably be businesses within luxury goods markets that choose not to adopt these voluntary measures, and even entire industries that will decline to do so. As an example, the Commission engaged with the Art Dealers Association of Canada in a manner similar to its communications with the BC Yacht Brokers Association. Whereas the BC Yacht Brokers Association responded by taking meaningful action to reduce the risk of money laundering in their industry, the Art Dealers Association of Canada responded with skepticism that their industry could be affected by money

laundering and by cautioning that "over-legislation" could harm the industry.[80] To be clear, the Commission did not ask the Art Dealers Association of Canada to take action to respond to the risk of money laundering in its industry, and I have no evidence supporting a conclusion that its members are anything but ethical, law-abiding business owners. That said, this response does underscore the limits of voluntary action and the need for active engagement by government to effectively address money laundering in the luxury goods sector.

Lessons from the Organization and Regulation of Luxury Goods Markets

The following section sets out a model for addressing money laundering in the luxury goods sector in British Columbia and describes the role that could be played within that model by a permanent AML Commissioner. Before discussing this model, however, I believe that it is useful to pause and identify three key lessons that can be learned from the discussion above regarding the regulation and organization of luxury goods markets and their implications for the risk and response to money laundering in this sector.

Access to Information

The Commission's own experience illustrates that the first step in addressing the risk of money laundering in this sector of the economy is to make it *possible* to understand what is happening in the markets that comprise the sector. The diffusion of the sector makes the task of collecting information onerous; the absence of regulation means that no one is tasked with attempting to do so (with the exception of FINTRAC in the case of jewellers); and the absence of any record-keeping or reporting requirements in most of the sector mean that useful information may not exist even if it was possible to collect and someone had the mandate to do so. I would add that even though many people have a superficial sense of money laundering, the stereotypical or simplistic view belies the complexity and the reality of money laundering. This is a topic area that is not intuitive, and if anything is often misunderstood or oversimplified. Any effort to combat money laundering in this sector must begin by solving this informational challenge, including statutory barriers that may exist.

The Importance of Focused Regulation

The example of the Vehicle Sales Authority demonstrates that, even where a robust regulatory regime exists within a luxury goods market, regulation must be targeted at preventing money laundering if it is likely to have a meaningful impact. The vehicle sales industry is heavily regulated – including registration and licensing requirements for dealerships and salespeople – yet there is no meaningful, industry-wide effort to prevent money laundering in the industry. If we are to expect a regulator like the

80 Exhibit 774, Overview Report: Luxury Goods, Appendix G, Letter of January 21, 2020, from Hillary E. Robinson, Executive Director, Art Dealers Association of Canada.

Vehicle Sales Authority to take effective action to prevent money laundering in the industry it regulates, it must be given a mandate – as well as the necessary authority and resources – to do so.

The Role of Voluntary Action

The experiences of the Canadian Jewellers Association and the BC Yacht Brokers Association demonstrate that voluntary action by industry is a viable, if limited, means of addressing risk in this sector. With the support and encouragement of government, industry may take on the task of combatting money laundering itself by setting voluntary standards and providing resources to individual retailers that may not have the knowledge or resources to limit their money laundering risk themselves. Voluntary action of this sort has the advantages of being extremely low cost for government and allowing an industry to develop a bespoke approach to combatting money laundering – one tailored to the culture, traditions, and practices of the industry. While the presence and potential of voluntary industry measures does not obviate the need for more direct and coercive action by government, encouragement and support of voluntary action is deserving of investment.

A Model for Addressing Money Laundering in the Luxury Goods Sector

The preceding discussions of the risk of money laundering facing the luxury goods sector and the regulation and organization of luxury goods markets offer valuable insight into the nature of the risk facing this sector of the economy and the very limited measures in place to address it. In what follows, I draw on these insights to develop a model for addressing the risk of money laundering in this sector by identifying six components essential to an effective money laundering response in the luxury goods sector.

The model here is not intended to be a prescriptive one. While it is not devoid of specific recommendations, it does not identify a comprehensive set of specific measures that must be implemented in all luxury goods markets. As discussed above, the luxury goods sector consists of a collection of distinct markets, each with its own unique cultures, practices, and risk factors. Due to the nature of the sector, it is my view that the response to the risk of money laundering in this sector must be flexible and adaptive to ensure that the response can be tailored to the unique circumstances and risk factors of individual markets and evolving activity within those markets. The model proposed below is intended to facilitate this flexible and adaptive response.

As I expand below, the model I am proposing will involve a central authority receiving reports on transactions involving $10,000 or more in cash. The Province is best placed to determine which entity should receive and store these reports (for the

purposes of this discussion, I will refer to this entity as the "central authority"). Indeed, the Province may consider that having the reports go directly to the AML Commissioner is desirable. In any event, it is essential that the AML Commissioner have access to these reports and the ability to communicate with the central authority about the usefulness of such reports and possible changes to the regime.

I add that the reports should ideally go to one central authority, rather than, for example, having reports about vehicles going to the Vehicle Sales Authority and those for other luxury goods elsewhere. The primary reason for this reporting regime is to permit the central authority and the AML Commissioner (who, again, must have access to the reports) to understand activity in the luxury goods sector, which is, at present, something of a black box due to the difficulties I have outlined above. Having the reports go to different entities would make it more difficult for the central authority and the AML Commissioner to assess the luxury goods sector as a whole.

Visibility into Activity Within Luxury Goods Markets

In order to effectively combat money laundering in the luxury goods sector, it is necessary to first understand the nature of the activity occurring within the markets that comprise the sector. As discussed above, among the challenges associated with combatting money laundering in the luxury goods sector are diversity, diffusion, and lack of regulation in the sector. Because of these features, as things presently stand, it is very difficult to gain an understanding of the extent to which money laundering is occurring within the sector and, if it is occurring, how it is being accomplished.

If there is any hope of ensuring that the luxury goods sector in British Columbia is not used to launder illicit funds, this challenge must be overcome by creating visibility into activity occurring within the markets that make up this sector. There are a range of possible measures that may assist in creating this visibility. These include reporting requirements like those applicable to reporting entities under the *PCMLTFA*, or the granting of audit and inspection powers to regulatory or other public authorities. The most appropriate measures will likely vary by market, and it will be necessary to work and consult with industry to identify the most appropriate approach for each market.

As I have discussed, one of the ways criminals launder proceeds through luxury goods is to use illicit cash to purchase the luxury goods, thereby transforming the cash into a less suspicious form that can be transferred or sold to provide a façade of legitimacy. Given the elevated risk associated with certain types of transactions, it is necessary, in my view, to establish a common basic reporting requirement that will ensure a minimum level of visibility into suspicious activity – not only in the luxury goods sector, but across the province's economy.

To this end, I recommend that the Province implement a universal record-keeping and reporting requirement for cash transactions of $10,000 or more for all businesses,

with limited, enumerated exceptions. This recommendation is not intended as a complete solution to the challenge of creating visibility into these markets, but rather as a minimum necessary starting point, onto which further measures will inevitably be added. This recommendation is discussed in detail below, followed by a discussion of the role that could be played by the AML Commissioner in evaluating the need for additional measures.

Recommendation 82: I recommend that the Province implement a universal record-keeping and reporting requirement for cash transactions of $10,000 or more. Every business that accepts $10,000 or more in cash in a single transaction or a series of related transactions should be required to:

- verify a customer's identification and record their name, address, and date of birth;
- inquire into and record the source of funds used to make the purchase;
- determine whether the purchase is being made on behalf of a third party and, if so, inquire into and record the identity of that third party; and
- report the transaction – including the total amount of cash accepted; the item or service purchased; the source of funds reported by the customer; whether the purchase was made on behalf of a third party and, if so, the identity of that third party; and the name, address, and date of birth of the customer – to the Province.

The Province should ensure that the AML Commissioner has access to these reports.

The universal record-keeping and reporting requirement should apply in all circumstances, with some narrow exceptions:

- one-time transactions between private individuals;
- financial institutions and financial services businesses;
- lawyers; and
- other situations where it is determined that the requirement would be unduly onerous, generate reports of little value, or is otherwise inappropriate.

I note that this recommendation is broad enough to encompass cash transactions involving both goods and services, in line with my discussion earlier in this chapter about the money laundering risks associated with services. It is also broad enough to encompass the receipt of cash by builders and building supply companies. As I elaborate in Chapter 17, the Commission conducted a small study into the acceptance

of cash by builders and building supply companies, which showed that five building suppliers took in over a million dollars in large cash transactions ($10,000 or more) between 2015 and 2020.

A Universal $10,000 Cash Record-Keeping and Reporting Requirement

As a general principle, I believe that anti–money laundering measures, including information-gathering mechanisms, should be tailored to the unique circumstances of individual luxury goods markets. There are some types of activity, however, that give rise to sufficient suspicion that they must be subjected to scrutiny regardless of the market in which they occur. The use of very large volumes of cash is one such type of activity.

Given the extent to which Canadian society has moved away from cash in favour of other payment methods, in most circumstances it is difficult to conceive of why a purchaser spending legitimate funds would choose to pay for any high-value good or service using cash. While I do not propose, at this stage, that the Province ban such transactions, I do believe that very large cash transactions pose a significant risk of money laundering and that this risk justifies requiring that additional information be gathered and reported to appropriate authorities. For this reason, I am recommending that any business that accepts $10,000 or more in cash as payment for a good or service in a single transaction or series of related transactions, with identified exceptions, be required to:

- verify and record the identity of the customer making the payment by viewing a piece of government-issued photo identification and recording the customer's name, address, and date of birth;
- inquire into and record the source of the funds used to make the purchase;
- determine whether the purchase is being made on behalf of a third-party, and if so, inquire into and record the identity of that third party; and
- report the transaction – including the total amount of cash accepted; the item or service purchased; the source of funds reported by the customer; whether the purchase was made on behalf of a third party and, if so, the identity of that third party; and the name, address, and date of birth of the customer – to the Province.

One-time transactions between private individuals, such as the private sale of a vehicle by a person not habitually in the business of selling vehicles, should not be captured by this requirement.

While this requirement should be applied to all businesses offering goods or services, I anticipate that there may be certain markets where this requirement is particularly onerous, where the reports generated are of little value, or where there are other reasons why it may be sensible to exempt some types of businesses or sectors of

the economy from this requirement. I am therefore recommending that exemptions be made where appropriate, including, from the outset, the following two exemptions:

1. **Financial institutions and financial services businesses, including credit unions and money services businesses:** By their nature, these businesses routinely handle cash in large volumes and, as such, are likely to generate a very large volume of reports that will be of little value in detecting genuinely suspicious activity.
2. **Lawyers:** As I explain in Chapter 27, I have concluded that the Province should not implement a reporting requirement for lawyers due to the significant constitutional difficulties that would arise in doing so, as well as in recognition of the strong anti–money laundering regulation already undertaken by the Law Society of British Columbia.

I expect that additional exemptions may well be added to this list prior to and following the implementation of this recommendation. The Province may wish to consider, for example, whether requirements to provide proof of the source of cash used in transactions of $10,000 or more are sufficient, such that, if they are continued, further reporting under this regime is unnecessary.

Unlike reporting to FINTRAC, I anticipate that the primary function of the information collected through this requirement will be to guide anti–money laundering policy development. By providing insight into the types of businesses and locations where suspicious transactions are occurring (and likewise where such transactions are *not* occurring), the information will assist the AML Commissioner to identify where suspicious activity is occurring. It will provide valuable insight into the markets and geographic locations that should be targeted with enhanced anti–money laundering measures. For example, if these records indicate a sudden increase in large cash purchases of luxury vehicles in one region of British Columbia, this may indicate the need to gather further information as to the cause of that increase and consider policy responses ranging from an education campaign for motor vehicle dealers in that region up to a permanent, province-wide prohibition on the use of cash to purchase vehicles.

In a similar way to informing policy development, the information will allow the AML Commissioner to have a strong evidence-based understanding of the realities of what is occurring in the luxury goods sector. As I have noted throughout this chapter, such a "real world" understanding is currently lacking, and there is little information (or even avenues to obtain such information) available that can inform the Province's or the new AML Commissioner's work. Further, the information may very well assist with improved regulatory responses. Armed with this new data, the AML Commissioner will be in a much better position to recommend changes in particular sectors in order to respond to particular risks.

Though not the primary purpose of collecting this information, an ancillary effect of a reporting regime would be the preservation of this information and the

potential for law enforcement, using established law enforcement procedures, to access that information in appropriate cases. I do not propose, at this stage, to replicate the FINTRAC model of analysis and proactive disclosure to law enforcement. Instead, the reports should initially be held by the central authority and available to law enforcement through established and familiar legal processes. While the AML Commissioner would review and analyze them for the primary purpose of guiding policy development identified above, I do not propose that the reports also be routinely analyzed for the purpose of identifying whether there is a basis to provide them to law enforcement. The reason for this is that, at this stage, I have little sense as to the volume or nature of the reports that will be made and, as such, I am unable to assess whether the value of these reports to law enforcement justifies the potentially significant effort and expense of analyzing these reports for this purpose. Accordingly, I believe the most sensible approach is to allow the Province (in consultation with the AML Commissioner) to determine whether this expense is justified once it has a clear understanding of the volume and nature of the reports that will be received in response to this requirement. Again, the absence of this analytical capacity does not mean that law enforcement will not have access to these reports, only that the reports will not be proactively analyzed for this purpose. I add that, prior to implementing a process in which the reports could be disclosed to law enforcement, the Province would need to conduct an assessment of the impact of legal or constitutional issues on the manner and feasibility of such proactive disclosure, or whether certain safeguards, such as a standard for disclosure, would have to be included in the system to protect legal and/or constitutional interests.

I also note that the volume of reports and the intensity of the work for the AML Commissioner will be proportional to what is actually occurring in the luxury goods sector. If, for example, few businesses are in fact accepting cash in amounts over $10,000, there will be few reports (and vice versa). It will be important for the AML Commissioner to assess, after a specified period of time, how many reports have been made and any utility gained from them. Further, the AML Commissioner should report to the Legislature on the progress of the regime.

In addition to the value of the reports submitted under this requirement to policy development (and preserved for potential access by law enforcement), I expect that a further ancillary, but significant, benefit of this recommendation will be to deter large cash transactions from occurring at all, especially by those seeking to avoid scrutiny. While I encourage government to streamline the reporting process to the extent possible, it is inevitable that the recommended record-keeping and reporting requirement will pose an administrative burden on businesses required to comply. I expect that this administrative burden will incentivize some businesses to simply refuse transactions of cash over $10,000 altogether, which would reduce the opportunities for those intent on laundering proceeds of crime to spend illicit cash. Similarly, the reporting requirement may also deter customers from using large volumes of cash. The knowledge that a large cash transaction will result in the production of a report

identifying the customer and their personal information (including name, address, and date of birth), the details of the transaction, and their explanation as to the source of the funds will surely make those intent on avoiding scrutiny of those funds think twice before proceeding with any such transactions in British Columbia.

As a final note, I do, as indicated above, recognize that the implementation of this recommendation will impose a new burden on many honest and legitimate businesses throughout the province. Given this impact, I do not make this recommendation lightly. However, I am convinced that it is necessary and, due in part to the evidence before me of similar requirements in other jurisdictions,[81] viable. I also note that the burden is optional, in that each business will have the option of declining cash transactions of this size, completely absolving them of the burden. Still, I encourage the Province to bear in mind the impact on legitimate businesses when implementing this recommendation and to seek to minimize that impact, including through the use of technology to streamline the reporting process.[82] I note as well that this recommendation poses a significant communication challenge for the Province, as virtually every business in British Columbia will require notice of this new requirement. I encourage the Province to take steps to ensure that no business suffers consequences for failing to comply with this requirement if they have not been given fair notice of its existence. Conversely, it will be necessary for the government to determine a suitable compliance regime to encourage observance once businesses have been notified of the requirement.

Role of the AML Commissioner

The potential role that the AML Commissioner may play in ensuring visibility into activity in luxury goods markets is not limited to analysis of reports submitted under the requirement that I have recommended above. As discussed previously, this reporting requirement is intended as a starting point for gathering information about money laundering risk and activity in luxury goods markets, and it must not be treated as a complete solution.

Alongside the analysis of these reports, I envision that the AML Commissioner will be engaged in additional efforts to collect information about luxury goods and other markets on an ongoing basis. These efforts could include consulting with businesses, industry associations, and regulators; studying activity in specific markets or regions; and monitoring international money laundering trends. In order to fulfill this function, the AML Commissioner must have the resources to carry it out. The Province may also wish to consider providing the AML Commissioner with the ability to compel information from private entities for the purpose of studying money laundering risks. This would require careful consideration of the manner in which the compulsion power should be limited.

81 Exhibit 966, Maria Bergstrom, "Report on the European Union Anti–Money Laundering Regulation – Draft," pp 15–16; Evidence of J. Rense, Transcript, May 13, 2021, pp 96–97.

82 For this recommendation to succeed, the Province must offer an easily accessible and intuitive platform where reports can be submitted. In designing this platform, the Province should seek to minimize the potential for human error and different reporting styles; for example, options such as drop-down menus or checkboxes will lead to more consistent data than allowing the user to write in responses.

Vehicle Sales Authority Cash Study

One innovative means of gaining insight into possible money laundering activity in the vehicle sales market that may serve as a model for the AML Commissioner's efforts in this regard was proposed by the Vehicle Sales Authority and the Ministry of Public Safety and Solicitor General in 2019 in response to Dr. German's second report.[83] The proposal would have seen the Vehicle Sales Authority conduct a study in which it would collect information from motor vehicle dealers regarding the use of cash and other anonymous forms of payment in transactions conducted by those dealers.[84] This data would have been collected voluntarily and in a form that would have preserved the anonymity of the dealer providing the information.[85]

In my view, there are clear deficiencies in this proposed study. Collecting information on a strictly voluntary basis would offer those intent on hiding their activities a simple means of doing so and would undermine the reliability of the results by allowing for the under-reporting of higher risk activity.[86] I understand as well that there were some concerns on the part of dealers about the suggestion that the data collected would be anonymous, as the source of some of the data may have been evident from the data itself.[87] It is necessary that these issues be resolved before any such study is undertaken; however, a study aimed at understanding the nature of activity in a particular market does strike me as a sound initial step in the process of creating necessary visibility into luxury goods markets. These types of studies may be an effective means of gathering information that will assist the AML Commissioner in understanding the types of activity prevalent in these markets and identifying the extent of the money laundering risk present, without undue disruption to the businesses involved. Based on the results of such studies, it may be possible to determine whether further, more permanent – and potentially more invasive – measures are required. For example, where the initial study reveals minimal activity of concern, it may be sufficient to plan a future follow-up study to ensure that there are no significant changes from the time of the first one. In contrast, where an initial study reveals significant high-risk activity, it may be necessary to consider enhanced regulation or additional reporting requirements.

Ongoing Assessment of Risk in Luxury Goods Markets

Closely associated with the need to provide visibility into what is taking place in luxury goods markets is the second component of the proposed model for combatting money laundering in this sector: the need for ongoing assessment of risk. Creating visibility into activity within these markets is of value only if the information made available is reviewed and, if necessary, acted upon. Accordingly, it is essential that an appropriate authority be charged with the responsibility for examining this

83 Exhibit 994, Affidavit No. 1 of Tobias Louie, Affirmed May 5, 2021 [T. Louie #1], para 8 and exhibits A, B, C, D.

84 Ibid, para 8 and exhibits A, B, C, D.

85 Ibid, para 8.

86 Ibid, para 12.

87 Ibid.

information and considering its implications for money laundering risk and the adequacy of existing measures.

As was the case with the first component, how this second component is enacted in practice is likely to vary between luxury goods markets. In general, this is clearly an appropriate task for the AML Commissioner; however, in markets that are already regulated, like the vehicle sales market, it may be prudent to empower – and provide necessary resources to – the existing regulator to review the available data and work in collaboration with the AML Commissioner to take action as needed.

In addition to examining previously identified luxury goods markets, the need to assess risk in the luxury goods sector on an ongoing basis also extends to the identification of new markets that fit the luxury goods risk profile described earlier in this chapter. It seems certain that new products and industries bearing a money laundering risk similar to that of existing luxury goods markets will emerge in the future. In order to adequately address this risk, it is essential that public authorities continuously examine new industries to determine whether they should be treated as luxury goods markets for anti–money laundering purposes. This again falls squarely within the anticipated role of the AML Commissioner.

Flexible and Adaptive Regulation

As crucial as ensuring that available data is reviewed and risk is assessed on an ongoing basis is ensuring that timely and effective action can be taken in response to this information. As the risk landscape for money laundering in luxury goods markets evolves, it is essential that action to address new and emerging risks can be taken quickly. Such action must be tailored to the market in question so as to respond to the risk effectively, while ensuring minimal disruption to legitimate business within the industry.

In the course of receiving the reports discussed above, the AML Commissioner may become aware of new and evolving money laundering threats requiring timely action. For example, the reporting may demonstrate an increase in suspicious transactions among yacht brokerages in a particular region of the province. A timely measure to respond to that increase might be a requirement that yacht brokers obtain proof of the source of funds used in any transaction above an identified threshold, or a temporary prohibition on using cash or another medium of exchange.

Accordingly, there should be a mechanism through which targeted measures can be put in place in response to emerging threats or changing risk landscapes that require participants to take action aimed at those threats. These actions could include requirements to report certain types of transactions, collect specific information about customers, or refuse transactions with identified risk factors – such as the use of large quantities of cash. These measures could be permanent but could also be imposed for short durations of time to respond to specific intelligence or threats or increases in suspicious activity.

My expectation is that this model will allow for significantly greater flexibility and adaptability than anti–money laundering regimes like the *PCMLTFA* while minimizing interference in legitimate business. In place of a one-size-fits-all approach that imposes the same set of permanent requirements on a broad array of industries, the targeted measures envisioned in this model would allow authorities to respond to threats rapidly and to focus their response on specific activity of concern. The response could also take into account the nature of the market in question to maximize the effectiveness of anti–money laundering measures, while reducing disruption and cost to retailers. It could also impose new restrictions or requirements only for as long as they are needed – again minimizing the burden on legitimate participants in the market.

The Province is best suited to determine how this mechanism is set up. It may be, for example, appropriate to assign the task to a particular minister (for simplicity, I will refer simply to "the minister"). The measures I am envisioning here are meant to address new and evolving money laundering risks. Consequently, the minister should be able to implement the measures quickly – without the need for legislative amendment. While the Province will determine what authority is appropriate, it strikes me that a minister having the power to issue binding directives or regulations would be effective in this regard. I add that it is essential that the minister be in close contact with – and responsive to – suggestions from the AML Commissioner and the central authority receiving the reports on cash transactions.

Recommendation 83: I recommend that the Province establish a mechanism by which a minister, in consultation with the AML Commissioner, can implement timely measures to address new and evolving risks in the luxury goods sector (as defined in Chapter 34 of this Report).

I also anticipate that this authority may have value as an information-gathering tool. The imposition of temporary measures will provide further insight into the nature of suspicious activity and the impact of possible responses. Where, for example, a temporary restriction seems to result in the complete cessation of suspicious activity, this will suggest a different kind of problem – and call for a different kind of response – than where the temporary restriction appears to result in the displacement of suspicious activity to a different market or geographic location.

Support for Voluntary Action by Industry

Based on the evidence before me, I am persuaded that coercive regulatory action is not the only means of addressing the risk of money laundering in luxury goods markets. The actions taken by the Canadian Jewellers Association and the BC Yacht Brokers Association, as described above, demonstrate that voluntary action by industry is a viable means of addressing money laundering risk. In my view, efforts to support and encourage such action should form an essential part of the Province's efforts to combat money laundering in the luxury goods sector.

The experiences of both the Canadian Jewellers Association and the BC Yacht Brokers Association suggest that while industry groups may be willing and able to take voluntary action to address money laundering risks, they will often require prompting from government to do so. The action taken by the Canadian Jewellers Association, for example, was prompted by the inclusion of dealers in precious metals and stones in the *PCMLTFA*, while the action taken by the BC Yacht Brokers Association appears to have been prompted by contact from this Commission.

While it may not be possible to persuade every luxury goods retailer to adopt measures of the sort implemented by the BC Yacht Brokers Association, the potential benefits of voluntary action are substantial and worthy of investment. In my view, the Province ought to encourage and support voluntary action by industry by proactively reaching out to industry to educate retailers and trade associations on the risks of money laundering in the markets in which they operate and strategies that industry can employ to reduce those risks. I fully expect that the vast majority of luxury goods retailers in this province want nothing to do with business connected with the proceeds of crime and would be more than willing to voluntarily implement measures to ensure that their businesses are not used to launder money.

Again, this function is well suited to the AML Commissioner, and I suggest that public engagement and education be made part of his or her mandate. Given the Commissioner's role in assessing risk and access to information, he or she will be well equipped to identify the kind of voluntary measures that will best respond to the risks facing particular industries and support those industries in taking action.

Leveraging Existing Regulatory Capacity

While the focus of the present discussion has primarily been on the role and functions of the AML Commissioner, this does not mean that there is no role for existing, industry-specific regulators in addressing the risk of money laundering. I encourage government to consider giving existing regulators, such as the Vehicle Sales Authority, explicit anti–money laundering mandates. In such instances, care should be taken to ensure that these regulators are able to work in coordination with the AML Commissioner and avoid duplication of efforts.

In my view, it is important to engage industry-specific regulators where possible for several reasons. First, as is the case with the Vehicle Sales Authority, regulators often already have access to – or at least the power to access – valuable information relevant to money laundering in the industries they regulate, which should be leveraged to advance anti–money laundering objectives. Secondly, where an industry is already regulated, it will often be the regulator and not government that is best positioned to implement new anti–money laundering measures, including those recommended by the AML Commissioner. By empowering regulators to directly implement anti–money laundering measures in the industries they already regulate, the Province can ensure that action to prevent money laundering can be taken as efficiently and effectively

as possible. Finally, adding the prevention of money laundering to the mandate of regulators reinforces that addressing this problem is a shared responsibility. There is a risk that creation of a distinct AML Commissioner can create the perception that "someone else" is responsible for solving the problem of money laundering. By explicitly tasking regulators with this responsibility, the Province can reinforce that they are an essential part of a society-wide response to this issue.

Sector-Wide Oversight and Coordination

The final necessary component of an effective anti–money laundering model for the luxury goods sector is sector-wide oversight and coordination. As discussed previously, because of the similarity in the nature of the money laundering risk facing different luxury goods markets, they may be viewed as largely interchangeable by those intent on laundering money. Moreover, efforts to discourage or disrupt money laundering activity in one luxury goods market may result in displacement to another market rather than the elimination of that activity altogether.

For this reason, it is insufficient to attempt to address the money laundering risk in individual luxury goods markets independently of one another. These efforts must be coordinated and subject to some form of sector-wide oversight. While there may be an important role to be played by market-specific regulators like the Vehicle Sales Authority, there must also be coordination between markets to assess evolving threats and the impact of anti–money laundering measures between markets. This kind of coordination may be useful in a number of ways. First, it may assist in identifying and addressing trends affecting multiple markets. An increase in suspicious activity in a single market may have different implications and call for a different response than a similar phenomenon affecting multiple luxury goods markets simultaneously. Secondly, coordination and communication across the sector may assist in identifying activity as suspicious in instances where the suspicious nature of the activity may not be apparent until connected to activity or trends elsewhere in the economy. Finally, coordination within the sector may assist in determining whether measures enacted in one market have led to displacement to another.

There is an obvious role for the AML Commissioner in ensuring coordination across the luxury goods sector (and beyond). To the extent that regulators are empowered to take direct action on money laundering, it is imperative that they share information and work collaboratively with the AML Commissioner to ensure that their actions are not unnecessarily redundant and that they avoid working at cross-purposes. While the precise nature of the relationship between the AML Commissioner and regulators will necessarily vary depending on the nature of the industry and role of the regulator, there must always be a strong relationship between the commissioner and the regulator that enables coordinated action.

Money Laundering Through Grey Market Vehicle Exports

Grey market export of vehicles involves the purchase of vehicles in British Columbia and their export and resale to purchasers in other jurisdictions for amounts that exceed the purchase price paid, resulting in a profit for the exporter. In theory, grey market vehicle exports could facilitate money laundering where the exported vehicle was initially acquired with the proceeds of crime. The export of such a vehicle would serve the purpose of transferring the illicit funds used to acquire it to another jurisdiction, while the resale of the vehicle would provide an apparently legitimate explanation for the funds and potentially facilitate their placement into the financial system.

This typology was the subject of some discussion in Dr. German's second report, which identified the grey market vehicle exports as a possible form of trade-based money laundering.[88] Dr. German concluded, based largely on provincial sales tax data obtained from the provincial government, that grey market vehicle exports had increased substantially in recent years.[89] The relevance of this data is that, in some circumstances, individuals who resell or export a vehicle following purchase are exempt from paying provincial sales taxes that would normally be payable on the sale of a vehicle.[90] Where provincial sales tax was paid at the time of purchase but the exemption applies, the purchaser can apply to the provincial government for a rebate.[91] On this basis, Dr. German concluded that "[t]he number of applications for refunds of PST on vehicles is a strong indication of the size of the grey market for exported vehicles from B.C."[92] He interpreted a substantial increase in applications for provincial sales tax rebates, beginning in 2016, as evidence of a substantial increase in vehicle exports.[93]

The Commission obtained further provincial sales tax data for years subsequent to those included in Dr. German's review.[94] This data disclosed that although applications for provincial sales tax rebates associated with the resale of vehicles had declined from their peak in 2018, they remained elevated – relative to 2015 levels – in the two years subsequent to the last year for which Dr. German received data.[95]

In addition to the potential money laundering risk associated with grey market vehicle exports, this activity is clearly of significant concern to vehicle manufacturers. Dr. German alluded to this concern and the efforts made by manufacturers to prevent this activity in his second report.[96] The Commission also received evidence from

88 Exhibit 833, *Dirty Money 2*, p 195.
89 Ibid, p 196.
90 Exhibit 779, Affidavit No. 1 of Michelle Lee, made on March 22, 2021 [M. Lee #1], paras 4–12.
91 Ibid, para 8.
92 Exhibit 833, *Dirty Money 2*, p 198.
93 Ibid, pp 198–99.
94 Exhibit 779, M. Lee #1.
95 Ibid, paras 19–20.
96 Exhibit 833, *Dirty Money 2*, p 197.

Norman Shields, vice-president of finance and administration at BMW Canada Inc., detailing the challenges that grey market exports pose for BMW and the efforts it has made to prevent and respond to this practice.[97]

I am persuaded that grey market vehicle exports pose a real risk of money laundering, and I accept that the practice has significant negative repercussions for vehicle manufacturers. The available data does not, however, allow me to draw conclusions as to the extent to which grey market vehicle exports from British Columbia are connected to actual money laundering.

While grey market vehicle exports present an opportunity for money laundering, they cannot be assumed to be connected to money laundering in all cases. Grey market exports may be contrary to the terms of agreements between motor vehicle dealers and purchasers, but do not amount to criminal activity per se.[98] It is apparent from the evidence before me that exporters engage in practices that may give their activities the appearance of criminality or illegality, such as the use of nominee or "straw" buyers.[99] However, it is unclear whether, and to what extent, these practices are motivated by a desire on the part of exporters to distance themselves from illicit proceeds used to purchase vehicles as opposed to a desire to circumvent manufacturer and dealer efforts to prevent grey market exports.[100]

The connection between grey market vehicle exports and criminality is rendered even more tenuous by the apparent economic rationality of engaging in grey market export of vehicles acquired with legitimate funds. Dr. German indicated in his report that international price differentials ensure "huge profits" for exported vehicles.[101] If this is the case, then the grey market export of vehicles offers the opportunity for profit and is economically viable even if the vehicles are acquired with legitimate funds.

Accordingly, while the grey market export of vehicles is often discussed in a manner that suggests it is synonymous with money laundering, in my view, the connection is not so clear. Based on the evidence before me, grey market export of vehicles is itself a potentially profitable business model, including where the exported vehicles are purchased with legitimate funds. Grey market vehicle exports may also be used by those intent on laundering money by offering a convenient market for the sale of vehicles purchased with the proceeds of crime; however, in my view, it is not the case that grey market vehicle exports invariably occur in the context of a money laundering scheme, nor is it necessarily the case that the increase in grey market vehicle exports in recent years correlates to an increase in money laundering.

97 Exhibit 778, Affidavit No. 1 of Norman Shields, made on March 26, 2021.

98 Exhibit 777, Affidavit No. 1 of Marko Goluza, made on March 25, 2021 [M. Goluza #1], p 210; Exhibit 779, M. Lee #1, exhibit E.

99 Exhibit 777, M. Goluza #1, p 210; Exhibit 779, M. Lee #1, para 21, see also exhibit E; Exhibit 778, T. Shields #1, paras 18–35.

100 Exhibit 777, M. Goluza #1, p 219.

101 Exhibit 833, *Dirty Money 2*, p 196.

In light of this tenuous connection between grey market vehicle exports and money laundering, I am not persuaded that such exports should be the primary point of focus for efforts to combat money laundering using motor vehicles. By the time a vehicle is exported, it will be difficult to immediately distinguish vehicles acquired with proceeds of crime from those purchased with legitimate funds and, consequently, difficult to distinguish those vehicles being exported as part of a money laundering scheme from those being exported in violation of a private agreement between dealer and purchaser – or even those being exported entirely legitimately. Further, by the time an attempt is made to export a vehicle purchased with proceeds of crime, the illicit funds have already successfully been converted into the vehicle and, to an extent, successfully laundered. For these reasons, in my view, the primary focus of efforts to combat money laundering through the trade of vehicles is at the point at which vehicles are acquired using illicit funds. It is at this stage that money laundering transactions can likely be most easily detected and money laundering most completely prevented.

This does not mean that vehicle exports are not a cause for concern. While the extent to which proceeds of crime are actually being laundered through vehicle exports is unclear, I am persuaded that the *risk* of vehicles purchased with illicit funds being exported through British Columbia's ports is sufficiently significant that some scrutiny should be applied to these activities. The Province should regulate the purchase and sale of vehicles for the purpose of export from British Columbia. Regulation of this activity should involve, at a minimum, a registration requirement for those who export more than an identified number of vehicles annually and a requirement that the export of all vehicles by registered exporters be reported prior to export. Failure to register and failure to report as required should amount to provincial offences. This reporting requirement will ensure that a clear record exists of what vehicles have been exported and by whom, obviating the need to rely on provincial sales tax data for this purpose. The Province should consult with the Vehicle Sales Authority in order to determine whether it is feasible and appropriate for the mandate of the Authority to be expanded to include vehicle exporters.

Recommendation 84: I recommend that the Province regulate the purchase and sale of vehicles for the purpose of export from British Columbia. This regulation should involve, at a minimum, a registration requirement for those who export more than an identified number of vehicles annually and a requirement that the export of all vehicles by registered exporters be reported prior to export.

To assist in the effective regulation of motor vehicle exports, the Province should amend the *Provincial Sales Tax Act*, SBC 2012, c 35, to ensure that information collected for the purpose of processing provincial sales tax rebates is available to the Vehicle Sales Authority or other body tasked with regulating this activity. Currently, the

limits on disclosure of this information[102] are so restrictive that the Commission was unable to obtain access to the complete records even through the use of its summons power.[103] While there is undoubtedly a need to limit dissemination of these records, I am convinced that this information – particularly that which was unavailable to the Commission – would be of significant assistance in efforts to regulate this practice.

Recommendation 85: I recommend that the Province amend the *Provincial Sales Tax Act* to ensure that information collected for the purpose of processing provincial sales tax rebates is available, at a minimum, to the Vehicle Sales Authority and the AML Commissioner.

Insurance Council of British Columbia

A final issue I wish to address before concluding this chapter is money laundering risk and regulation in the insurance industry. Alongside evidence related to money laundering in the luxury goods market, the Commission received evidence from Marko Goluza, director of professional conduct for the Insurance Council of British Columbia, regarding the risk of money laundering in the insurance market and efforts being made by the Insurance Council of BC to address this risk.[104] The Insurance Council of BC is a regulatory body established under section 220 of the *Financial Institutions Act*, RSBC 1996, c 141, with responsibility for licensing and regulating insurance agents, insurance salespersons, insurance adjusters, and employed insurance adjusters.[105]

I would not consider insurance itself to meet the criteria for inclusion in the "luxury goods" category as outlined above. I have included it in the present chapter, however, because of the close connection between insurance and money laundering through vehicle sales, and particularly vehicle exports.

Mr. Goluza's evidence touches briefly on an identified theoretical risk of money laundering through the life insurance market, involving individuals purchasing life insurance policies with the proceeds of crime and subsequently cashing in those policies, thereby obscuring the source of the funds used to purchase the original policy.[106] I refer to this risk as "theoretical" as the Insurance Council of BC has not confirmed any cases in which this money laundering typology has actually been employed, and as such, there is no evidence that money laundering using this method is actually occurring in this province.[107]

102 *Provincial Sales Tax Act*, SBC 2012, c 35, s 228.
103 *Public Inquiry Act*, SBC 2007, c 9, s 22.
104 Exhibit 777, M. Goluza #1.
105 Ibid, para 6.
106 Ibid, paras 30–31.
107 Ibid, para 30.

In his evidence, Mr. Goluza indicated that the indicators of money laundering that the Insurance Council of BC has actually observed have related predominantly to the motor vehicle insurance and the role of insurance professionals in facilitating the grey market export of vehicles.[108] These indicators include:[109]

- vehicle type (late-model, luxury vehicles);
- quick transfers of ownership from straw buyers to exporters;
- pre-determined and timely cancellation of one-year insurance policies;
- a contact known by a licensed insurance professional at a dealership; and
- a common exporter across multiple transactions.

Mr. Goluza's evidence also detailed the efforts being made by the Insurance Council of BC to take action to address money laundering in and connected to the insurance market.[110] Money laundering was specifically referred to in the following strategy identified in the Insurance Council's 2020–2023 Strategic Plan:

> Assess regulatory processes and modify as needed to detect and counter money laundering activities in the insurance industry.[111]

Three key performance indicators connected to money laundering have also been identified as part of the Insurance Council's strategic planning:[112]

a. to ensure staff are trained on money laundering detection techniques;

b. to complete random practice audits to review licensee compliance with [FINTRAC] money laundering and terrorist finance guidelines; and

c. to ensure applicants for licensure are screened for money laundering and terrorist financing activities per FINTRAC guidelines.

Since the 2020–2023 Strategic Plan has come into effect, the Insurance Council of BC has taken action to pursue these goals by increasing organizational competency, including via staff training; reviewing processes to ensure alignment with FINTRAC guidelines; identifying activity that may be associated with money laundering in practice audits and investigations; and actively participating in the Counter Illicit Finance Alliance of British Columbia, discussed in Chapter 39.[113]

Notably, Mr. Goluza indicates in his evidence that the actions taken by the Insurance Council of BC with respect to money laundering in the industry it regulates have led to

108 Ibid, paras 32–35 and exhibits 11–14.

109 Ibid, para 32.

110 Ibid, paras 21–29, 36–41.

111 Ibid, para 18.

112 Ibid, para 20.

113 Ibid, para 21.

disciplinary action against two licensees related to the issuance of insurance connected to the grey market vehicle exports.[114] The Insurance Council was unable to confirm whether these matters were also connected to money laundering, and for the reasons discussed above, I caution against the assumption that they were. Mr. Goluza suggests, however, that it may have been possible to make this determination with access to additional information about the source of funds used to acquire the vehicles in question.[115]

In my view, the Insurance Council of BC should be commended for the efforts it has made to address money laundering in and connected to the insurance industry, and the Province should consider providing the Insurance Council with additional support to further enhance its efforts. The Insurance Council has managed to take these limited but meaningful steps to address money laundering risks in its industry in the absence of an explicit anti–money laundering mandate and using its existing authority and resources.[116]

I encourage the Province to work with the Insurance Council of BC to ensure that it has the support required to further advance its efforts to address money laundering in and connected to the insurance industry. This could include giving the Insurance Council an explicit anti–money laundering mandate. In his evidence, Mr. Goluza identified a number of additional measures that would assist the Insurance Council in effectively addressing money laundering in the industry it regulates.[117] On the evidence before me, I am unable to determine whether each of these measures should be implemented or to make a recommendation in this regard. However, given the efforts already made by the Insurance Council to address this issue – even in the absence of an explicit statutory mandate to do so – the Province should take these proposals seriously and begin consultations with the Insurance Council and other affected parties to determine how the efforts already being made by the Insurance Council can be supported and advanced by the Province. These consultations should include, in particular, consideration of the following measures proposed by Mr. Goluza:

- adding a "duty to report" provision to the *Financial Institutions Act* that would require licensees to report identified conduct to ensure that the Insurance Council of BC has timely access to information related to suspicious transactions and possible money laundering in the insurance industry;[118]
- clarifying section 231(1)(b) of the *Financial Institutions Act* to ensure that it clearly provides that the Insurance Council of BC may levy separate fines up to the maximum allowable fine for each individual contravention of "a term, condition or restriction of the licence of the licensee";[119]

114 Ibid, paras 33–34.
115 Ibid, para 35.
116 Ibid, paras 12–14.
117 Ibid, paras 42–53.
118 Ibid, para 45.
119 Ibid, paras 46–48.

- increasing the maximum fines that can be levied by the Insurance Council of BC;[120]
- creating an administrative penalty regime for minor and technical breaches by licensees;[121]
- expanding the type of disciplinary measures that may be imposed by the Insurance Council of BC;[122] and
- exempting the Insurance Council of BC from the Public Sector Employees' Council Guidelines to ensure that it is able to offer remuneration adequate to permit hiring experienced insurance professionals.[123]

Conclusion

For the reasons discussed above, it is clear to me not only that the luxury goods sector is at high risk for money laundering but that illicit funds are being used to purchase luxury goods in this province. While I am unable to identify with precision the extent to which such activity is occurring, I am convinced it is presently a significant problem that is largely unchecked. Because of the high value, capacity to retain value, transferability, and portability of luxury goods, there is the very real potential that enormous amounts of illicit funds are being converted, transferred, transported, and ultimately laundered through the markets that comprise this economic sector. It is clear that this potential has been realized in British Columbia. That there is limited data available about money laundering through the luxury goods markets in British Columbia is the product of the reality that, in this province, no one has been watching.

Given the elevated risk associated with luxury goods markets, this is unacceptable. The Province must proactively work to uncover money laundering and the use of illicit funds in this sector and take action to drastically reduce the elevated risk of money laundering present in this sector by implementing measures that give effect to the principles outlined above.

120 Ibid, para 49.
121 Ibid, para 50.
122 Ibid, para 51.
123 Ibid, para 53.

Chapter 35
Virtual Assets

Unlike other topics I have discussed in this Report, virtual assets are unique in that many cannot readily describe what they are, let alone imagine how they might be misused for money laundering purposes. By far the most well-known virtual asset is Bitcoin, which emerged roughly 13 years ago and continues to dominate the sector. Yet, some 7,700 other virtual assets exist, and their characteristics, functions, and uses – both legitimate and illegitimate – have developed rapidly in a relatively short period of time. That criminals are already exploiting this new technology is illustrative of the need for governments, regulators, and law enforcement to actively monitor new technologies and develop the expertise needed to disrupt the use of virtual assets in money laundering schemes.

It is challenging to define a virtual asset in simple terms. The Financial Action Task Force describes a virtual asset as "a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes."[1] In some ways, we can make an analogy between virtual assets and normal "fiat" currency (i.e., real-world money or bank-issued currencies[2]); however, as I elaborate below, the analogy is not a perfect fit. Further, alongside the term "virtual asset," a new vocabulary has emerged, which includes terms such as "cryptocurrency," "cryptography," "blockchain," "hot wallets," "cold wallets," and "mining."

In this chapter, I first explain various concepts relating to virtual assets and how transactions are completed. Notably, many virtual asset transactions are, despite their complexity, highly visible: a good deal of information is publicly available on

1 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 126, definition of "virtual asset."

2 Evidence of A. Vickery, Transcript, November 23, 2020, p 21.

the blockchain, which essentially functions as a public ledger of transactions. I then set out the regulatory scheme applicable to virtual assets, which is largely contained in the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, SC 2000, c 17 (*PCMLTFA*). The scheme is new, having come into force in June 2020 and June 2021, rendering it difficult to determine how effective it is at this stage. Nonetheless, it is a promising step. Finally, I discuss crime involving virtual assets and methods of investigation. The virtual asset space poses unique challenges for law enforcement, because it is a rapidly developing and complex area, as well as opportunities for disruption of money laundering activity, because a significant amount of information is available publicly on the blockchain. It is essential that law enforcement, regulators, and government develop and maintain expertise in the area of virtual assets, which will undoubtedly continue to be exploited by criminals.

What Is a Virtual Asset?

As noted above, the Financial Action Task Force defines "virtual asset" as "a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes." It further notes that virtual assets do *not* include digital representations of fiat currencies, securities, or other financial assets covered in its 40 recommendations (discussed in Chapter 6).[3] As that definition suggests, a virtual asset can serve a few functions:

- as a medium of exchange, by operating like a currency in some environments;
- as a unit of account, by defining, recording, or comparing value; and/or
- as a store of value, by having value to a creditor willing to accept it.[4]

There are two broad categories of virtual assets. A **non-convertible virtual asset** has value only within the domain in which it is used. For example, some online games have their own "currency," such as World of Warcraft Gold.[5] In contrast, a **convertible virtual asset** can be converted into fiat money; in other words, it has an equivalent value in real currency or acts as a substitute for real currency.[6] A convertible virtual asset can be centralized, meaning it has a single administering authority or a kind of central bank, or decentralized, meaning it lacks a central administrator and instead operates peer to peer.[7]

3 Exhibit 4, Appendix E, *FATF Recommendations*, p 126, definition of "virtual asset."

4 Exhibit 253, RCMP Virtual Assets Slideshow, slide 4; Evidence of A. Vickery, Transcript, November 23, 2020, p 17.

5 A "real life" comparison is Canadian Tire money, which has value at Canadian Tire but not elsewhere: Evidence of A. Vickery, Transcript, November 23, 2020, p 19.

6 Exhibit 253, RCMP Virtual Assets Slideshow, slide 5; Evidence of A. Vickery, Transcript, November 23, 2020, pp 19–21; Exhibit 248, Overview Report: FATF Publications on Virtual Assets, Appendix H, *US Department of Justice, Report of the Attorney General's Cyber Digital Task Force: Cryptocurrency Enforcement Framework* [US Cryptocurrency Enforcement Framework], pp 2–3.

7 Exhibit 248, Appendix H, US Cryptocurrency Enforcement Framework, p 3; Exhibit 253, RCMP Virtual Assets Slideshow, slide 5; Evidence of A. Vickery, Transcript, November 23, 2020, p 20.

Bringing the above points together, a cryptocurrency is a type of virtual asset that (a) is convertible; (b) is decentralized; and (c) uses cryptography, which is a method of securing transactions.[8] Unlike traditional currencies, cryptocurrencies do not have legal tender status in any country, and their exchange value depends on agreement or trust among their community of users.[9] As I elaborate below, cryptocurrency can be exchanged directly from person to person, through a cryptocurrency exchange, or through other intermediaries.

Bitcoin is the most popular and well-known cryptocurrency. Although more than 7,700 cryptocurrencies exist, over 62 percent of cryptocurrency transactions are done in bitcoin.[10] Its popularity is due mostly to its accessibility: it was the first widely accepted and used cryptocurrency and is the most widely featured, accepted, and exchanged, rendering it more accessible for new users.[11] People sometimes use the term "Bitcoin" when generically referring to cryptocurrency,[12] and much of the focus in the evidence before me was on Bitcoin rather than cryptocurrencies generally.

The value of Bitcoin has varied considerably since its inception. In 2017, its value notably reached $20,000, at which time its market capitalization[13] was approximately $20 billion. At that time, 10 other cryptocurrencies had a market capitalization of over $100,000. The value of Bitcoin varied between 2017 and 2020, falling to $10,000 in 2018. However, in 2020, Bitcoin's market capitalization had grown to approximately $300 billion, and the values of the other top 10 cryptocurrencies were 10 times those of 2017.[14] As of April 19, 2022, Bitcoin's value was $52,186.30.[15]

How Does a Cryptocurrency Transaction Work?

Understanding how a cryptocurrency transaction works requires a review of some key concepts. First, transactions require the use of a "private key" and a "public key."

8 Exhibit 253, RCMP Virtual Assets Slideshow, slide 5; Exhibit 248, Appendix H, US Cryptocurrency Enforcement Framework, p 3; Evidence of A. Vickery, Transcript, November 23, 2020, pp 20–21.

9 Exhibit 248, Appendix H, US Cryptocurrency Enforcement Framework, pp 2–3. However, Sgt. Vickery noted that some countries, such as China and Venezuela, are considering the possibility of a virtual currency tied to or managed by a national banking authority. Canada is part of a working group with other countries seeking to identify best practices and approaches in this regard: Evidence of A. Vickery, Transcript, November 23, 2020, p 26.

10 Evidence of A. Vickery, Transcript, November 23, 2020, p 88. "Bitcoin" with an uppercase B refers to the payment system, whereas units of bitcoin take a lowercase B: Exhibit 254, Senate Report, *Digital Currency: You Can't Flip This Coin!* (June 2015), p 6.

11 Evidence of J. Spiro, Transcript, November 24, 2020, pp 55–56; Evidence of A. Gilkes, Transcript, November 23, 2020, pp 24–25.

12 Evidence of A. Gilkes, Transcript, November 23, 2020, p 25.

13 Market capitalization refers to the overall value of a cryptocurrency, which is obtained by multiplying the value of each coin by the number of coins in circulation: Evidence of A. Gilkes, Transcript, November 23, 2020, p 21.

14 Exhibit 253, RCMP Virtual Assets Slideshow, slides 6 and 7; Evidence of A. Gilkes, Transcript, November 23, 2020, pp 21–22.

15 Coinbase, "Price Charts: Bitcoin Price," online: https://www.coinbase.com/price/bitcoin.

A private key functions as a PIN or password and is needed to spend cryptocurrency.[16] A public key is roughly akin to a bank account number and is used to actually send or receive cryptocurrency.[17] Private and public keys consist of lengthy combinations of numbers and letters.[18]

Cryptocurrency is stored in a digital wallet, which is similar to a virtual account. Wallets interface with blockchains and generate or store the public and private keys.[19] There are several kinds of wallets:

- **Online wallets** are associated with cryptocurrency exchanges, which, as I discuss below, are services that provide a forum to exchange cryptocurrency with other users. Online wallets provide the least amount of control for the user, as the exchange maintains control of the user's private key through a "custodial wallet."[20]
- **Desktop wallets** are generated on a computer. Users maintain control of both the private and the public keys and have full control over their transactions. Conducting transactions using a desktop wallet tends to be very fast.[21]
- **Mobile wallets** are essentially the same as desktop wallets except that they are generated on a smartphone.[22]
- **Hardware wallets** are small, encrypted devices similar to USB keys, which are created specifically to store private keys. With a hardware wallet, users can spend cryptocurrency completely free from the internet. However, because they cost around $100, they tend to be less popular for casual users.[23]
- **Paper wallets** are private and public keys printed on paper. They can be generated automatically through a visit to a cryptocurrency ATM, which, as I elaborate below, is a machine similar to a traditional ATM that allows a user to buy or sell cryptocurrency.[24]

Wallets can be "hot" or "cold." A hot wallet is one where the user's private key is or has been online, whereas with a cold wallet, the private key has never been online.

16 Exhibit 248, Appendix H, US Cryptocurrency Enforcement Framework, p 3; Evidence of A. Gilkes, Transcript, November 23, 2020, p 50.

17 Exhibit 248, Appendix H, US Cryptocurrency Enforcement Framework, p 3; Evidence of A. Gilkes, Transcript, November 23, 2020, pp 51–52.

18 See Exhibit 253, RCMP Virtual Assets Slideshow, slide 12 for examples.

19 Exhibit 248, Appendix H, US Cryptocurrency Enforcement Framework, p 3.

20 Evidence of A. Gilkes, Transcript, November 23, 2020, pp 53–54; Evidence of A. Vickery, Transcript, November 23, 2020, p 62.

21 Evidence of A. Gilkes, Transcript, November 23, 2020, p 54; Exhibit 248, Appendix H, US Cryptocurrency Enforcement Framework, p 3.

22 Evidence of A. Gilkes, Transcript, November 23, 2020, p 54; Exhibit 248, Appendix H, US Cryptocurrency Enforcement Framework, p 3.

23 Evidence of A. Gilkes, Transcript, November 23, 2020, pp 56–58; Exhibit 248, Appendix H, US Cryptocurrency Enforcement Framework, p 3.

24 Evidence of A. Gilkes, Transcript, November 23, 2020, pp 56–57; Exhibit 248, Appendix H, US Cryptocurrency Enforcement Framework, p 3.

The first three wallets listed above are hot wallets, and the last two are cold wallets. Cold wallets are more secure than hot wallets in that, if prepared properly, they have never been online and are therefore not at risk of being targeted by malware or related threats. The trade-off is that spending cryptocurrency using a cold wallet requires a little more time and effort. Desktop and mobile wallets are less secure insofar as users risk losing their keys or cryptocurrency if a device becomes corrupted, lost, or subject to malware. However, a user may be able to use a "seed phrase," which is a combination of 12 to 24 words, to recover a wallet. Finally, an online wallet with an exchange is secure in the sense that the exchange takes care of the private keys and uses its network security to ensure that no one else has access. The exchange can also help a user who loses their wallet or login information to recover the wallet.[25]

Cryptocurrency transactions occur on the blockchain,[26] which is a public ledger that captures the history of all verified transactions.[27] (Note, however, that not all cryptocurrencies have a public blockchain;[28] the discussion that follows relates primarily to those that do.) A report prepared by the Standing Senate Committee on Banking, Trade, and Commerce explains the concept of a public ledger as follows:

> The public ledger is exactly what it sounds like – a large bulletin board (written in a cryptic computer database called the blockchain). The public ledger logs and broadcasts transactions to the entire network.
>
> Everyday transactions – using, for example, a debit or credit card to buy a cup of coffee – are tied to a bank. If you have enough money in your account, or credit on the card, the bank authorizes the transaction and you get your coffee. If you bought that same cup of coffee with bitcoin, you would simply announce it on the public ledger without the bank or any other financial institution (and all their transaction fees) being involved. The merchant gets their money and you get your coffee.
>
> The public ledger is always accessible through computers literate in the blockchain. It cannot be forged or changed. It provides a permanent record of all bitcoin transactions that have ever happened, a history that within an hour is unalterable.[29]

Each block in the blockchain consists of a group of reported transactions in chronological order.[30] Once a transaction has been verified and added to the

25 Evidence of A. Gilkes, Transcript, November 23, 2020, pp 54–59.

26 While my focus here is on blockchain technology used in cryptocurrencies, I note that blockchain can also be used for non-cryptocurrency purposes. For example, Walmart has used it to track the movement of produce from the crops through to the distribution centre and the store shelf, which can assist with tracking outbreaks of listeria and the like: Evidence of A. Vickery, Transcript, November 23, 2020, p 92. Blockchain has also been used in situations such as digital voting, art, music, and collective decision-making: Transcript, November 25, 2020, p 142.

27 Exhibit 248, Appendix H, US Cryptocurrency Enforcement Framework, p 4.

28 Evidence of A. Gilkes, Transcript, November 23, 2020, p 33.

29 Exhibit 254, Senate Report, *Digital Currency: You Can't Flip This Coin!* (June 2015), pp 6–7.

30 Exhibit 248, Appendix H, US Cryptocurrency Enforcement Framework, p 4.

blockchain, the block is permanent and cannot be modified, deleted, or removed. In this way, the use of a blockchain prevents double-spending and counterfeiting.[31]

The blockchain is often called "pseudo-anonymous" because almost all the information is publicly available except the identity and location of the person who conducted the transaction.[32] The blockchain shows information such as the date and time of transactions, the accounts that the cryptocurrency was sent from and to, the transaction number, the transaction fee, and the amount transacted.[33] As I elaborate later in this chapter, the public nature of the blockchain is helpful for law enforcement when investigating crime involving virtual assets.

Transactions are verified and added to the blockchain through a process called "mining." When a user initiates a transaction, it is encrypted with a private key and then submitted on the network for verification by special users known as "miners." Miners verify that the units have not already been spent and validate the transaction by solving a complex algorithm called a "random hash algorithm." In exchange for mining, miners are paid transaction fees by the sender of the funds. These fees do not depend on the size of the transaction but rather by demand: if there is a high demand for transactions, senders may increase their transaction fee to incentivize miners to validate the transaction faster.[34]

As Sergeant Aaron Gilkes of the RCMP explained, the mining process is competitive. He noted that there is a finite number of bitcoins that will exist. To ensure that there are enough bitcoins to be distributed at a proper pace, it has to take approximately 10 minutes for each block of the blockchain to be solved. Depending on how many miners are working to solve the blocks, the software will adjust the difficulty of solving the random hash algorithm. The first miner to reach the "hash" number set by the software is awarded the block and receives transaction fees as well as the initial coins that are discovered.[35] Thus, "it is a competition as to who can solve that equation the fastest and who can add that block of transactions to the blockchain the fastest."[36]

31 Evidence of A. Gilkes, Transcript, November 23, 2020, pp 27–28; Exhibit 248, Appendix H, US Cryptocurrency Enforcement Framework, p 4.

32 Evidence of A. Gilkes, Transcript, November 23, 2020, pp 35–36.

33 Ibid, pp 34–35. For an example of information available on the blockchain see Exhibit 253, RCMP Virtual Assets Slideshow, slide 10.

34 Exhibit 254, Senate Report, *Digital Currency: You Can't Flip This Coin!* (June 2015), p 29; Exhibit 248, Appendix H, US Cryptocurrency Enforcement Framework, p 4; Evidence of A. Gilkes, Transcript, November 23, 2020, pp 28–29, 30–31, 35; Evidence of A. Vickery, Transcript, November 23, 2020, pp 31–32.

35 Sgt. Gilkes noted that the term "miners" is used because when a block is added, the miners are paid in newly minted bitcoin, that is, coins that "didn't exist before or they weren't in circulation before, but now they're being distributed through the discovery of a new block": Transcript, November 23, 2020, p 30.

36 Evidence of A. Gilkes, Transcript, November 23, 2020, pp 30–31. Sgt. Gilkes explained that mining requires special, powerful computers that generate an enormous amount of heat and require an enormous amount of electricity to function. He added that, given the cold climate, inexpensive electricity, and minimal regulation in Quebec, it has become a popular place for miners to locate their computers: Evidence of A. Gilkes, Transcript, November 23, 2020, pp 38–39; Exhibit 253, RCMP Virtual Assets Slideshow, slide 9.

Alternative Coins

While Bitcoin is by far the most popular cryptocurrency, some of its features are unattractive to certain users, both legitimate and illicit. First, the fact that the blockchain is transparent poses obvious problems for criminals and may also be unattractive for legitimate users concerned about privacy. Second, there is the potential for high transaction fees during times of high demand. For example, when Bitcoin was at its highest value in 2017, transaction fees were US$55 per transaction. Third, the volatility of Bitcoin's value leads to unstable purchasing power. Fourth, there can be long wait times because only about seven transactions can be processed per second (compared to around 24,000 Visa transactions or 200 PayPal transactions per second). Fifth, as Bitcoin is not backed by a central authority, there is no insurance or legal recourse if a user's account is compromised. Finally, transactions are irreversible: if a user sends funds to the wrong key, there is no way to undo the transaction.[37]

Alternative coins have developed to address these deficiencies.[38] Stable coins are backed by fiat currency, a stable commodity such as gold, other cryptocurrencies, or algorithms. This backing addresses the volatility issue, rendering the coin less vulnerable to fluctuation.[39] Meanwhile, privacy coins (also known as "anonymity-enhanced cryptocurrencies") offer enhanced encryption and privacy features that potentially obfuscate the ability to trace transactions. Privacy coins are very attractive for illicit users, as they allow the movement of funds across borders without detection by law enforcement, government, regulators, or the private sector. They can, however, also be attractive to legitimate users, such as those who are particularly concerned about data privacy or who are living under authoritarian regimes.[40]

Privacy coins pose obvious money laundering vulnerabilities. Notably, aftermarket software tools are not able to provide services with respect to closed blockchain ledgers, with the result that these tools cannot provide analysis on transactions involving privacy coins.[41] This is an area requiring further study and attention, as criminals will undoubtedly seek to take advantage of the anonymity provided by privacy coins and the difficulties in investigating transactions on closed blockchains.

Modes of Exchange

There are various methods of exchanging cryptocurrency, each with its own advantages and risks. I review each in turn.

37 Evidence of A. Vickery, Transcript, November 23, 2020, pp 88–90; Evidence of A. Gilkes, Transcript, November 23, 2020, pp 32–33.

38 Evidence of A Vickery, Transcript, November 23, 2020, p 90.

39 Exhibit 253, RCMP Virtual Assets Slideshow, slide 25; Evidence of J. Spiro, Transcript, November 24, 2020, p 56; Evidence of A. Vickery, Transcript, November 23, 2020, pp 90–91.

40 Evidence of J. Spiro, Transcript, November 24, 2020, pp 54–60; Evidence of A. Vickery, Transcript, November 23, 2020, p 91; Exhibit 248, Appendix H, US Cryptocurrency Enforcement Framework, p 4; Exhibit 253, RCMP Virtual Assets Slideshow, slide 25.

41 Evidence of J. Spiro, Transcript, November 24, 2020, p 57.

Public Exchanges

Public exchanges, also known as centralized exchanges, are the most popular method for individuals to purchase cryptocurrency. They allow users to purchase or sell cryptocurrency, as well as convert it into other cryptocurrencies, and are usually funded through transaction fees. They can be brick-and-mortar businesses or online businesses.[42]

As I noted above, exchanges take custody of a user's private key through a custodial wallet. As a result, users are not really in control of their private keys.[43] The private keys are not retained within the exchange itself – an arrangement meant to protect both the exchange and users from potential hacks. Most private keys are stored in a cold wallet, and the exchange keeps only what is necessary to meet the supply and demand of transactions in its hot wallet. As the reserve depletes, the exchange can replenish it from the cold wallet.[44]

Concerns about the storage of private keys by exchanges were raised in the case of an exchange called QuadrigaCX (Quadriga), whose co-founder and chief executive officer was found by staff at the Ontario Securities Commission to have engaged in fraudulent activities. I discuss Quadriga and the Ontario Securities Commission report below.

As of June 2021, public exchanges are deemed to be money services businesses under the *PCMLTFA* and therefore have all the typical customer due diligence and other obligations under that regime. They are also required to register with FINTRAC. However, prior to the amendments, most exchanges gathered a significant amount of information from clients, including their name, address, phone number, a photo of the client holding their government-issued photo identification, bank account information, and transaction history.[45] The exchange would usually run an algorithm on the photo of the client holding their government-issued ID to confirm that they were who they said they were.[46]

Sergeant Adrienne Vickery, the national cryptocurrency coordinator at the RCMP, characterized exchanges as being the "on ramps" or "off ramps" of cryptocurrencies in the sense that they provide methods of cashing out cryptocurrency into fiat currency. When law enforcement can trace a transaction going to an exchange, it can seek a production order to obtain the information in their possession.[47]

42 Exhibit 253, RCMP Virtual Assets Slideshow, slide 15; Evidence of A. Vickery, Transcript, November 23, 2020, p 62; Evidence of A. Gilkes, Transcript, November 23, 2020, p 59.

43 Evidence of A. Vickery, Transcript, November 23, 2020, p 62.

44 Ibid, p 63.

45 Exhibit 253, RCMP Virtual Assets Slideshow, slide 16.

46 Some exchanges had been victims of fraud where corrupt entities had bought images of individuals holding a driver's licence on the dark web. The algorithm was meant to prevent that from happening: Evidence of A. Vickery, Transcript, November 23, 2020, pp 60–62.

47 Evidence of A. Vickery, Transcript, November 23, 2020, pp 45–46. See also Evidence of J. Spiro, Transcript, November 24, 2020, pp 63–64.

Private Exchanges

A private exchange is a peer-to-peer platform that connects buyers and sellers of cryptocurrency. In a similar way to Craigslist or Kijiji, a seller or purchaser of cryptocurrency can post an advertisement to buy or sell cryptocurrency.[48] Many private exchanges exist. One of the most common is Paxful, which advertises over 300 payment methods, including cash and gift cards.[49]

Sergeant Vickery testified that from a law enforcement perspective, private exchanges are a very risky way to purchase cryptocurrency. They are very expensive compared to public exchanges: whereas a public exchange typically charges fees of ¼ to 4 percent, private exchanges charge around 10 to 15 percent. Users are willing to pay those fees because the exchange offers anonymity.[50] Further, the variety of payment options makes it difficult for law enforcement to follow the flow of funds.[51]

Individuals using private exchanges often meet in person to exchange cash. Although transactions on the blockchain take at least 10 minutes, it may take an hour or more for the transaction to be validated and to appear on the blockchain. As individuals meeting in person are unlikely to wait the 30 to 60 minutes to ensure a transaction is validated, there is a risk of fraud. In some cases, individuals have been assaulted or had bags of cash stolen.[52]

Cryptocurrency ATMs

Cryptocurrency ATMs or "kiosks" are "stand-alone machines that allow users to convert fiat currency to and from Bitcoin and other currencies." Users can buy or sell cryptocurrency with their mobile devices or have it delivered in the form of a paper wallet.[53]

Fees associated with using cryptocurrency ATMs are typically higher than with exchanges. There are certainly uses for legitimate users: for example, ATMs can be useful for traditionally unbanked people to be able to deal with and transact currency all over the world.[54] Further, they are attractive to those who do not want to rely on a third party holding assets for them or to share personal information with companies.[55] However, as I elaborate later in this chapter, there are significant money laundering risks associated with the use of cryptocurrency ATMs.

The use of cryptocurrency ATMs has increased substantially in recent years. Sergeant Vickery testified that, at the time of the hearings, there had been a 100 percent

48 Evidence of A. Vickery, Transcript, November 23, 2020, p 68.
49 Ibid, p 70.
50 Ibid, pp 68–69.
51 Ibid, p 70.
52 Ibid, pp 69–70.
53 Exhibit 248, Appendix H, US Cryptocurrency Enforcement Framework, p 38.
54 Evidence of A. Vickery, Transcript, November 23, 2020, p 75.
55 Evidence of C. Cieslik, Transcript, November 25, 2020, pp 98–100.

increase in a year, from around 6,000 to 12,000 ATMs worldwide. Of approximately 1,000 such machines in Canada at the time of the hearings, 101 were in Vancouver.[56]

There are different ways to run a cryptocurrency ATM. An operator may have an open account with an exchange, such that transactions will be mirrored on an open account at an exchange. This arrangement ensures that the wallet used to support the ATM is fully replenished and will meet the supply and demand of the machine. It also helps with volatility, ensuring the operator of the machine is paying the same for cryptocurrency as it is being sold for. Alternatively, operators may purchase machines and support them with their own hot wallets – a practice requiring a lot of cryptocurrency reserves.[57]

As of June 2021, cryptocurrency ATMs are considered money services businesses under the *PCMLTFA* and are therefore subject to that regime's customer due diligence and other measures.[58] Sergeant Vickery testified that there is not much incentive for operators to do more than is required under the *PCMLTFA*, noting that operators have reported that business has dropped since implementing even basic customer due diligence measures.[59] She expressed the view that the vast majority of cryptocurrency ATMs will not be doing any form of customer due diligence under the required threshold of $1,000 (discussed below).[60]

Prepaid Cryptocurrency Cards

Although cryptocurrency is increasingly accepted by merchants as a form of payment, it is still relatively uncommon. This is due to the volatility of cryptocurrency: merchants cannot be sure of their purchasing power from one day to the next. Prepaid cryptocurrency cards offer a solution. These cards involve a user transferring cryptocurrency to a third-party operator that funds the cards, which can then be spent anywhere.[61] As I discuss below, these cards present money laundering risks.

Over-the-Counter Brokers

Over-the-counter (OTC) brokers facilitate trades between buyers and sellers who cannot or do not want to transact on an open cryptocurrency exchange. They are usually associated with – but operate independently from – exchanges.[62] This arrangement is sometimes referred to as being "nested" within an exchange and means that a transaction conducted by an OTC broker may show up on the blockchain as being conducted by the exchange.[63]

56 Evidence of A. Vickery, Transcript, November 23, 2020, pp 70, 75, 78; Exhibit 253, RCMP Virtual Assets Slideshow, slide 19.

57 Evidence of A. Vickery, Transcript, November 23, 2020, pp 71–72.

58 Evidence of C. Cieslik, Transcript, November 25, 2020, pp 100–1.

59 Transcript, November 23, 2020, pp 76–77.

60 Ibid, p 80.

61 Ibid, pp 80–81.

62 Exhibit 257, Chainalysis, *The 2020 State of Crypto Crime* (January 2020) [Chainalysis 2020 Report], p 12.

63 Exhibit 1021, Overview Report: Miscellaneous Documents, Appendix 1, Chainalysis, *The 2021 Crypto Crime Report* (February 16, 2021) [Chainalysis 2021 Report], p 13.

OTC brokers provide an avenue to exchange large amounts of cryptocurrency outside of an open exchange.[64] Large cryptocurrency transactions can have an impact on the liquidity of the market and pricing, with the result that there are usually limits set on how much cryptocurrency can be converted or transferred at a given time. OTC brokers are therefore attractive to those looking to move large amounts of cryptocurrency. They are generally seen as off-market service providers and provide increased privacy in that transactions are not directly connected to individuals on an exchange.[65]

An exchange's level of insight into the activities of a nested OTC broker varies. Further, customer due diligence practices among OTCs vary wildly, with some being very compliant and others not requiring any customer due diligence.[66]

Chainalysis, a company that provides blockchain forensics investigative services (discussed further below), observes in an annual report that there is a "huge range in how much illicit transaction volume nested services process – some are just as compliant as mainstream exchanges, while others appear to cater specifically to cybercriminals." It continues:

> Many appear to be large businesses for whom illicit activity is just a small share of total transaction volume, suggesting that these services are likely inadvertently moving illicit funds due to lax compliance policies, but could continue to operate if they stopped. However, some of these deposit addresses receive such a high percentage of their funds from illicit addresses that it seems impossible the activity could be accidental, or that the services could even continue to operate without serving cybercriminals.[67]

Chainalysis has identified 100 "rogue" OTCs that have processed trades with bad actors and wallets associated with large volumes of illicit cryptocurrency or proceeds of crime.[68] Jesse Spiro, global head of policy and regulatory affairs at Chainalysis, agreed that OTCs are disproportionately favoured by bad actors, including money launderers. In his estimation, this is likely because they either solicit that kind of business or have been identified as OTCs conducting little or no customer due diligence. Indeed, some OTCs are nested within exchanges that conduct little or no due diligence.[69]

There are clear money laundering vulnerabilities associated with OTC brokers. This is evident from their business model, which involves facilitating large cryptocurrency transactions for individuals without accounts at exchanges, and the absence of regulation over their activities. To borrow Sergeant Vickery's terminology, OTC brokers can be seen as "on ramps" or "off ramps" of virtual currencies, potentially allowing criminals

64 Evidence of A. Vickery, Transcript, November 23, 2020, p 82; Exhibit 253, RCMP Virtual Assets Slide-show, slide 23.

65 Evidence of J. Spiro, Transcript, November 24, 2020, pp 61–62, 85.

66 Ibid, pp 85–86.

67 Exhibit 1021, Appendix 1, Chainalysis 2021 Report, p 13.

68 Exhibit 257, Chainalysis 2020 Report, p 13; Evidence of J. Spiro, Transcript, November 24, 2020, p 87.

69 Evidence of J. Spiro, Transcript, November 24, 2020, pp 88–89.

to launder and cash out large amounts of cryptocurrency with little or no oversight.[70] However, I am mindful that there are legitimate uses of these services as well.[71]

It appears that OTC brokers may constitute dealers of virtual currencies for the purposes of the *PCMLTFA*. FINTRAC may wish to work in co-operation with exchanges to identify OTC brokers and, where appropriate, ensure that they are registered.

Private Off-Chain Transactions

Private off-chain transactions are another way of exchanging cryptocurrency. These are transactions that are not recorded on the blockchain. For example, an individual might give their private key to someone else in exchange for cash, thereby allowing the recipient of the key to access the cryptocurrency. In that way, the recipient has essentially received cryptocurrency without a formal transfer appearing on the blockchain.[72]

Lightning Network

A final way of exchanging cryptocurrency is through the lightning network. This network essentially runs like a tab: it enables users to perform multiple transactions outside the main blockchain and be recorded as a single transaction at the end.[73] Sergeant Vickery testified that, from a law enforcement perspective, the lightning network poses problems because it is not possible to see what occurred in the various transactions leading up to the final one that is recorded. In fact, it may not be possible to see that more than one transaction has occurred.[74]

Regulation of Cryptocurrencies

Regulation of cryptocurrencies is fairly recent both at the international and domestic level. In what follows, I review the Financial Action Task Force's recommendations[75] and guidance on virtual assets, the recent amendments to the *PCMLTFA,* and the potential for provincial regulation.

The Financial Action Task Force's Recommendations and Guidance

The Financial Action Task Force first addressed virtual assets in 2012 as a "new technology" in Recommendation 15. Over the years, the recommendation has become

70 Exhibit 257, Chainalysis 2020 Report, p 12.

71 Evidence of J. Spiro, Transcript, November 24, 2020, p 89; Exhibit 257, Chainalysis 2020 Report, p 12.

72 Evidence of A. Vickery, Transcript, November 23, 2020, pp 83–84; Exhibit 253, RCMP Virtual Assets Slide-show, slide 23.

73 Evidence of A. Vickery, Transcript, November 23, 2020, pp 84–85; Exhibit 253, RCMP Virtual Assets Slide-show, slide 23.

74 Transcript, November 23, 2020, pp 84–85.

75 I discuss the recommendations, which set out anti–money laundering and counterterrorist financing measures that member countries are encouraged to adopt, in Chapter 6.

more precise and new guidance has been made available.[76] Recommendation 15, "new technologies," currently states:

> Countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products. In the case of financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. They should take appropriate measures to manage and mitigate those risks.
>
> To manage and mitigate the risks emerging from virtual assets, countries should ensure that virtual asset service providers are regulated for [anti–money laundering / counterterrorist financing] purposes, and licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the [Financial Action Task Force] Recommendations.[77]

The recommendations also contain the following definitions of "virtual asset" and "virtual asset service provider":

> A virtual asset is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the [Financial Action Task Force] Recommendations.
>
> ...
>
> Virtual asset service provider means any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:
>
> i. exchange between virtual assets and fiat currencies;
>
> ii. exchange between one or more forms of virtual assets;
>
> iii. transfer of virtual assets;
>
> iv. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and

76 For a chronology of the evolution of the FATF standards and guidance, see Exhibit 249, Overview Report: Federal Regulation of Virtual Currencies, pp 1, 5–9.

77 Exhibit 4, Appendix E, *FATF Recommendations*, p 15.

v. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.[78]

The interpretive note to Recommendation 15 clarifies a number of points, of which I highlight a few. First, it notes that all value-based terms in the recommendations (namely "property," "proceeds," "funds," "funds or other assets," or other "corresponding value") should include virtual assets. As a result, all relevant measures under the recommendations should apply to virtual assets and virtual assets service providers.[79] Second, it states that virtual asset service providers should be required to be licensed or registered. Licensing or registration should be done at minimum in the jurisdiction in which the virtual asset service provider is created, but countries may also require virtual asset service providers that offer products and/or services to customers in, or conduct operations from, their jurisdiction to be licensed or registered in that jurisdiction.[80] Third, member jurisdictions must ensure that virtual asset service providers are supervised and regulated by a competent authority (which should not be a self-regulatory body) with recourse to a range of different disciplinary and financial sanctions.[81]

Virtual asset service providers should be subject to the same customer due diligence, record-keeping, and reporting requirements as other reporting entities, with two qualifications: (a) the threshold for requiring customer due diligence should be US$1,000 or 1,000 euros, and (b) virtual asset service providers should be required to gather originator and beneficiary information on virtual asset transfers, submit the information to the beneficiary provider or financial institution immediately and securely, and make it available on request to appropriate authorities.[82]

The latter qualification, referred to as the "travel rule," is based on Recommendation 16, which relates to wire transfers.[83] The travel rule is an anti–money laundering and counterterrorist financing measure that ensures originators and beneficiaries of financial transactions are identifiable and not anonymous.[84] It is meant to track and have a record of the movement of funds: who sends and receives them, which jurisdictions they are in, and which accounts are used.[85]

The Financial Action Task Force has also released a number of guidance documents, including its *Guidance for a Risk-Based Approach: Virtual Assets and Virtual*

78 Exhibit 4, Appendix E, *FATF Recommendations*, pp 126–27.

79 Exhibit 248, Overview Report: FATF Publications on Virtual Assets, Appendix D, Interpretive Note to FATF Recommendation 15, para 1.

80 Ibid, para 3.

81 Ibid, paras 5, 6.

82 Ibid, para 7.

83 Financial Action Task Force, *Updated Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers* (October 2021), online: https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf, para 178.

84 Exhibit 248, Overview Report: FATF Publications on Virtual Assets, Appendix F, FATF, *12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers* (June 2020), para 38.

85 Evidence of P. Warrack, Transcript, November 25, 2020, p 45–46.

Asset Service Providers, which was most recently updated in October 2021.[86] This lengthy guidance document explains how each of the 40 recommendations should be applied in the virtual asset space, provides examples of measures in place in certain jurisdictions, and sets out best practices in terms of information sharing and co-operation by supervisors.

In July 2020, the Financial Action Task Force published a 12-month review of members' implementation of the recommendations relating to virtual assets.[87] It found that 35 of 54 reporting jurisdictions had implemented the revised standards and emphasized the need for all members to implement the standards to ensure their effectiveness.[88] Jurisdictions were encountering issues in implementing the travel rule, with many noting that technological solutions were lacking.[89] The review provided some observations on the use of virtual assets for money laundering and terrorist financing purposes, including:

- The value of virtual assets involved in detected cases had been relatively small so far compared to cases using more traditional services and products, though ongoing monitoring is necessary.
- The most prominent typology observed so far has been the use of virtual assets for layering, possibly due to the ease of rapid transfer.
- Professional money laundering networks appeared to be starting to exploit this vulnerability and use virtual assets as a means of laundering.
- Bad actors tended to use virtual assets service providers registered or operating in jurisdictions lacking effective anti–money laundering or counterterrorist financing regulation, as well as multiple providers, rendering it challenging for authorities to follow the trail of funds.
- Bad actors tended to use tools and methods to increase the anonymity of transactions, including anonymizing domain names, tumblers or mixers, privacy coins, chain hopping, and other techniques (many of which I review below).[90]

The July 2020 review concluded that there was no clear need to amend the recommendations or the interpretive note as of yet. It committed to publishing a further

86 Financial Action Task Force, *Updated Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers* (October 2021), online: https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf.

87 Exhibit 248, Overview Report: FATF Publications on Virtual Assets, Appendix F, FATF, *12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers* (June 2020).

88 Ibid, paras 2–3.

89 Ibid, paras 2, 43.

90 Ibid, paras 16, 18.

review in July 2021,[91] which it subsequently did.[92] Among the second review's findings were the following:

- Fifty-eight of 128 jurisdictions had introduced the necessary legislation to implement the revised Financial Action Task Force standards, but global implementation is uneven.
- Although there had been clear progress in the implementation of the standards by the public sector, there was not yet sufficient implementation to enable a global anti–money laundering and counterterrorist financing regime for virtual assets and providers.
- As in 2020, there was not yet sufficient implementation of the travel rule or the development of associated technological solutions.
- There had been strong and rapid growth in the virtual assets sector since the revised standards, including a large increase in the use of virtual assets to collect ransomware payments and to launder proceeds.
- There was no need to amend the standards or interpretive note as of yet.[93]

In September 2020, the Financial Action Task Force released a series of "red flag indicators" associated with virtual assets.[94] These indicators were developed by examining over 100 case studies contributed by member jurisdictions between 2017 and 2021 as well as other Financial Action Task Force reports and information in the public domain.[95] The cases revealed that the majority of offences focused on predicate or money laundering offences, with the most common type of misuse being illicit trafficking in controlled substances and the second most common being frauds, scams, ransomware, and extortion.[96] The various indicators are divided into six categories: transactions, transaction patterns, anonymity, senders or recipients, source of funds or wealth, and geographical risks. Several case studies are included to illustrate the involvement of red flags. I would encourage law enforcement bodies in British Columbia tasked with investigating money laundering or cryptocurrency-related crime to carefully review these red flag indicators.

Notably, the Financial Action Task Force red flag indicators were significantly influenced by a private sector initiative. Peter Warrack, a consultant specializing in blockchain technology, anti–money laundering, and cryptocurrency, testified that the

91 Ibid, paras 4, 70.

92 Financial Action Task Force, *Second 12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers* (July 2021), online: https://www.fatf-gafi.org/media/fatf/documents/recommendations/Second-12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf.

93 Ibid at paras 2–7.

94 Exhibit 248, Overview Report: FATF Publications on Virtual Assets, Appendix G, *FATF Report: Virtual Assets: Red Flag Indicators of Money Laundering and Terrorist Financing* (September 2020).

95 Ibid, para 6.

96 Ibid, p 4.

Financial Action Task Force document was based on a report that he and peers in the industry (including exchanges, aftermarket software companies, and law enforcement) developed through an initiative called Project Participate (discussed below).[97] While I applaud this private sector initiative, I emphasize that law enforcement, regulators, and government must develop their own expertise in cryptocurrency.[98] The evidence before me showed that many private sector actors are committed to implementing measures to fight cryptocurrency-related crime, and this is certainly positive. However, the ultimate responsibility to investigate cryptocurrency-related crime, as with other criminal activity, lies with the state. It is crucial that law enforcement, government, and regulators – whose primary motivation is to act in the public interest – develop their own expertise in this area. Although private sector initiatives are to be welcomed, state actors must remain the primary investigators of this activity and ensure they are not overly dependent on private sector expertise and activity, given that law enforcement will likely need to investigate private sector actors in some cases. I recommend that the government, in consultation with the proposed AML Commissioner (see Chapter 8), ensure that law enforcement and regulators are trained to recognize indicators and typologies of money laundering through virtual assets. Prosecutors who are routinely tasked with advising on or supporting proceeds-of-crime and money laundering investigations may also benefit from such training. Members of the new anti–money laundering intelligence and investigation unit (discussed in Chapter 41), who will have or will need to develop a high degree of expertise in this area, would be well placed to develop and deliver such training.

Recommendation 86: I recommend that the Province, in consultation with the AML Commissioner and the dedicated provincial money laundering intelligence and investigation unit, ensure that law enforcement, regulators, and Crown counsel with relevant duties are trained to recognize indicators and typologies of money laundering through virtual assets.

The *PCMLTFA*

Amendments to the *PCMLTFA* to include virtual assets were introduced in June 2014. However, these and subsequent amendments needed to be brought into force

97 Transcript, November 25, 2020, pp 105–8.

98 In this regard, I agree with Detective Inspector Craig Hamilton of New Zealand's Financial Crime Group: "[Virtual assets are] an emerging area of opportunity for money laundering. It's also an emerging area of opportunity for regular career enhancement and policing response. It's here to stay. We need to understand it, and our people need to understand it. We need to be vigilantly looking for it. It's not something to be scared of or intimidated by. Quite the reverse. And it's an area that … law enforcement globally need to work together to respond to because the way it operates is that money can obviously transfer very, very quickly between people and certainly almost in other parts of the world, and it can finance illegal activity. And we need to be responsive to those issues": Transcript, May 12, 2021, p 62.

by regulation, which ultimately occurred in June 2020 and June 2021.[99] With these amendments, dealers in virtual currencies have been deemed to be money services businesses, and foreign money services businesses now include virtual currency dealers that do not have a place of business in Canada.[100] The *Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations*, SOR/2002-184, define "virtual currency" and "virtual currency exchange transaction" as follows:

> *virtual currency* means
>
> (a) a digital representation of value that can be used for payment or investment purposes, that is not a fiat currency and that can be readily exchanged for funds or for another virtual currency that can be readily exchanged for funds; or
>
> (b) a private key of a cryptographic system that enables a person or entity to have access to a digital representation of value referred to in paragraph (a). (*monnaie virtuelle*)
>
> *virtual currency exchange transaction* means an exchange, at the request of another person or entity, of virtual currency for funds, funds for virtual currency or one virtual currency for another. (*opération de change en monnaie virtuelle*)

Dealers in virtual currencies must now, among other things, do the following:

- register with FINTRAC;
- report various transactions to FINTRAC, including large cash and large virtual currency transactions and suspicious transactions;
- engage in client identification and verification measures in various circumstances, including:
  - when remitting $1,000 or more at the request of a customer;
  - conducting a foreign exchange transaction of $1,000 or more;
  - entering into an ongoing service agreement with a customer; and
  - conducting a large cash or large virtual currency transaction;
- take efforts to identify individuals who attempt to undertake a suspicious transaction; and
- implement compliance programs and policies.[101]

99 For a chronology of the amendments and regulations, see Exhibit 249, Overview Report: Federal Regulation of Virtual Currencies.

100 *PCMLTFA*, ss 5(h)(iv) and 5(h.1)(iv); *Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations*, SOR/2002-184 [*PCMLTF Regulations*], s 1, "money service business" and "foreign money service business."

101 *PCMLTFA*, ss 7, 11.1; *PCMLTF Regulations*, ss 30–37, 84, 85, 95, 156.

In line with the Financial Action Task Force's recommendations, the regulations also implement a travel rule:

> **124.1 (1)** A financial entity, money services business or foreign money services business that is required to keep a record under these Regulations in respect of a virtual currency transfer shall
>
> **(a)** include, with the transfer, the name, address and, if any, the account number or other reference number of both the person or entity who requested the transfer and the beneficiary; and
>
> **(b)** take reasonable measures to ensure that any transfer received includes the information referred to in paragraph (a).
>
> **(2)** Every person or entity referred to in subsection (1) shall develop and apply written risk-based policies and procedures for determining, in the case of a virtual currency transfer received by them that, despite reasonable measures taken under paragraph (1)(b), does not have included with it any of the information required under paragraph (1)(a), whether they should suspend or reject the virtual currency transfer and any follow-up measures to be taken.

The evidence before me revealed that there have been some difficulties in the implementation of the travel rule. Mr. Warrack testified that no single workable technological solution for the travel rule existed when the Financial Action Task Force formulated the corresponding recommendation. However, he noted that the industry has come together to establish technology solutions, common standards, and common language.[102] Ryan Mueller, chief compliance officer at the cryptocurrency platform Netcoin, added that there are many ways to move cryptocurrency, not all of which require customer due diligence measures, and that not all providers are willing to share information. Cryptocurrency exchanges have different ways of identifying the device initiating a transaction and of encrypting information, and "not all of those methods [can] talk to each other." Further, techniques exist to obfuscate the trail of funds.[103] Mr. Warrack added that the travel rule applies only between virtual asset service providers – it does not apply when a transaction is between a virtual asset service provider and a private wallet.[104]

The amendments have also placed obligations on other reporting entities. For example, all reporting entities that deal in virtual currencies (such as financial entities, casinos, securities dealers, and traditional money services businesses) must report large and suspicious transactions conducted in virtual currency.[105] Similarly, as part of their compliance programs, reporting entities must perform a risk assessment before using new technologies.[106]

102 Transcript, November 25, 2020, pp 46–47.

103 Transcript, November 25, 2020, pp 44–45.

104 Transcript, November 25, 2020, p 47.

105 Evidence of C. Cieslik, Transcript, November 25, 2020, pp 49–51.

106 *PCMLTF Regulations*, s 156(2).

In February 2022, in the context of the so-called "Freedom Convoy" protests in Ottawa, Windsor, and elsewhere in Canada, the federal government took swift and unprecedented action to expand the ambit of the *PCMLTFA* as it applies to virtual assets. On February 15, 2022, it invoked the *Emergencies Act*[107] for the first time and implemented various measures intended to target the blockades and their funding.[108] The measures were in force from February 15 to 23, 2022.[109] Significantly, some of the emergency measures related to virtual assets and reporting under the *PCMLTFA*: an emergency economic measures order required various financial entities to (a) cease dealing with property – including virtual assets – owned, held, or controlled by members of the Freedom Convoy, and (b) determine on a continuing basis whether they were in possession or control of such property.[110]

Notably, the financial entities targeted by the order were *not* limited to banks, credit unions, and other similar institutions; the order also extended to crowdfunding platforms that raise funds or virtual currency through donations.[111] Crowdfunding platforms were also required to register with FINTRAC and report suspicious and other transactions involving Freedom Convoy participants to FINTRAC.[112] It appears that the federal government intends to bring crowdfunding platforms into the *PCMLTFA* on a permanent basis.[113]

The amendments to the *PCMLTFA* that brought virtual assets into the regime were not in force at the time of the Financial Action Task Force's 2016 mutual evaluation of Canada.[114] The evaluation accordingly concluded that Canada was non-compliant with Recommendation 15, but noted that legislative steps had been taken to include virtual currencies in the regime.[115] In its recent re-rating of Canada, the Financial Action Task Force re-rated the country as largely compliant with Recommendation 15, given the amendments to the *PCMLTFA*.[116] The re-rating noted with approval the broad

107 RSC, 1985, c 22 (4th Supp).

108 Proclamation Declaring a Public Order Emergency, SOR/2022-20, *Canada Gazette*, Part II, Vol 156, No 1, Extra, February 15, 2022; Emergency Measures Regulations, SOR/2022-21, *Canada Gazette*, Part II, Vol 156, No 1, Extra, February 15, 2022; Emergency Economic Measures Order, SOR/2022-22, *Canada Gazette*, Part II, Vol 156, No 1, Extra, February 15, 2022.

109 Proclamation Revoking the Declaration of a Public Order Emergency, SOR/2022-26, *Canada Gazette*, Part II, Vol 156, No 2, Extra, February 23, 2022.

110 Emergency Economic Measures Order, SOR/2022-22, *Canada Gazette*, Part II, Vol 156, No 1, Extra, February 15, 2022, ss 2, 3.

111 Ibid, s 3(k), (l).

112 Ibid, ss 1, 4.

113 Melissa Tait, "Video: Trudeau Invokes Emergencies Act to End Convoy Blockades," *Globe and Mail*, February 14, 2022, 3:19, online: https://www.theglobeandmail.com/canada/video-trudeau-invokes-emergencies-act-to-end-convoy-blockades/; Rita Trichur, "Trucker blockades expose the weaknesses of Canada's anti-money-laundering regime," *Globe and Mail*, February 17, 2022, online: https://www.theglobeandmail.com/business/commentary/article-trucker-blockades-expose-the-weaknesses-of-canadas-anti-money/.

114 Exhibit 4, Overview Report: FATF, Appendix N: FATF, *Anti–Money Laundering and Counter-Terrorist Financing Measures – Canada, Fourth Round Mutual Evaluation Report* (Paris: FATF, 2016). See Chapter 6 for an explanation of the mutual evaluation regime.

115 Exhibit 4, Overview Report: FATF, Appendix N: FATF, *Anti–Money Laundering and Counter-Terrorist Financing Measures – Canada, Fourth Round Mutual Evaluation Report* (Paris: FATF, 2016), pp 77, 83, 150.

116 Exhibit 1061, FATF, *Anti–Money Laundering and Counter-Terrorist Financing Measures – Canada, 1st Regular Follow-up Report & Technical Compliance Re-Rating* (October 2021), p 5.

definitions of "virtual asset" and "virtual asset service providers," the requirement for the latter to register with FINTRAC and take preventive measures, and the steps taken by Canada to understand the money laundering and terrorist financing risks associated with virtual assets.[117]

In Mr. Warrack's view, deeming virtual asset service providers as money services businesses is not a perfect fit. He noted that a traditional money services business, such as one used to remit funds to another country, "is a very different model to the way that a lot of [virtual asset service providers] operate where in fact they are actually trading platforms with very, very different rules – a very, very different activity to what would be expected in a traditional [money services business]." He observed that rapid trading and rapid movement of funds might be very normal for a virtual asset service provider but a red flag in the traditional financial sector.[118] He also expressed the view that the requirement to report the receipt of virtual currency of more than $10,000 seems "somewhat ridiculous," as it would be "very normal for a customer who's a trader to have maybe thousands of transactions in an hour above that amount in and out of their account, particularly if they're using automated trading bots, et cetera"; nor does it take into account change transactions[119] or the fact that exchanges may value a cryptocurrency differently at any given time.[120]

Charlene Cieslik, a consultant on anti–money laundering and counterterrorist financing matters for financial and virtual currency businesses, testified that the $10,000 "magic number" was set around 30 years ago as a high amount but is not necessarily a good fit for cryptocurrency, given the price fluctuations. In her view, this threshold results in noise being reported to FINTRAC, and the number should be revisited.[121] Ms. Cieslik was also concerned that some virtual asset service providers and money service providers can allow various transactions under the $1,000 threshold for conducting client identification and verification to avoid doing those measures. In her view, some guidance on this matter is needed.[122] Conversely, Mr. Mueller noted that in some situations, such as with liquidity providers, every single transaction will meet the $1,000 threshold because they are servicing other high-volume entities.[123]

117 Ibid.

118 Transcript, November 25, 2020, pp 53–54.

119 Mr. Warrack explained a "change transaction" as follows. In the same way as an individual might pay for something worth $10 with a $20 bill and receive $10 in change, an individual may send 20 bitcoins worth $300,000 and want to send 10 bitcoins elsewhere. To do so, the individual would have to send the 20-bitcoin transaction through the blockchain and then receive 10 bitcoins in change. Mr. Warrack understands that the change transaction – the 10 bitcoins back – would trigger the $10,000 reporting rule, despite its being, in his view, "noise" being reported to FINTRAC that could obscure information that might actually lead to valuable information: Transcript, November 25, 2020, pp 54–57. Ms. Cieslik added that it would be helpful for FINTRAC to clarify whether change transactions need to be reported, as there is a wide discrepancy in industry practice: Transcript, November 25, 2020, p 57.

120 Transcript, November 25, 2020, pp 54–55.

121 Transcript, November 25, 2020, pp 57–58, 168–69.

122 Ibid, pp 63–65.

123 Transcript, November 25, 2020, p 167.

Sergeant Vickery testified that she would like to see FINTRAC be able to issue higher monetary penalties for non-compliance. She noted that the US Financial Crimes Enforcement Network (FinCEN) issued a US$250 million penalty for a former exchange called BTC-e, which was found to have facilitated money laundering. In her view, penalties such as these would be good deterrents.[124]

Having just come into force in June 2020 and June 2021, the *PCMLTFA* amendments are very new, and it is too soon to evaluate their effectiveness. Although the above concerns are well taken and could very well materialize, the amendments appear to be promising and long overdue. Nonetheless, criminals are adaptive and will certainly find ways around them.[125] It is therefore crucial that the federal government, FINTRAC, and industry members closely monitor the implementation of these new amendments as well as new trends and money laundering techniques that emerge.

Potential Provincial Regulation

The inclusion of virtual currencies in the *PCMLTFA* regime is a good first step for regulation in this industry. It does not, however, preclude complementary provincial regulation. As the *PCMLTFA* is focused on money laundering and terrorist financing risks, it does not address the internal activities of virtual asset service providers, consumer and investor protection, consumer fraud, or the regulation of third-party payment processors.[126]

In the next section, I review the rise and fall of QuadrigaCX (Quadriga), a Canadian cryptocurrency exchange that operated from December 2013 to February 2019. In a 2020 report, staff at the Ontario Securities Commission[127] concluded that Quadriga had committed various types of fraud. While Quadriga's story does not involve money laundering specifically, the circumstances leading to its downfall are illustrative of regulatory gaps in the virtual asset space and how lack of provincial regulation in this sector may facilitate criminal activity.

It seems likely that provincial regulation of virtual assets could have prevented many of the issues, including likely criminality, that arose in relation to Quadriga. In my view, the Province should regulate virtual asset service providers. The virtual asset space is developing quickly – as is cryptocurrency-related crime. It is essential that the Province put a regulatory regime in place promptly to address the risks that arise in this sector.

124 Transcript, November 23, 2020, p 157.

125 Ibid, pp 149–50; Evidence of A. Gilkes, Transcript, November 23, 2020, p 150.

126 Evidence of R. Mueller, Transcript, November 25, 2020, pp 65–66.

127 Exhibit 265 is a report prepared by Ontario Securities Commission staff. It notes that, in normal circumstances, there would likely have been an enforcement action before the Ontario Securities Commission itself against Mr. Cotten and/or Quadriga; however, this was not practical because Mr. Cotten was deceased and Quadriga was bankrupt. Instead, staff at the Ontario Securities Commission prepared a report summarizing their findings: Exhibit 265, Ontario Securities Commission, *QuadrigaCX: A Review by Staff of the Ontario Securities Commission* (April 14, 2020) [OSC Quadriga Report], p 4.

In Chapter 21, I have recommended that the Province regulate money services businesses and that this regulation be carried out by the British Columbia Financial Services Authority (BCFSA). Given that virtual asset service providers are deemed to be money services businesses for the purposes of the *PCMLTFA*, it may be that subjecting them to the same provincial regulation as money services businesses is appropriate. However, as I explain further below, securities regulators are developing guidance specifying when virtual asset service providers are engaged in activities that fall under their purview. It is not clear at this stage what proportion of virtual asset service providers engage in activities that would require them to register with a securities regulator. If many or most are engaged in such activity, there would seem to be a risk of duplication between a regulator of virtual asset service providers and regulation by the BC Securities Commission. It is also notable that Quebec – the only province that regulates money services businesses at the time of writing – has not included virtual asset service providers in its regime.[128]

Given the foregoing, I am not prepared to recommend that a particular body be responsible for regulation of virtual asset service providers. The Province is best placed to determine whether this regulation should be carried out by the BCFSA, the BC Securities Commission, or some other authority. In doing so, it should consult with the AML Commissioner, the BCFSA, the BC Securities Commission, industry members, and other stakeholders.

Recommendation 87: I recommend that the Province implement a regulatory regime for virtual asset service providers. In determining which authority is best placed to act as the regulator, the Province should consult with the AML Commissioner, the British Columbia Financial Services Authority, the British Columbia Securities Commission, industry members, and other stakeholders.

Quadriga

As I noted above, the circumstances of the rise and fall of Quadriga illustrate that an absence of regulation in the virtual asset field at the provincial level may allow criminal activity to occur undetected. Quadriga's story illustrates the pitfalls that can arise when an industry is able to operate free from meaningful scrutiny. I emphasize, however, that my discussion should not be taken as suggesting that all cryptocurrency-based entities are risky and non-compliant. To the contrary, the evidence before me indicates that many cryptocurrency exchanges seek to be compliant and had been long awaiting the amendments to the *PCMLTFA*.[129]

128 See Chapter 21 for a more detailed discussion of Quebec's regime. Under the *Money Services Businesses Act*, CQLR c E-12.000001, money services are defined to include currency exchange, funds transfer, the issue or redemption of traveller's cheques, money orders or bank drafts, cheque cashing, and the operation of automated teller machines: s 1.

129 Evidence of R. Mueller, Transcript, November 25, 2020, p 29; Evidence of C. Cieslik, Transcript, November 25, 2020, pp 22–23, 30–31; Evidence of P. Warrack, Transcript, November 25, 2020, pp 31–32.

Quadriga was a Canadian cryptocurrency exchange that operated from December 2013 to February 2019. Its downfall – which staff at the Ontario Securities Commission concluded was caused by fraud perpetrated by its co-founder and CEO, Gerald Cotten – led to over 76,000 clients being owed a combined $215 million in assets.

The Quadriga platform allowed users to store, buy, and sell various cryptocurrencies. Fuelled by rising cryptocurrency asset prices, Quadriga became the largest crypto-currency asset trading platform in Canada between 2016 and 2017.[130] Staff at the Ontario Securities Commission considered that its business model[131] meant that clients' entitlements constituted securities or derivatives; however, Quadriga did not register with any securities regulator.[132]

When the price of virtual assets began to fall in 2018, Quadriga became unable to meet client withdrawal requests. In January 2019, Quadriga announced that Mr. Cotten had died in India in December 2018. By February 2019, Quadriga had ceased operations and filed for creditor protection.[133]

Initial media reports said that Mr. Cotten had died without sharing the passwords to Quadriga's cold storage, which meant that client assets were inaccessible. However, the Ontario Securities Commission staff determined that this was not the case; rather, Mr. Cotten had been engaged in various forms of fraud, and, even before his death, Quadriga did not have enough assets to support its clients' holdings.[134] The report concludes that Mr. Cotten's fraud took many forms:

- Most of the shortfall (approximately $115 million) arose from fraudulent trading on the Quadriga platform. Mr. Cotten opened accounts under aliases and credited himself with fictitious currency and crypto-asset balances, which he traded with clients. He sustained real losses when the price of crypto assets fell, leading to a shortfall in assets to satisfy client withdrawals. He then covered clients' shortfalls with other clients' deposits – effectively, a Ponzi scheme.[135]
- He lost $28 million while trading client assets on three external crypto-asset trading platforms, without his clients' authorization or knowledge.[136]
- He misappropriated millions in client assets to fund his own lavish lifestyle. He transferred approximately $24 million of client funds to himself and his partner

130 Exhibit 246, Overview Report: Quadriga CX, p 1; Exhibit 265, OSC Quadriga Report, pp 10, 18.

131 The report notes that "this custody model – whereby Quadriga retained custody, control, and possession of its clients' crypto assets and only delivered assets to clients following a withdrawal request – meant that clients' entitlements to the crypto assets held by Quadriga constituted securities or derivatives": Exhibit 265, OSC Quadriga Report, p 11.

132 Exhibit 265, OSC Quadriga Report, p 11.

133 Ibid, pp 3, 20–22.

134 Exhibit 246, Overview Report: Quadriga CX, p 1; Exhibit 265, OSC Quadriga Report, p 3.

135 Exhibit 265, OSC Quadriga Report, pp 3, 15.

136 Ibid, p 3.

and bought a Tesla, a Lexus, a luxury yacht, a plane, a share in a private jet, and multiple properties.[137]

The Ontario Securities Commission staff and Ernst & Young (which was appointed monitor for the *Companies' Creditors Arrangement Act* proceedings) identified various problems with the way that Quadriga had handled its clients' assets, both virtual and fiat. These problems included:

- holding all client assets in a central Quadriga account rather than separate client accounts;[138]
- storing clients' assets primarily in hot wallets and other crypto-asset trading platforms, despite assuring clients that their assets would be stored in cold storage;[139]
- relying almost exclusively on third-party payment processors to hold clients' fiat assets, since banks refused to hold the funds;[140]
- doing millions of dollars of business in cash, despite Mr. Cotten knowing that such cash would surely not be accepted by banks;[141]
- failing to maintain boundaries between client assets and business administration assets;[142] and
- failing to maintain proper accounting ledgers or accounting records.[143]

The Ontario Securities Commission report determined that of the $215 million that Quadriga owed, $46 million was recovered – a collective loss of $169 million.[144] The RCMP and the FBI have confirmed that they have opened investigations into Quadriga.[145]

Access to Banking Services

The Quadriga case also illustrates the difficulty that some cryptocurrency exchanges have in securing banking services. Prior to the *PCMLTFA* amendments, these businesses were not covered by the regime and had no obligation to register with

137 Ibid, pp 3, 21; Exhibit 266, Ernst & Young, Fifth Monitor Report (June 19, 2019) [EY Monitor Report], para 10(f).

138 Exhibit 265, OSC Quadriga Report, p 12; Exhibit 266, EY Monitor Report, para 10(a).

139 Exhibit 265, OSC Quadriga Report, p 12; Exhibit 266, EY Monitor Report, para 10(f).

140 Exhibit 265, OSC Quadriga Report, p 13; Exhibit 266, EY Monitor Report, para 10(e).

141 Exhibit 265, OSC Quadriga Report, p 13; Exhibit 266, EY Monitor Report, para 10(c).

142 Exhibit 265, OSC Quadriga Report, p 14; Exhibit 266, EY Monitor Report, para 10(b).

143 Exhibit 265, OSC Quadriga Report, p 15.

144 Ibid, p 2. Of the $215 million owing, $115 million was due to Mr. Cotten's trading losses on the Quadriga platform; $28 million was lost by Mr. Cotten on other crypto-asset trading platforms; $2 million was misappropriated for himself; $1 million was attributed to Quadriga's operating losses; and $23 million was unaccounted for: ibid, pp 25–26.

145 Exhibit 246, Overview Report: Quadriga CX, p 3; Evidence of A. Vickery, Transcript, November 23, 2020, p 64.

FINTRAC or otherwise comply with the scheme. Further, some businesses obtained bank accounts through "less than transparent methods," with the result that "banks were not at all happy with people using their accounts for crypto-services when they found out and started closing all of their accounts."[146] Many financial institutions decided that the risk of dealing with virtual asset service providers was too high and declined to provide access to them.[147] This is known as "de-marketing" or "de-risking," and a similar issue has occurred with money services businesses (see Chapter 21). The lack of access to banking poses difficulties for virtual asset service providers, who lose access to "fiat on-ramp[s] and off-ramp[s]" and therefore have difficulty serving their clients, supporting their businesses, making payroll, and generally running their businesses.[148] To address the need for banking services, virtual asset service providers have turned to third-party service providers, including providers with less stringent concerns about regulatory status and some offshore financial institutions willing to provide banking services.[149] Indeed, Quadriga initially had access to banking services, but, over time, banks began to refuse to hold Quadriga-related funds. As a result, by 2017, Quadriga relied almost exclusively on third-party payment processors to hold its clients' fiat assets.[150]

Mr. Mueller testified that third-party service providers are a "grey area" when it comes to the *PCMLTFA*. Technically, businesses that remit funds need to register as money services businesses; however, there is "no clear designation" that payment processors constitute money services businesses.[151] As a result, use of these processors creates a "black box" from FINTRAC's perspective because engaging a third-party service provider – rather than a bank with reporting obligations – means that transactions may not be reported.[152] Further, from a law enforcement perspective, the use of third-party service providers tends to further distance the funds from the source, which can in turn facilitate money laundering.[153]

With the introduction of the *PCMLTFA* amendments and the requirement for cryptocurrency exchanges to register with FINTRAC, it appears that access to banking services for virtual asset service providers has been improving.[154] The AML Commissioner recommended in Chapter 8 would be well placed to monitor developments in this area, including whether access to banking services is improving and whether continued reliance on third-party service providers is problematic from an anti–money laundering perspective. The Commissioner should report on these matters to the Province and make recommendations as needed.

146 Evidence of C. Cieslik, Transcript, November 25, 2020, pp 88–89.

147 Ibid, pp 89–90.

148 Ibid, pp 90–91.

149 Ibid, pp 92–93.

150 Exhibit 265, OSC Quadriga Report, p 13.

151 Evidence of R. Mueller, Transcript, November 25, 2020, pp 94–95.

152 Ibid, p 95.

153 Evidence of A. Vickery, Transcript, November 23, 2020, p 60.

154 Evidence of C. Cieslik, Transcript, November 25, 2020, pp 90–91.

Availability of Auditing Services

Virtual asset service providers have had difficulties obtaining the kinds of auditing services available to "traditional" financial institutions. Giles Dixon, an anti–money laundering advisor to the financial services and virtual currency industries at Grant Thornton Canada, explained that traditional financial institutions obtain audits or reports on matters including the risks associated with their businesses and the efficacy of their financial and system controls. They can also obtain "public-facing" reports meant to assure the public of the efficacy of the financial and system controls.[155]

Some virtual asset service providers in the United States have begun to seek such reports.[156] However, in Canada, it has been difficult to identify auditors with the skills and capabilities required to conduct audits involving virtual assets, and there has been a lack of guidance from central bodies about how audit standards apply in this context.[157] Further, as virtual asset service providers are focused on getting their businesses "up and running," they do not necessarily have all the controls in place that an auditor would be assessing, and the cost of obtaining audits can be high.[158]

Regulation of Virtual Asset Service Providers by Securities Regulators

As noted above, staff at the Ontario Securities Commission considered that Quadriga's business model meant that it was engaging in securities or derivatives activities requiring it to register with a securities regulator. Indeed, the Canadian Securities Administrators (the umbrella organization of Canada's provincial and territorial securities regulators) has issued guidance on virtual asset services and when registration with a securities regulator will be necessary.[159] This guidance has explained when "initial coin offerings" and "initial token offerings" will constitute securities or derivatives,[160] as well as when platforms that facilitate buying and selling of crypto assets will be considered to fall under securities legislation.[161] The Canadian Securities Administrators and the Investment Industry Regulatory Organization of Canada have also prepared a joint consultation paper setting out a proposed regulatory framework for crypto-asset trading platforms.[162]

155 Transcript, November 25, 2020, pp 73–75.

156 Ibid, pp 75–79.

157 Evidence of C. Cieslik, Transcript, November 25, 2020, pp 79–81; Evidence of G. Dixon, Transcript, November 25, 2020, pp 81–82.

158 Evidence of G. Dixon, Transcript, November 25, 2020, pp 83–85.

159 See Exhibit 247, Overview Report: Canadian Securities Administrators Publications on Virtual Assets.

160 Exhibit 247, Appendix A, Canadian Securities Administrators, "CSA Staff Notice 46-307: Cryptocurrency Offerings" (August 24, 2017); Exhibit 247, Appendix B, Canadian Securities Administrators, "CSA Staff Notice 46-308: Securities Law Implications for Offerings of Tokens" (June 11, 2018).

161 Exhibit 247, Appendix C, Canadian Securities Administrators, "CSA Staff Notice 21-327: Guidance on the Application of Securities Legislation to Entities Facilitating the Trading of Crypto Assets" (January 16, 2020).

162 Exhibit 247, Appendix D, Canadian Securities Administrators and Investment Industry Regulatory Organization of Canada, "Joint Canadian Securities Administrators / Investment Industry Regulatory Organization of Canada Consultation Paper 21-402: Proposed Framework for Crypto-Asset Trading Platforms" (March 14, 2019).

As of the hearings in November 2020, there were representatives of at least two virtual asset service providers who were in the process of applying for status as securities dealers.[163] Mr. Mueller testified that obtaining this status can be beneficial for cryptocurrency exchanges that are seeking to show customers – particularly new customers – that they are established, stable, and abiding by regulations.[164]

It is encouraging that securities regulators are developing frameworks for virtual assets and providing guidance to businesses about when they will be subject to securities regulation. I expect that this work will continue, which will provide an additional layer of oversight over activities in the virtual asset space.

Cryptocurrency and Crime

The 2015 national risk assessment assessed virtual assets – particularly convertible, decentralized virtual currencies – as posing a high money laundering and terrorist financing risk. It noted that they are highly vulnerable due to their anonymity, ease of access, and complexity and that these characteristics pose significant challenges for law enforcement in determining the beneficial ownership of virtual currency involved in criminal activities.[165]

It is true that virtual assets pose money laundering risks and must be regulated accordingly. In what follows, I review some key areas of risk and ways in which the virtual asset space has been misused for money laundering and other criminal purposes. However, it is important to keep in mind that there are many legitimate users of cryptocurrency and that, by some estimates, the criminality associated with virtual assets appears to be a fairly low percentage. Regulation must strike a careful balance to take care not to stifle innovation in this area or penalize legitimate users, while also addressing key risks that arise.

How Much Crime Is Related to Cryptocurrencies?

It is difficult to ascertain with certainty how much crime involving cryptocurrencies is occurring. Sergeant Gilkes testified that it is more prevalent than most of us know, noting that many of the phone scams we regularly receive demand payment in cryptocurrencies. He added that many of these crimes go unreported or under-reported because people may be unsure whether they have fallen victim to them, may be ashamed that they have fallen victim, or may think they are encountering a technological issue rather than fraud.[166]

163 Evidence of R. Mueller, Transcript, November 25, 2020, p 85; Evidence of C. Cieslik, Transcript, November 25, 2020, p 86.

164 Evidence of R. Mueller, Transcript, November 25, 2020, pp 86–87.

165 Exhibit 3, Overview Report: Documents Created by Canada, Appendix B, Department of Finance, *Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada, 2015* (Ottawa: 2015), p 41.

166 Transcript, November 23, 2020, p 15.

Conversely, in its recent annual report on trends in the cryptocurrency universe, Chainalysis concludes that the number of cryptocurrency transactions involving illicit activity is low, at 2.1 percent of the transaction volume it analyzed from 2019 and 0.34 percent in 2020. Those low percentages do, however, translate into large numbers, totalling approximately US$2.4 billion and US$10 billion, respectively.[167] Chainalysis concludes that although the number may in fact be higher due to unreported criminal activity, the "good news is three-fold: Cryptocurrency-related crime is falling, it remains a small part of the overall cryptocurrency economy, and it is comparatively smaller than the amount of illicit funds involved in traditional finance."[168] Importantly, however, the Chainalysis report relies on transactions involving entities and would not capture, for example, peer-to-peer activity or other activity outside the "controlled ecosystem"; in other words, it does not purport to summarize the entire blockchain ledger.[169] Further, as noted above, companies such as Chainalysis do not have visibility into cryptocurrencies that do not have a public blockchain, including privacy coins.

The Chainalysis numbers do highlight that there is a large proportion of legitimate cryptocurrency activity. Its 2020 report notes that the use of cryptocurrency is increasing, with 18 percent of all Americans and 35 percent of American millennials purchasing it in one year. Further, mainstream financial institutions including JP Morgan Chase and popular retailers such as Amazon and Starbucks have made use of cryptocurrency.[170] Proponents of cryptocurrency also point to various advantages for legitimate users, including the potential to minimize transaction costs, avoid inflation in fiat currencies, grant access to individuals in the developing world who are not served by banks or other financial institutions, and provide increased privacy.[171]

Given the limitations on the Chainalysis data and the anecdotal nature of evidence suggesting that cryptocurrencies are regular features in some crimes and are increasingly prevalent in money laundering operations, I am unable to arrive at definitive conclusions on the precise magnitude of the problem. Nonetheless, the available information is sufficient to convince me that cryptocurrencies offer significant benefits to criminals, including those seeking to launder illicit funds, and that cryptocurrencies and those offering services associated with them present a significant money laundering risk. Indeed, as I discuss below, there have been several cases in which investigations have identified virtual assets being used to facilitate criminal activity, including money laundering. These cases are likely only the tip of the iceberg, given that there are obvious benefits virtual assets offer to criminals looking to launder illicit funds, that this area of economic activity and criminality is relatively new, and that law enforcement is still developing its knowledge and expertise in this area.

167 Exhibit 1021, Appendix 1, Chainalysis 2021 Report, pp 4–5.

168 Ibid.

169 Evidence of J. Spiro, Transcript, November 24, 2020, pp 12–13.

170 Exhibit 257, Chainalysis 2020 Report, p 5.

171 Exhibit 248, Appendix H, US Cryptocurrency Enforcement Framework, p 5.

I expect that cases will continue to come into public view as law enforcement, regulator, and government expertise in cryptocurrency continues to develop. I encourage government and law enforcement to monitor developments in the use of cryptocurrencies by the criminal element and be progressive in developing strategies to combat such use. The many benefits of cryptocurrency for criminals suggest that its use will only increase and that this is an area of significant money laundering vulnerability.

It is convenient to consider crime involving cryptocurrencies in four broad categories. First, and of most obvious importance to this Commission, is the use of cryptocurrency in money laundering. Second, cryptocurrency has been used to engage in financial transactions and activities associated with the commission of crimes such as scams, ransomware, and activities on the dark web. Third, cryptocurrency can be used to support terrorist activity. Finally, crimes occur on the cryptocurrency platform itself, such as theft or fraud. Although the last three categories do not squarely relate to money laundering, it is useful to review them as the categories tend to overlap.

Using Cryptocurrency for Money Laundering

Money laundering using cryptocurrency dates back at least to the early 2000s. In this section, I review some early cases before describing methods of money laundering using cryptocurrency and the advantages and disadvantages of doing so.

Early Cases

Sergeant Gilkes testified that identified criminality associated with virtual assets dates back at least to a virtual asset called E-gold. In 2003 or 2004, law enforcement determined that a group called Shadowcrew was engaged in laundering funds from stolen credit cards, identity theft, selling counterfeit identities, and other criminal activities through E-gold. Law enforcement arrested around 20 people involved in the scheme. Further, E-gold itself, which was based in the United States, was indicted in 2007 and had many bank accounts and assets seized.[172]

Some years later, a company called Liberty Reserve became what Sergeant Gilkes termed "version 2.0 of E-gold."[173] Liberty Reserve was an international online payment processor based in Costa Rica.[174] It had more than a million users worldwide and processed approximately 55 million transactions, almost all of which were illegal. It had its own virtual currency, Liberty Dollars, but at each end, transfers were denominated and stored in US dollars. Liberty Reserve required its users to make deposits and withdrawals through recommended third-party exchangers, which were typically unlicensed money-transmitting businesses operating in countries without significant money laundering oversight or regulation. As users

172 Evidence of A. Gilkes, Transcript, November 23, 2020, pp 99–100.

173 Ibid, p 100.

174 Exhibit 254, Senate Report, *Digital Currency: You Can't Flip This Coin!* (June 2015), p 41.

could not directly deposit or withdraw from their Liberty Reserve account, the company "evaded collecting information about them through banking transactions or other activity that would create a paper trail."[175] For an extra "privacy fee" of 75 cents per transaction, users could hide their Liberty Reserve account numbers when transferring funds, rendering the transfers completely untraceable.[176] As Sergeant Gilkes explained, Liberty Reserve's practices attempted to avoid pitfalls that had occurred with E-gold:

> Now, what we can see is a variation on a theme, right? So, I mean, rather than starting another virtual assets company within the United States, they started it overseas. Rather than dealing with actual fiat money and potentially being accused of money laundering, they were dealing simply with virtual currency, which didn't mean anything or had no actual intrinsic value to anyone. And by dealing with a broker, a middleman, then they could simply say that they had no involvement or had no way of knowing who was actually behind the funds that were actually being transacted.[177]

In May 2013, the US Department of Justice charged Liberty Reserve with operating an unregistered money transmitter and money laundering for facilitating the movement of more than US$6 billion in illicit proceeds. The Department of the Treasury identified Liberty Reserve as a financial institution of primary money laundering concern under the US *Patriot Act*, which effectively cut it off from the US financial system.[178]

Sergeant Gilkes explained that Bitcoin was very popular for those who lost money through E-gold and Liberty Reserve because it responded to two issues. First, it created a decentralized network, which meant that police could not simply go to one place and seize all the accounts belonging to clients. Second, it provided anonymity because, at the time, there were no tools or means to aid police in tracking people behind a transaction.[179]

Methods of Obfuscating the Source of Funds

Criminals have resorted to a number of techniques to obfuscate the source of funds in cryptocurrency transactions.

First, criminals seek out unregulated exchanges – those that operate in countries with little to no customer due diligence requirements or anti–money laundering regulation, or properly registered exchanges that operate under lax rules or flout anti–

175 Exhibit 248, Overview Report: FATF Publications on Virtual Currencies, Appendix A, *FATF Report: Virtual Currencies: Key Definitions and Potential AML/CFT Risks* (June 2014), p 10; Evidence of A. Gilkes, Transcript, November 23, 2020, p 101.

176 Exhibit 248, Overview Report: FATF Publications on Virtual Currencies, Appendix B, FATF, *Guidance for a Risk-Based Approach: Virtual Currencies* (June 2015), p 33.

177 Transcript, November 23, 2020, p 102.

178 Exhibit 248, Overview Report: FATF Publications on Virtual Currencies, Appendix B, FATF, *Guidance for a Risk-Based Approach: Virtual Currencies* (June 2015), p 10.

179 Transcript, November 23, 2020, pp 102–3.

money laundering protocols.[180] Chainalysis has observed that jurisdictions with lax regulation and low to no enforcement are particularly attractive for illicit activity.[181] The Financial Action Task Force has made similar observations.[182] Given that virtual assets remain a relatively new technology and that the Financial Action Task Force's recommendations on this subject are fairly recent, it is not surprising that some countries have experienced delays in implementing anti–money laundering measures. It is my hope that this loophole will become less pronounced as more countries implement robust anti–money laundering regimes relating to virtual assets.

In the meantime, there is unfortunately an effect on compliant Canadian exchanges. Ms. Cieslik testified that Canadian exchanges find it challenging that other exchanges can operate in countries with less regulation and still offer services to Canadians.[183] Mr. Dixon added that many exchanges are compliant and are seeking to understand what they can do proactively to better recognize risk. He has observed increased levels of co-operation between stakeholders in which they, for example, alert each other to hacks and potential thefts. Stakeholders have also participated in public-private initiatives such as Project Participate (discussed below).[184]

A second method of obfuscating the source of funds is through cryptocurrency ATMs. As I noted above, these are now considered money services businesses under the *PCMLTFA* and therefore have ensuing obligations. However, previously the standards of customer due diligence varied widely,[185] and there are examples of criminals exploiting loopholes. For example, in May 2019, a criminal organization was found to be importing drugs from a Colombian cartel, selling them in Spain, feeding the proceeds into two Bitcoin ATMs, and then instantly sending the money back to the cartel. The organization had created a fictitious money services business and fabricated its books to justify this influx of cash. They were caught by the Spanish police.[186] A similar situation arose in California when a man pled guilty in July 2020 for exchanging $25 million in cash through 17 cryptocurrency ATMs and creating a fictitious money services business to justify the proceeds.[187]

A third method of obfuscating the source of funds is through services known as "mixers" or "tumblers." These are third parties that, for a fee, mix cryptocurrency provided by a user with cryptocurrencies from other users before delivering it to its ultimate recipient. The result is that the cryptocurrency received by the recipient is not connected to the initial

180 Exhibit 253, RCMP Virtual Assets Slideshow, slide 47; Exhibit 248, Appendix H, US Cryptocurrency Enforcement Framework, pp 13–14.

181 Evidence of J. Spiro, November 24, 2020, pp 79–80.

182 Financial Action Task Force, *Second 12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers* (July 2021), para 26, online: https://www.fatf-gafi.org/media/fatf/documents/recommendations/Second-12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf.

183 Transcript, November 25, 2020, pp 116–18.

184 Transcript, November 25, 2020, pp 25–27.

185 Exhibit 253, RCMP Virtual Assets Slideshow, slide 49; Evidence of A. Vickery, Transcript, November 23, 2020, pp 77–80.

186 Evidence of A. Vickery, Transcript, November 23, 2020, pp 72–73.

187 Ibid, pp 73–74.

sender.[188] Mr. Spiro testified that FinCEN recently issued a penalty to a money services business that was providing mixing and tumbling services to customers it solicited off the darknet. The money services business was not conducting record keeping and, in fact, was specifically deleting user information. Nor was it filing suspicious transaction reports.[189] Mr. Spiro testified that there may be some legitimate users of tumblers and mixers who are concerned with privacy, but he expressed the view that most users are illegitimate.[190]

A fourth method of obfuscating the source of funds is through prepaid cryptocurrency cards. Sergeant Vickery testified that such cards are extremely vulnerable to money laundering: criminals can buy several of them online using a fake ID or straw buyer and then transfer the PIN or virtual card number to a bad actor. She noted that many of the websites ask for very little customer information. Similarly, gift cards bought with cryptocurrency are considered "closed loop" and therefore do not have any customer due diligence requirements.[191]

A fifth method is through online gaming websites. Cryptocurrency can be used to buy credit or virtual chips, which users can cash out after just a few transactions. When users cash out, they do not necessarily receive the same cryptocurrency back, which effectively cleans it.[192] Online gambling also allows for direct deposit from an ATM to the online account.[193]

A sixth method is through crowdsourcing or angel investor websites such as GoFundMe. Criminals may fund those websites with deposits from their own cryptocurrency addresses. Sergeant Vickery testified that a money laundering threat arises because there is no limit on how many addresses or wallets someone can hold, such that a money launderer could create a GoFundMe page and funnel transactions to it through various addresses. A bad actor may also commingle the transactions with legitimate ones. The result is a large reserve of cryptocurrency that is difficult for law enforcement to trace.[194] Further, as I discuss below, websites such as these have been used to fund terrorist activity.

Criminals may also conduct special kinds of transactions on the blockchain to obfuscate the source of funds. "Peel chains" involve conducting a number of transactions that are then consolidated.[195] Meanwhile, "chain hopping" involves moving

188 Exhibit 253, RCMP Virtual Assets Slideshow, slide 51; Evidence of J. Spiro, Transcript, November 24, 2020, p 54; Evidence of A. Vickery, Transcript, November 23, 2020, p 125; Exhibit 248, Appendix H, US Cryptocurrency Enforcement Framework, p 41. Mr. Spiro walked me through a diagram illustrating how mixers work: see Exhibit 257, Chainalysis 2020 Report, p 21; Evidence of J. Spiro, Transcript, November 24, 2020, pp 94–95.

189 Evidence of J. Spiro, Transcript, November 24, 2020, pp 97–99.

190 Ibid, p 99.

191 Evidence of A. Vickery, Transcript, November 23, 2020, pp 81–82.

192 Exhibit 253, RCMP Virtual Assets Slideshow, slide 47; Evidence of A. Vickery, Transcript, November 23, 2020, p 119.

193 Evidence of A. Gilkes, Transcript, November 23, 2020, p 119.

194 Evidence of A. Vickery, Transcript, November 23, 2020, pp 120–21.

195 Evidence of J. Spiro, Transcript, November 24, 2020, p 54. Mr. Spiro walked me through a diagram illustrating a peel chain, which shows several wallets being used by the same individual processing a number of different transactions, ending with a consolidation point: Exhibit 257, Chainalysis 2020 Report, p 22; Evidence of J. Spiro, Transcript, November 24, 2020, p 96.

one cryptocurrency to another, often in rapid succession. Converting cryptocurrency into another kind, and thus a different kind of blockchain, makes it difficult to trace the flow of funds, even using aftermarket software.[196]

Finally, Sergeant Vickery highlighted some particular practices that may be indicative of money laundering, which combine a number of the above techniques:

- depositing funds into an account from a cryptocurrency exchange, followed by rapid deletion via cash, email, or wire transfers;
- making several cash deposits into a cryptocurrency ATM and then immediately crediting them to a cryptocurrency exchange (a variation on smurfing);
- making frequent deposits or withdrawals from cryptocurrency exchanges;
- the presence of unusual third-party deposits from online wallets or payment processors; and
- prolonged meets in vehicles with smartphones, which, as noted above, may indicate that individuals are waiting for transactions to clear on the blockchain.[197]

As the above discussion demonstrates, criminals have already identified ways to launder money through cryptocurrency despite the industry being relatively new. While new federal regulation will help, it will not eliminate the risk. Law enforcement must stay on top of the evolving risks and money laundering methods involving cryptocurrencies. The rapid development of virtual assets technology and the uptake by criminals highlight the pressing need for law enforcement, government, and regulators to maintain expertise in this area and monitor developments in technology.

In Chapter 41, I recommend the creation of a dedicated provincial money laundering intelligence and investigation unit. As I expand in that chapter, the new unit should be staffed with individuals who have experience and expertise in virtual assets and the money laundering typologies that make use of them.

Advantages and Disadvantages of Using Cryptocurrency for Money Laundering

As my discussion this far has shown, cryptocurrency contains some obvious attractions to money launderers but also some pitfalls. Having reviewed various money laundering techniques using cryptocurrency, it is useful to tie together the various advantages and disadvantages identified thus far.

196 Exhibit 248, Appendix H, US Cryptocurrency Enforcement Framework, p 44; Exhibit 253, RCMP Virtual Assets Slideshow, slide 51; Evidence of J. Spiro, Transcript, November 24, 2020, pp 54, 97; Evidence of A. Vickery, Transcript, November 23, 2020, pp 124–25.

197 Exhibit 253, RCMP Virtual Assets Slideshow, slide 52; Evidence of A. Vickery, Transcript, November 23, 2020, pp 127–28.

Some advantages of using cryptocurrency for money laundering are:

- **fast transactions with minimal fees** (which are, on average, about $11 per transaction);
- **accessibility:** as noted above, the availability of cryptocurrency ATMs has rapidly increased;
- **easy conversion:** a bitcoin is a bitcoin anywhere in the world and can be converted into different fiat currencies;
- **ease of moving value globally:** cryptocurrency can be moved across borders instantaneously, in any amount, for minimal fees, which is in contrast to difficulties in moving large amounts of cash;
- **pseudo-anonymity:** although cryptocurrency is not as anonymous as cash, its pseudo-anonymous nature makes up for it, as transactions are very fast and information about the account holder is not immediately available to law enforcement;
- **lack of understanding by law enforcement:** there is a lack of understanding worldwide by law enforcement on what cryptocurrencies are, how to investigate crime involving them, and how to seize them; and
- **lack of global regulations:** although Canada now has regulations in place, many countries do not, and there is nothing to stop Canadians from using services operating in other countries.[198]

There are, however, disadvantages to laundering money through cryptocurrencies:

- **volatility of value:** as criminals cannot be sure of the purchasing power of cryptocurrencies, holding on to them for long periods may be a disadvantage if the value drops exponentially;
- **traceability:** criminals may realize that law enforcement can purchase aftermarket software tools and trace the flow of funds; and
- **lack of understanding by criminals:** although cryptocurrencies have been used by criminals, many may still not understand them.[199]

The transparency, visibility, and traceability of many virtual assets are unprecedented.[200] As I elaborate below, aftermarket software tools have been developed that have assisted law enforcement in their investigations.

198 Exhibit 253, RCMP Virtual Assets Slideshow, slide 27; Evidence of A. Vickery, Transcript, November 23, 2020, pp 95–97.

199 Exhibit 253, RCMP Virtual Assets Slideshow, slide 27; Evidence of A. Vickery, Transcript, November 23, 2020, pp 97–98; Evidence of J. Spiro, Transcript, November 24, 2020, pp 60–61.

200 Evidence of J. Spiro, Transcript, November 24, 2020, pp 62–63; Evidence of P. Warrack, Transcript, November 25, 2020, pp 24–25.

Using Cryptocurrency to Commit Other Crimes

In addition to money laundering, criminals use cryptocurrency to facilitate other crimes and avoid detection in ways that would be more difficult with fiat currency. Such crimes include, among others, scams, ransomware, distributed denial of service attacks, and money muling. It is useful to discuss these crimes as they can serve as predicate offences for money laundering, and there is often overlap between the predicate and money laundering offences.

In its 2021 report on crime, Chainalysis notes that scams are the highest-grossing form of cryptocurrency-based crime. In 2019, six Ponzi schemes took in nearly US$7 billion in cryptocurrency, and total scam revenue was roughly US$9 billion. In 2020, when there were no large-scale Ponzi schemes, the total revenue fell to US$2.7 billion. Chainalysis observes that scammers in 2020 primarily moved cryptocurrency received from victims to exchanges to convert it into cash, noting an increase in proceeds being sent to mixers and high-risk exchanges (being those with weak or non-existent compliance programs).[201] A report from the US Department of Justice notes that the FBI has noticed an increase in cryptocurrency fraud scams during the COVID-19 pandemic, with scammers threatening to infect victims and their families unless they sent payment via bitcoin or selling phony or defective products that would cure or prevent the disease.[202] Further, some phishing scams, such as emails or phone calls that purport to be from the Canada Revenue Agency (CRA), attempt to extort bitcoin from their victims.[203]

Another common crime involving cryptocurrency is ransomware, which is a type of malicious software that encrypts or blocks access to a victim's data. To regain access, the victim must pay a ransom, typically in bitcoin.[204] Chainalysis observed a significant increase in ransomware attacks in 2020, with the total amount paid by victims reaching nearly $350 million in cryptocurrency (a 311 percent increase from 2019). This large figure is likely lower than the amounts that were actually paid due to under-reporting.[205]

Cryptocurrency has also been used in distributed denial of service (known as "DDoS") attacks. These are a process of flooding a network with traffic so that websites hosted on it can no longer operate unless the victim pays an amount of bitcoin. Sergeant Gilkes explained that this disruption can be a big problem for certain websites, such as gambling websites, that can sustain considerable losses if shut down for even half an hour.[206]

201 Exhibit 1021, Appendix 1, Chainalysis 2021 Report, pp 71–74.

202 Exhibit 248, Appendix H, US Cryptocurrency Enforcement Framework, p 7.

203 Evidence of A. Gilkes, Transcript, November 23, 2020, pp 104–5; Exhibit 253, RCMP Virtual Assets Slideshow, slide 33.

204 Evidence of A. Gilkes, Transcript, November 23, 2020, pp 103–4; Exhibit 248, Appendix H, US Cryptocurrency Enforcement Framework, p 7.

205 Exhibit 1021, Appendix 1, Chainalysis 2021 Report, pp 6, 26; Exhibit 253, RCMP Virtual Assets Slideshow, slide 32.

206 Evidence of A. Gilkes, Transcript, November 23, 2020, p 105; Exhibit 253, RCMP Virtual Assets Slideshow, slide 34.

Criminals have also used cryptocurrency for money muling. Sergeant Gilkes gave the example of a cybercriminal who breaches an account, such as by stealing credentials, at a bank. The criminal then transfers the stolen funds to money mules, who are individuals recruited in various ways. The money mules buy cryptocurrency with the funds and transfer the cryptocurrency back to the cybercriminal.[207]

A significant amount of crime using cryptocurrency occurs on the dark web or darknet.[208] Between 50 and 70 percent of the websites hosted on the dark web are illegal. They include websites to buy drugs, child exploitation materials, weapons, counterfeit identification documents, unlawfully obtained personal information, and the like. However, there is also some legal activity, such as journalists trying to transmit messages without being intercepted.[209]

A number of darknet markets selling a variety of these illegal products and services exist. A well-known example was Silk Road, which was similar to eBay but with illicit products (including drugs, guns, and child exploitation material). Silk Road's payment system was novel. Buyers purchased bitcoin through an exchange or broker and sent the bitcoin to Silk Road. The latter would then hold the bitcoin in escrow until the product was delivered, at which point it would release the funds, minus a commission, to the vendor.[210] The FBI dismantled Silk Road in 2013. It was estimated to have generated sales revenue of over 9.5 million bitcoin (US$1.2 billion) and the operators collected over 600,000 bitcoin (US$80 million) in commission. In 2015, the creator was found guilty in the United States of seven charges, including money laundering, narcotics trafficking, and computer hacking.[211]

Another well-known darknet market was AlphaBay, which Sergeant Gilkes described as "Silk Road on steroids."[212] At the time of its takedown by law enforcement in 2017, it was the dark web's largest criminal marketplace, serving over 200,000 users and facilitating the sale of illegal drugs, firearms, malware, toxic chemicals, counterfeit identification documents, and more. It used a number of different kinds of virtual assets and had approximately 200,000 users, 40,000 vendors, and 250,000 listings, and facilitated more than US$1 billion in virtual asset transactions between 2015 and 2017. The administrator was arrested in 2017 in

207 Evidence of A. Gilkes, Transcript, November 23, 2020, pp 107–8. For a diagram of a money mule transaction, see Exhibit 253, RCMP Virtual Assets Slideshow, slide 36.

208 Sgt. Gilkes explained that there are three layers to the internet. First, the "surface web" contains the websites that most of us interact with, such as Wikipedia and Google. Second, most of the internet is in the "deep web," which contains information that we do not want indexed, such as medical records, and is usually accessed through portals that require credentials. Finally, the "dark web" is an alternate internet hosted on voluntary computers. It is encrypted, rendering it very difficult to trace traffic coming to, from, or through it: Transcript, November 23, 2020, pp 108–9.

209 Evidence of A. Gilkes, Transcript, November 23, 2020, pp 109–10, 167–68; Exhibit 248, Appendix H, US Cryptocurrency Enforcement Framework, p 6.

210 Evidence of A. Gilkes, Transcript, November 23, 2020, pp 110–11.

211 Exhibit 254, Senate Report, *Digital Currency: You Can't Flip This Coin!* (June 2015), p 41; Exhibit 248, Overview Report: FATF Publications on Virtual Assets, Appendix A, *FATF Report: Virtual Currencies: Key Definitions and Potential AML/CFT Risks* (June 2014), p 11.

212 Transcript, November 23, 2020, p 112.

Thailand and had 1,600 bitcoins seized (worth US$16 million at the time, around US$38 million today).[213]

A third and well-known example of illegal darknet activity is Welcome to Video, a child pornography website that was the world's largest online child sexual exploitation market at the time of its seizure. It offered child sexual exploitation photos and videos for sale using virtual currency. The alleged operator was arrested in the United States in October 2019, and at least 337 users have been arrested around the world.[214]

Finally, the Chainalysis 2021 report on crime indicates that alt-right groups and personalities involved in the January 2021 US Capitol riot received cryptocurrency donations prior to the storming of the US Capitol Building. The largest recipient received 13.5 bitcoin, worth approximately US$250,000 at the time of the transfer. Other recipients included the anti-immigration organization VDARE and an alt-right streamer.[215] Similarly, the 2022 "Freedom Convoy" appears to have received a large amount of cryptocurrency funding.[216] On February 17, 2022, a proposed class action lawsuit obtained an order (referred to as a "Mareva injunction") that froze various cryptocurrency wallets connected with members of the convoy.[217]

Using Cryptocurrency to Support Terrorism

Terrorist groups have also begun to use cryptocurrency as a method of funding their activities. A high-profile case involved "SamSam" ransomware. A terrorist group extorted US$6 million from various hospitals, universities, and government institutions by installing the ransomware and demanded a ransom to be paid in bitcoin.[218] US law enforcement determined that the scammers had supplied the same two bitcoin addresses to the entities that were extorted; as a result, they were able to use aftermarket software tools to trace and identify the suspects. The two bitcoin addresses were the first ever to be added to the US Office of Foreign Assets Control list.[219] Sergeant Vickery testified that the SamSam case was a great success, except that

213 Ibid; Exhibit 248, Appendix H, US Cryptocurrency Enforcement Framework, p 47; Exhibit 248, Appendix G, *FATF Report: Virtual Assets: Red Flag Indicators of Money Laundering and Terrorist Financing* (September 2020), p 11.

214 Exhibit 248, Appendix H, US Cryptocurrency Enforcement Framework, p 9.

215 Exhibit 1021, Appendix 1, Chainalysis 2021 Report, pp 99–105.

216 Temur Durrani and James Bradshaw, "Crypto Enthusiasts Keep Funding Convoy Protests as Traditional Banks Take Action Against It," *Globe and Mail*, February 11, 2022, online: https://www.theglobeandmail.com/business/article-crypto-enthusiasts-keep-funding-convoy-protests-as-traditional-banks/.

217 Mareva Injunction, Ontario Superior Court of Justice, Court File No CV-22-00088514-00CP, February 17, 2022; Priscilla Ki Sun Hwang, " Court Extends Rare Order to Freeze Up to $20M in Crypto, Cash Donations to 'Freedom Convoy,'" February 28, 2022, online: https://www.cbc.ca/news/canada/ottawa/mareva-injunction-order-extended-freedom-convoy-crypto-financial-donations-frozen-1.6366975.

218 Exhibit 253, RCMP Virtual Assets Slideshow, slide 50; Exhibit 248, Appendix H, US Cryptocurrency Enforcement Framework, p 8.

219 Evidence of A. Vickery, Transcript, November 23, 2020, pp 122–23.

it alerted the criminal element that law enforcement can trace transactions and that they would be caught if they used the same bitcoin address every time.[220]

Indeed, a case involving the al-Qassam Brigades sought to avoid the pitfalls in the SamSam case. The group posted requests for bitcoin donations on its social media page and official websites, claiming that the donations would be untraceable and used to support violent causes. However, unlike SamSam, the donation process involved creating a link that would generate a new bitcoin address for every donation.[221] The group then used a mainstream cryptocurrency exchange, cryptocurrency merchant services provider, and two unlicensed money services businesses to convert the cryptocurrency into cash.[222] Despite these measures, US law enforcement tracked and sought forfeiture of 150 cryptocurrency accounts used to launder funds to and from the al-Qassam Brigades' account.[223]

Al-Qaeda and ISIS have also engaged in criminal activities using cryptocurrency. Al-Qaeda has conducted social media campaigns to solicit donations that claim to be for charities but in fact solicit funds for terrorist attacks. US law enforcement identified and sought forfeiture of 155 virtual currency assets linked to the group.[224] Similarly, US law enforcement determined that individuals associated with ISIS marketed fake personal protective equipment such as N95 respirator masks to customers around the world during the COVID-19 pandemic.[225]

Crime Within the Cryptocurrency Space

A final type of crime associated with virtual assets is that occurring in the cryptocurrency space itself. This includes theft that occurs when criminals exploit vulnerabilities in wallets and exchanges. The Chainalysis 2021 report on crime indicates that cryptocurrency worth over US$520 million was stolen from services and individuals through hacks and other attacks in 2020.[226]

Another form of crime in the cryptocurrency space is cryptojacking. This occurs when a criminal makes unauthorized use of someone else's computer to generate or mine cryptocurrency. This can be done through the use of malware or compromised websites that cause the victim's computer to run crypto-mining code.[227]

220 Ibid, p 123.

221 Exhibit 248, Appendix H, US Cryptocurrency Enforcement Framework, p 11; Evidence of A. Vickery, Transcript, November 23, 2020, p 123.

222 Exhibit 1021, Appendix 1, Chainalysis 2021 Report, p 96.

223 Exhibit 248, Appendix H, US Cryptocurrency Enforcement Framework, p 11.

224 Evidence of A. Vickery, Transcript, November 23, 2020, p 124; Exhibit 248, Appendix H, US Cryptocurrency Enforcement Framework, p 11.

225 Exhibit 248, Appendix H, US Cryptocurrency Enforcement Framework, p 11.

226 Exhibit 1021, Appendix 1, Chainalysis 2021 Report, p 82; Exhibit 248, Appendix H, US Cryptocurrency Enforcement Framework, p 15.

227 Exhibit 248, Appendix H, US Cryptocurrency Enforcement Framework, p 16.

Finally, fraud can occur in the cryptocurrency space. The events leading to Quadriga's downfall (discussed above) illustrate how fraud can take place in the cryptocurrency space. Indeed, as the staff at the Ontario Securities Commission put it, Quadriga is an example of "an old-fashioned fraud wrapped in modern technology."[228]

Investigating Cryptocurrency-Related Crime

The evidence before me revealed that law enforcement in Canada has begun to identify the risks with cryptocurrency and investigate cryptocurrency-related crime. It was clear to me that Sergeants Vickery, Gilkes, and Warren Krahenbil (RCMP Federal Cybercrime Operations Group team leader) understood the risks, have developed some expertise in relation to virtual currencies, and have made good use of aftermarket software tools to aid in their investigations. It is less clear whether other units have developed the same expertise and abilities. I have recommended above that the Province and the AML Commissioner ensure that training is accessible for all law enforcement units, which will be crucial to ensure that this new area of criminality is investigated and prosecuted effectively in this province. It will also be important for the new provincial anti–money laundering unit to have particular expertise in this area. I also encourage law enforcement, regulators, and government to continue exploring innovative ways to investigate crime relating to virtual assets.

Law Enforcement's Ability to Investigate Cryptocurrency-Related Crime in Canada

Sergeant Vickery testified that a notable file in May 2018 provided an impetus for the RCMP to significantly ameliorate its capacity to handle cryptocurrency-related investigations. That file involved a prolific darknet vendor that was selling fentanyl. The RCMP's Milton detachment, despite most of its members only recently learning what Bitcoin was, became aware of cryptocurrency to be seized and contacted the digital forensics unit to re-create the wallet and facilitate the seizure. The case resulted in a conviction and around 22 seized bitcoins with a value of approximately $200,000 successfully forfeited as offence-related property.[229]

Sergeant Vickery testified that, although the investigation was a success, it made clear to the RCMP that, from a national headquarters level, it was deficient at the time in its ability to handle these investigations and support its members. It became clear that they needed policies, guidelines, and training to be put in place. The RCMP named Sergeant Vickery as the national cryptocurrency coordinator to put these in place and ensure that they could meet operational demands and support officers.[230]

The RCMP has since developed guidelines that direct members on how to conduct these investigations and how to seize virtual currencies. It also offers

228 Exhibit 265, OSC Quadriga Report, p 4.

229 Evidence of A. Vickery, Transcript, November 23, 2020, p 136.

230 Ibid, pp 136–37.

national financial crime courses on topics such as proceeds of crime, counterfeiting, financial integrity, terrorist financing, cybercrime, and online undercover activities. The RCMP has also organized one-day workshops and are putting together an online cryptocurrency 101 course that will be available to all RCMP members and, hopefully, to municipal and provincial law enforcement through the Canadian Police Knowledge Network.[231] The RCMP also created a virtual currency working group in 2017 in response to several initiatives across different divisions that were encountering cryptocurrency in their investigations.[232]

The RCMP also works with other government agencies. For example, the Canadian Anti-Fraud Centre is the "first point of contact" for RCMP members in cases involving frauds facilitated by cryptocurrency. The RCMP also has partnerships with the CRA, the federal Department of Finance, FINTRAC, and the Forensic Accounting Management Group.[233] Further, the RCMP has international partnerships through the Five Eyes Cryptocurrency Readiness Group, which discusses best practices and trade craft as well as strategies to build capacity internally and how to leverage it.[234]

The Seized Property Management Directorate is a government entity designed to manage seized offence-related property and proceeds of crime. It manages the seized property until it is either ordered returned upon no conviction or forfeited. Although the directorate's services were previously limited to federally prosecuted crimes, a June 2019 amendment now allows it to be used for all seized assets, including cryptocurrency, and by municipal and provincial police forces as well. Sergeant Vickery testified that the directorate has been a strong partner of the RCMP for 25 years and that its services save government money because it has contracts across the country allowing for storage of seized assets for a limited fee.[235]

A new unit in the RCMP "E" Division, the Federal Cybercrime Operations Group, was created in April 2020 and has a mandate to investigate cybercrime in accordance with federal policing strategic priorities. The unit currently has three members and an analyst, with plans to expand the unit.[236]

Finally, a notable public-private partnership called Project Participate[237] warrants discussion. A working group made up of virtual asset service providers, Project Participate focuses on increasing compliance and implementation of anti–money

231 Ibid, pp 137–38.

232 Ibid, pp 138–39.

233 Ibid, pp 140–41.

234 Ibid, p 141.

235 Ibid, pp 143–44, 147–48.

236 Evidence of W. Krahenbil, Transcript, November 23, 2020, pp 145–46; Closing submissions, Government of Canada, para 59.

237 A similar working group focused on anti–human trafficking efforts called Project Protect was created in 2016 by Mr. Warrack. The working group came together to share best practices, indicators of suspicion, and the like, with the result that a massive number of suspicious transaction reports and disclosures to law enforcement were made: Evidence of P. Warrack, Transcript, November 25, 2020, pp 112–13.

laundering and customer due diligence measures within the exchanges. The RCMP has a representative in the working group. Sergeant Vickery testified that the working group has helped law enforcement to identify virtual assets and targets of transactions. For example, it produced a list of information that virtual asset service providers regularly capture through their normal business activity and provided it to law enforcement as a starting point or template for how to get information through production orders.[238]

The above demonstrates that the RCMP has taken steps to address the cryptocurrency threat. I am encouraged that there appears to be a desire to share tools and training with provincial and municipal police units. It remains to be seen whether the RCMP's new cybercrime unit from 2020 will be expanded and achieve success in investigating and prosecuting these offences. Although federal efforts are important and should continue, provincial law enforcement units – particularly the dedicated provincial money laundering intelligence and investigation unit – must also develop their own expertise in virtual assets, provide training to their members, and ensure that they have access to the tools needed to effectively investigate this form of crime. These tools include aftermarket software tools, to which I turn now.

Aftermarket Software Tools

Aftermarket software tools and open-source technology allow law enforcement to analyze transactions and obtain a history of the movement and flow of funds. Companies providing these services can analyze the blockchain, attribute, and cluster addresses together, and then link them to criminality, risky cryptocurrency addresses, exposure to the darknet, and mixing services. Specialized law enforcement officers are trained to use the software and analyze the information. In doing so, they may identify IP addresses or other data, enabling them to seek judicial authorization for information from exchanges or third-party service providers.[239]

The largest software companies used by Canadian law enforcement are Chainalysis and CipherTrace. The National Cybercrime Coordination Centre has acquired several licences to these services to support Canadian law enforcement at the municipal, provincial, and federal level.[240] Below I review services provided by Chainalysis in further detail.

While there are undoubtedly advantages to using these tools, Sergeant Gilkes emphasized that they are not an exact science:

> I would like to add that the tools are not an exact science. So we're thinking about heuristics here. So there is clustering, basically trying to attribute multiple transactions to the control of one or several individuals. There are

238 Transcript, November 23, 2020, pp 141–43.

239 Ibid, pp 45, 47–48.

240 Ibid, pp 48–49, 139–40.

> also some properties inherent in the blockchain which … aid in providing a location for where a transaction may have occurred. But a lot of, I would say – I don't want to call it guesswork because [these are] educated guesses. But [a lot is] based on information which is collected in the clearnet, the darknet … circle information, reports from police … journalistic reports, [which] will provide information that will help to attribute ownership or attribute usership of particular addresses. But, like I mentioned, [it is] not an exact science, and regular policework has to be done in collaboration.[241]

As I have emphasized throughout this chapter, although private sector initiatives and tools are certainly useful and to be encouraged, it is crucial that law enforcement develop its own expertise and capabilities and should be cautious about overreliance on private sector tools.

Chainalysis

Mr. Spiro and Ian Place, director of solutions architecture at Chainalysis, gave detailed evidence about the operation and uses of Chainalysis' services. In what follows, I describe a few of Chainalysis' services as an example of how aftermarket software tools work and can assist law enforcement.

Chainalysis provides several services to its clients, which include virtual asset service providers, governments, regulatory agencies, and domestic and international police.[242] It also has a professional services team of investigators specialized in cryptocurrency investigations that is available to assist clients with investigations. Mr. Spiro testified that this team is particularly helpful in complex cases or those requiring a quick turnaround (for example, if there is an urgent need to freeze funds) or limited resources.[243] Chainalysis also produces publications, which include:

- an annual cryptocrime report, which reviews blockchain data and information Chainalysis has collected to generate new insights to share with the community;
- geography reports, which identify and map out cryptocurrency-related activity around the world and identify trends;
- occasional case studies about a certain kind of illicit activity and how Chainalysis was able to investigate and generate information; and
- thought leadership about regulatory developments and how the regulation aligns with different products and services.[244]

241 Transcript, November 23, 2020, pp 46–47.

242 Evidence of J. Spiro, Transcript, November 24, 2020, pp 143, 149.

243 Ibid, pp 14–16.

244 Ibid, pp 8–9, 11–12. Two examples of annual cryptocrime reports that I have discussed already can be found in Exhibit 257, Chainalysis, *The 2020 State of Crypto Crime* (January 2020), and Exhibit 1021, Overview Report: Miscellaneous Documents, Appendix 1, Chainalysis, *The 2021 Crypto Crime Report* (February 16, 2021).

Mr. Place walked me through three services provided by Chainalysis: Know Your Transaction (KYT), Reactor, and Kryptos. I will discuss each in turn.

KYT is a transaction-monitoring tool that provides real-time alerts to identify potential risks and transaction histories.[245] It is predominantly used by virtual asset service providers for compliance purposes.[246] KYT shows when a client has "direct exposure" or "indirect exposure" to risks. The former refers to a risk connected to a direct counterparty to a transaction – that is, the entity receiving or sending funds. Meanwhile, indirect exposure refers to funds that go indirectly from the platform to intermediary addresses; KYT therefore identifies a potential change of ownership or intermediaries conducting a transaction.[247] Alerts can include things such as darknet market flags, which identify transactions into and out of darknet markets.[248]

Reactor is a graphing, mapping, and investigative tool used to follow the flow of funds visually and to perform enhanced due diligence.[249] It can be used to identify entities that control wallets and to discover related entities.[250] Reactor is predominantly used by law enforcement rather than private sector clients. It is currently only able to look at Bitcoin transactions, not other cryptocurrencies.[251] Mr. Place walked me through a real-world example in which a client received an alert that it had indirect exposure to a sanctioned entity. Reactor generated a graphic representation of the various entities that provided funding for the transaction. The way the transaction was structured suggested that the person who sent the funds to an intermediary was the same person who sent funds to the entity designated by the US Office of Foreign Assets Control. It also suggested that the person was using a personal unhosted wallet, which is a common obfuscation technique.[252]

Finally, Kryptos provides "market intelligence and specific information in relation to entities that are within the cryptocurrency ecosystem."[253] It allows users to see what kinds of services they are interacting with (e.g., whether a service is a hosted wallet, a mining pool, or an exchange) and whether services are engaged in risky or non-risky activities.[254] Users can flag particular businesses that they want to monitor. Each business has a profile that shows information such as a risk rating given by Chainalysis, the kind of fiat currencies used, the country of headquarters, legal names, place and

245 Evidence of I. Place, Transcript, November 24, 2020, pp 18–19; Evidence of J. Spiro, Transcript, November 24, 2020, p 8.

246 Evidence of I. Place, Transcript, November 24, 2020, p 39; Evidence of J. Spiro, Transcript, November 24, 2020, p 8.

247 Evidence of I. Place, Transcript, November 24, 2020, pp 28–31.

248 Evidence of J. Spiro, Transcript, November 24, 2020, pp 27–28.

249 Evidence of I. Place, November 24, 2020, p 19.

250 Evidence of J. Spiro, November 24, 2020, pp 129–30. Mr. Spiro explained that an "entity" might be a company, a kind of service, a darknet market, or an unidentified wallet. However, Chainalysis would never have any information pertaining to the identities or personal identifying information for owners of wallets: Transcript, November 24, 2020, pp 153–54.

251 Evidence of I. Place, Transcript, November 24, 2020, pp 39, 48–49.

252 Evidence of I. Place and of J. Spiro, Transcript, November 24, 2020, pp 41–48.

253 Evidence of J. Spiro, Transcript, November 24, 2020, p 8.

254 Evidence of I. Place, Transcript, November 24, 2020, pp 19, 22–23.

country of incorporation, assets traded or accepted on the platform, stable and privacy coins offered, trading pairs, and recent news.[255]

Aftermarket software tools can therefore assist law enforcement in being able to trace transactions on the blockchain and monitor entities. I expect that they will also be useful for virtual asset service providers in fulfilling their new obligations under the *PCMLTFA*. I encourage law enforcement in this province to remain current on available software and technology that might assist them in identifying and investigating the potential use of cryptocurrency in money laundering and to trace and seize such illicit funds.

Conclusion

Virtual assets are a relatively new technology whose functionality and uses have rapidly developed in a short amount of time. Just as this technology has developed swiftly, criminals have learned to exploit it. Law enforcement in this country has begun to develop capacity and expertise in this area, and specialized tools and services now exist to assist in tracing transactions that use cryptocurrency. The virtual asset space will undoubtedly continue to transform, and new methods of criminality will certainly emerge. It is crucial that government, law enforcement, and regulators stay current on the risks facing this sector.

It will be important for the AML Commissioner to keep a particular focus on money laundering techniques using virtual assets. The virtual asset space is a rapidly evolving sector, and its complexities mean that state actors whose work involves identifying crime in this space – including law enforcement and regulators – must receive regular updates and training on emerging and developing typologies in this space. It will be key for the AML Commissioner to monitor whether that training occurs and report to government on any additional measures that should be taken.

255 Ibid, pp 20–22.