Overview Report: Criminal Intelligence Service Canada National Criminal Intelligence Estimate on the Canadian Criminal Marketplace: Money Laundering and Fraud (2020)

A. Scope of Overview Report

1. This overview report is intended to introduce into evidence a 2020 report produced by the Criminal Intelligence Service Canada (the **"CISC"**) titled "National Criminal Intelligence Estimate on the Canadian Criminal Marketplace: Money Laundering and Fraud."

B. National Criminal Intelligence Estimate on the Canadian Criminal Marketplace: Money Laundering and Fraud (2020)

2. On June 9th, 2020, Commission counsel called a panel of witnesses consisting of Chief Superintendent Rob Gilchrist of the CISC and Inspector Leslie Stevens and Ryland Wellwood of the Criminal Intelligence Service British Columbia.

3. In the course of the evidence of that panel, Chief Superintendent Gilchrist referred to a national intelligence estimate on money laundering and fraud prepared by the CISC and indicated that a public version of this report would be forthcoming:

> …in May of 2020, we produced a national intelligence estimate on money laundering and fraud. It's a Protected B strategic assessment that provides an overview of the scope and magnitude of money laundering and important fraud criminal markets in Canada and the role that serious and organized crime plays within those criminal markets. That protected version report was shared with Canadian police, including through our provincial bureaus, and CISC is currently working on a public version of that report, anticipated to be released in the summer.

4. The public National Criminal Intelligence Estimate on the Canadian Criminal Marketplace: Money Laundering and Fraud was published on September 28, 2020. This report is attached as Appendix 'A' to this overview report.

Appendix A:

Canada, Criminal Intelligence Service Canada, *National Criminal Intelligence Estimate on the Canadian Criminal Marketplace: Money Laundering and Fraud 2020* (Ottawa: Criminal Intelligence Service Canada, 2020).

CRIMINAL INTELLIGENCE SERVICE CANADA

NATIONAL CRIMINAL INTELLIGENCE ESTIMATE ON THE CANADIAN CRIMINAL MARKETPLACE: MONEY LAUNDERING AND FRAUD

2020

PUBLICATION DATE: SEPTEMBER 28, 2020

FOREWORD FROM THE DIRECTOR GENERAL, CRIMINAL INTELLIGENCE SERVICE CANADA

I am pleased to present the *2020 National Criminal Intelligence Estimate on the Canadian Criminal Marketplace: Money Laundering and Fraud (NCIE)*. This strategic assessment provides an overview of the scope and magnitude of money laundering and important fraud markets in Canada and the role of serious and organized crime within these markets. It combines federal, provincial, and municipal law enforcement reporting, open source reporting, and intelligence from other domestic and international government agencies to explore existing and emerging threats to Canada.

While most intelligence produced by CISC is shared only with law enforcement agencies, CISC is increasingly releasing information to the public in order to raise awareness about the nature and extent of organized crime threats in Canada. This national perspective helps to ensure that law enforcement, government, and the general Canadian public have a consistent view of serious and organized crime, and contributes to building and maintaining the partnerships that are instrumental to our ability to combat this threat.

CISC works collaboratively with its provincial bureaus and with many federal, provincial, and municipal law enforcement agencies. These partnerships allow for the exchange of vital information without which our ability to assess and ultimately disrupt organized crime threats would be compromised. I would like to express my sincere appreciation to our partners for their valued contributions to this report.

Chief Superintendent Rob Gilchrist
Director General
Criminal Intelligence Service Canada

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Market Implications

Estimated extent of money laundered in Canada: *$45-$113 billion CAD*

Some professional money launderers launder *$100s of millions CAD per year*

Losses due to fraud reported to Canadian Anti-Fraud Centre (CAFC) in 2019: *$100 million CAD*

Victims of fraud include:

- ✓ Individuals (life savings)
- ✓ Government (revenue, social services, reputation)

Perception: "white collar" crime
Reality: capable & interconnected organized crime groups (OCGs), in Canada and abroad

Criminal Enablers

Placing legal ownership in corporations, trusts, partnerships, or nominees allows for the *concealment of true ownership* of assets

Legislation does not require mortgage brokers, private lenders, lawyers, and notaries (in Quebec) to report suspicious activities or large cash transactions to FINTRAC

Global Connectivity

- ✓ International online platforms to facilitate fraud and money laundering
- ✓ Technology gives near-instant access to victims all over the world

Data-Mining Sources

- ✓ Unsecured online platforms providing names, birthdates, addresses, and pictures
- ✓ Data breaches of government or financial institutions' systems
- ✓ Data brokers selling targeted contact lists
- ✓ Dark web to buy, sell, and trade financial information and fraud guides

Insulation via intermediaries, including private sector businesses, or lower-level OCGs and money mules

Enforcement Challenges

A need for increased law enforcement training, resources, and knowledge in relation to money laundering

Complexity of international trade agreements make trade-based money laundering (TBML) difficult to recognize

Anonymity via online systems complicates the identification of criminal bases and jurisdictional primacy

Combatting *multi-jurisdictional* activities require partnerships with domestic and international agencies

Money laundering and fraud are believed to be greatly *under-reported*

Money Laundering

Majority of OCGs seek to *disguise proceeds of crime*

176 OCGs assessed in 2019 involved in money laundering; actual number believed to be higher

76 percent of these OCGs are based in *Ontario, British Columbia, and Quebec*

50 percent maintain international links

- ✓ Top five countries: United States, Mexico, China, Colombia, and Australia
- ✓ Almost half of these groups are involved in the cocaine market

Trade-Based Laundering

Used to move *hundreds of millions of dollars* through Canada

Canadian *professional money launderers* (PMLs) are engaging in significant TBML activities for international clients

Trade payments from *unrelated third party import / export companies* in jurisdictions that are high-risk for money laundering represent a significant risk in suspected TBML schemes

Cryptocurrency

Commonly used as *payment for fraud and dark web* purchases, and mechanism for money laundering

Use of anonymizing services and tools to obscure transaction routing *has tripled* over the past year

Commonly-Reported Frauds

Government services schemes erode public confidence in government institutions

12 OCGs involved in *identity theft*

Spear phishing losses:
$21.4 million CAD +

Romance schemes losses:
$24 million CAD +

3200 *ransomware* attacks a day, averaging $1-3 million CAD per incident

Elder-targeted scheme losses:
$35 million CAD +

9 OCGs involved in *securities fraud*, in which one scheme can generate millions of dollars in losses

22 OCGs involved in *payment card fraud*, losses of which are greatly under-reported

8 OCGs involved in *real estate fraud*

INTRODUCTION

Background

The 2020 NCIE on Money Laundering and Fraud is produced by CISC Central Bureau, in collaboration with its network of ten Provincial Bureaus through the Integrated Threat Assessment (ITA) process, as well as contribution from member agencies and other federal and provincial partners. The NCIE is one of CISC's flagship products, recognizing the need for law enforcement decision-makers, government policy makers and the general Canadian public to receive specific strategic intelligence on the scope and magnitude of criminal markets in Canada.

Structure

The present NCIE is a comprehensive strategic assessment of the threat posed to Canada by domestic and international money laundering and fraud. The feature focus of the report addresses the increasing concerns relating to money laundering in Canada, and delves into significant contributors to the issue, including trade-based money laundering (TBML) and cryptocurrency. This report also includes other market assessments on fraud typologies that pose significant levels of threat to Canada, including mass-marketing, securities, payment card, and real estate frauds.

Money Laundering Implications

Money laundering enables criminals to convert proceeds from criminal activities into Canada's legal economy, obscuring the origin and avoiding the detection and confiscation of illegally obtained assets or funds. The United Nations Office of Drugs and Crime (UNODC) estimates that the amount of money laundered globally is between two and five percent of the global Gross Domestic Product (GDP). Using this formula and current Canadian data[1], the extent of money laundered in Canada is estimated to be between $45 billion and $113 billion CAD.

Professional money launderers (PMLs), also called money laundering service providers, are of particular concern, as they coordinate operations for organized crime groups (OCGs), individual criminals, and also themselves. PMLs sell their services to OCGs and other criminals, but are often not part of the criminal activities that generate the proceeds of crime that they launder. This permits them to remain insulated from the predicate offences, and makes it difficult for investigators and prosecutors to prove knowledge of the illicit origins of the funds. Some Canadian PMLs are estimated to launder $100s of millions CAD per year.

In addition to the use of such intermediaries, money laundering in Canada is enabled by its inherent clandestine nature, legislation that does not require fulsome transparency, and the complexity in investigating TBML schemes.

Fraud Market Implications

Canadians are losing millions of dollars to fraud every year. In 2019, nearly $100 million CAD in losses was reported to the Canadian Anti-Fraud Centre (CAFC). These financial damages are felt by individuals who sometimes lose their life savings, represent lost tax revenue for the government, and can lead to additional strain placed on government social services. Some fraudulent schemes also collect sensitive personal information in addition to money, which can be used to further other crimes, such as identity theft. Moreover, many victims undeservedly feel shame or embarrassment for having become victims of fraud, resulting in mental health, substance abuse, and social isolation issues, as well as deaths by suicide.

[1] Canada's GDP in 2018 is estimated at $1.7 trillion USD. Using an exchange rate of 1.33 CAD for 1 USD, Canada's GDP in 2018 is $2.26 trillion CAD.

Despite the many resources available to educate the public on financial schemes, victims often do not pause to consider whether they are being targeted for fraud, either due to pressure from criminal actors, social isolation, financial literacy, or over-confidence.

Financial crime, often seen as "white collar" crime, is committed by highly capable criminals and interconnected OCGs, both in Canada and abroad, with some Canadian OCGs directly involved in running boiler rooms (i.e. telemarketing centres used in fraud), and others simply collect a portion of profits. The lucrative financial returns produced by frauds are likely used to fund other criminal activity, primarily drug importation and trafficking.

Whereas some OCGs and other criminals continue to commit frauds in person, which presents a higher level of risk of detection and interception, many now exploit new technological resources and other enablers to commit their frauds. These trends present new and continually evolving challenges for law enforcement agencies to address and curtail.

CRIMINAL ENABLERS / LAW ENFORCEMENT CHALLENGES

This section addresses key enablers that relate to money laundering, TBML, and cryptocurrency, as well as those that are common to most fraud markets. Insomuch as the terms "criminal enabler" and "law enforcement challenge" are often interchangeable, depending on the perspective taken to assess them, both perspectives are included in this section.

Criminal Enablers: Money Laundering (including Trade-Based)

Clandestine Nature

The inherent clandestine nature of money laundering, and the fact that it often occurs separately from the predicate offences that generate the illicit funds, enable OCGs and other criminals to conduct money laundering schemes with low risk of detection from law enforcement.

Beneficial Ownership

Beneficial ownership is a term that represents the individual that ultimately controls or benefits from an asset or transaction. Criminals hide true ownership of assets from law enforcement and regulators to avoid suspicion and reduce the risk of seizure from authorities. A lack of beneficial ownership transparency facilitates the concealment of the true ownership of all forms of assets, including businesses, real estate, personal property, bank accounts, and investments, by placing legal ownership in corporations, trusts, partnerships, or nominees.

Currently, the federal government and several provincial governments are addressing beneficial ownership by implementing regulations regarding the transparency of ownership to prevent the use of corporations and partnerships for criminal purposes, including money laundering (see **Table 1**). These new requirements have the potential to improve law enforcement's ability to identify the true owners of assets in support of money laundering investigations.

Table 1 – New Regulations

Canadian Business Corporations Act
As of June 2019, all federally-incorporated corporations must maintain a register, accessible by law enforcement, tax authorities, and certain regulators, of individuals who have a significant control over a company.
At the provincial level, British Columbia, Saskatchewan, Manitoba, and Quebec have passed similar regulations related to provincially-incorporated corporations, which are at various stages of implementation.
BC's Land Owner Transparency Act (LOTA)
LOTA, which received royal assent in 2019, and has not yet come into force, will require the disclosure of all individual, corporate, and partnership structures that directly or indirectly have a beneficial interest in property in British Columbia, as well as the creation of a public, searchable registry of this information. British Columbia will be the first province to address beneficial ownership in real estate.

Gaps in PCMLTFA Reporting Obligations

Not all professionals involved in real estate transactions have obligations under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)*. As mortgage brokers, private lenders, lawyers, and notaries (in Quebec) are not subject to the *PCMLTFA*, they are not required to report suspicious activities or large cash transactions to FINTRAC. This creates an opportunity for the exploitation of these entities by criminals and complicit professionals for money laundering purposes and contributes to the opaqueness of their actions.

Law Enforcement Challenges: Money Laundering (including Trade-Based)

A Need for Increased Training and Resources

A need for increased training, resources, and knowledge are the challenges most often identified by the law enforcement community in relation to money laundering – gaps that will need to be bridged in order to ensure a more accurate picture of the threat and to develop a more targeted threat response.

Complexity of International Trade Agreements

As money laundering activities hide within the vast scope of Canada's legitimate economy and financial systems, law enforcement is challenged to not only detect the money laundering schemes but to link them to criminality.

TBML is difficult to recognize because of the complexity of international trade, the ease with which proceeds of crime can be co-mingled with legitimate funds, the lack of regulations or oversight for agreements between international companies, and the sheer volume of imports and exports that flow across the border. PMLs engaging in TBML may be involved in both the import and export elements of the transactions. TBML requires complicity on the part of both parties, but the schemes are simplified for launderers when they are able to control both the companies shipping (or claiming to ship) goods in one country, and the receiving entities in another jurisdiction.

Criminal Enablers: Fraud Markets

Global Connectivity

Global connectivity – via internet, smart devices, and social media platforms – has resulted in expanded criminal reach. Frauds are becoming evermore international in scope, and the use of technology to facilitate these crimes has resulted in near-instant access to victims all over the world.

Online platforms are boundless, and wireless and mobile technologies are constantly changing and updating, providing criminals with increasing opportunities to target users through their devices, with relative impunity. The ever-growing transition to the internet and digital technologies, and security weaknesses coupled with the increasing development of sophisticated attacks specifically designed to exploit those weaknesses, exposes individuals, institutions, and governments to greater cyber security threats.

Data-Mining Sources

There is an ever-increasing amount of personal and financial information easily accessible by criminals. In addition to traditional "dumpster diving" to retrieve hard-copy documents that have been improperly discarded (e.g. financial and medical records thrown out rather than shredded or incinerated), criminal actors can comb through various online platforms to gather sensitive information, including names, birthdates, addresses, and pictures. Data-mining facilitates criminal activities, such as phishing (whereby criminals communicate with individuals while purporting to be from reputable entities in order to induce the disclosure of personal information), extortion, and identity theft.

Targeted fraudulent marketing can be facilitated by the acquisition of contact information that can be obtained through data breaches of restricted systems (e.g. using malware to infiltrate government or financial institutions' holdings to access files), and via data brokers, which are businesses that take personal information from various sources (social media, magazines, charities, contests, loyalty programs, etc.), and sell specific data packages to other businesses for marketing purposes. Contact lists, tailored by various demographic criteria, such as age, location, and interests, can be acquired through such brokers.

The dark web marketplace is an increasingly attractive hub to anonymously buy, sell, and trade financial information and fraud guides. Cybersecurity firm Sixgill, in its *2019 Underground Financial Fraud Report*, indicates that data from over 23 million credit and debit cards were available on the dark web in the first half of 2019. The dark web also provides guides for amateur fraudsters looking to engage in financial crime; intelligence company Terbium Labs released a report in 2019 examining approximately 30,000 fraud guides on the dark web.

Insulation

Intermediaries, such as promotion companies, can be exploited for their vast network of contacts through email blasts, websites, forums, and mass-mailer subscriptions. Such methods provide a layer of insulation between criminals and their victims.

Another layer of insulation is provided by compartmentalizing fraudulent schemes (see **Figure 1**). Separate OCGs can carry out individual stages of schemes, thereby shielding higher-level threats from identification by law enforcement and rendering investigations more difficult. Funds are transferred via money service businesses (MSBs), and runners, or "money mules" are those that make contact with victims, if required. An example of the latter are individuals who are at times recruited through a "work at home" scheme, where they are told they are processing payments for a company, but in reality are creating a layer of insulation between the victim and the ultimate receiver of the funds. Schemes such as these often also require contact lists, a designer and printer for fake letters and cheques (for prize schemes), and a mail service provider. In some cases, the various service providers are not aware that they are involved in criminal activity.

Figure 1 – Example of Compartmentalization

Law Enforcement Challenges: Fraud Markets

Criminal Anonymity

Online technologies provide criminals with a virtual and anonymous platform, increasing difficultly for law enforcement to target fraudsters domestically and abroad. This cyber element complicates the identification of criminal bases of operations, and hence jurisdictional primacy, and limits the ways in which some investigations can be carried out.

Multi-Jurisdictional Nature of Schemes

Fraudulent schemes are increasingly multi-jurisdictional and international in nature. Consequently, investigations are resource-intensive and complex, and often require partnership with domestic and international law enforcement agencies. The latter can prove challenging when dealing with agencies in some countries that may be less cooperative.

Limited Reporting

Fraud is believed to be greatly under-reported across all scheme types. Many individuals are suspected of declining to report due to feelings of shame or embarrassment from having been defrauded, some fear reprisals, and some are unaware of the venues through which to report the frauds.

There are no comprehensive statistics across Canada, as victims who do report frauds submit them to various agencies, including the CAFC[2], provincial securities commissions, banks, civil courts, and various police agencies. Moreover, third-party companies are often reluctant to share information on frauds for fear of reputational and clientele loss.

Without comprehensive statistics regarding the number of complaints, victims, and costs, the full impact of frauds on Canadian society is challenging to assess, as is the degree to which the threat of different fraud typologies is evolving.

[2] Nevertheless, despite the lack of unified reporting, CAFC data provide the most inclusive snapshot available of what is occurring in Canada.

MONEY LAUNDERING

Key Highlights

- The majority of OCGs and other criminals seek to disguise their proceeds of crime. Though 176 OCGs assessed in 2019 were reported to be involved in money laundering activities, the actual number of groups involved is believed to be higher.
- Approximately 50 percent of the 176 Canadian OCGs involved with money laundering maintain international links, with the top five countries being the United States, Mexico, China, Colombia, and Australia. Almost half of the groups with international links are involved in the cocaine market.
- The highest reported number of groups involved in money laundering activities are in Ontario, followed by British Columbia and Quebec, with all three provinces collectively representing more than 76 percent of the groups identified nationally as being involved in money laundering.
- Over the past two years, the federal government and a number of provincial counterparts have implemented legislative changes to strengthen anti-money laundering regimes, including updates to beneficial ownership record requirements and an amendment to the *Criminal Code* offence of money laundering to improve prosecution. Despite the revisions, other regulatory issues remain that challenge Canadian responses to money laundering issues.

Introduction

In its most recent evaluation of Canada, the Financial Action Task Force stated in 2016 that though Canada had a strong anti-money laundering regime in general, elements in its legal framework and implementation were missing. The report further stated that law enforcement results were not commensurate with the money laundering risk in the country. In November 2018, as part of its review of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, the House of Commons Standing Committee on Finance heard from witnesses who stated that terms such as "snow washing" and the "Vancouver model" of money laundering were associated to Canada, causing damage to its anti-money laundering reputation.

The Financial Transactions and Reports Analysis Centre of Canada's (FINTRAC) 2018-19 *Annual Report* provided more than 2200 disclosures to law enforcement across Canada and some foreign financial intelligence units. Over 70 percent of the disclosures were related to suspected money laundering activities, with the top three associated predicate offences reported as fraud (32 percent), drugs (30 percent), and tax evasion (11 percent).

Agencies and institutions globally describe a three-step process for money laundering that involves placement, layering, and integration. Depending on the complexity of the scheme, not all three steps may be required to successfully launder proceeds of crime. Using FINTRAC's model, the first step is the placement of proceeds of crime into the financial system. The second step involves the further hiding or disguising of proceeds of crime by adding financial transactions to make it difficult to audit the trail, source, or ownership of the illegal funds. The final step involves the moving of laundered proceeds of crime back into the economy through legitimate means. **Figure 2** on the next page depicts the three steps of ML.

Market Analysis

Members of OCGs and other criminals engage in money laundering, from the most basic levels to more complex schemes that layer and disguise the source of funds. They use illicit funds to pay for real estate, purchase luxury goods, such as vehicles, and use private sector businesses to disguise the true source of their proceeds of crime. For OCGs that generate limited profits that are masked through such basic laundering, schemes that are more complicated are not necessary. In contrast, OCGs that generate significant wealth through their criminal endeavours often use sophisticated methods, as well as the more straightforward techniques, to legitimize their illegally-gained profits.

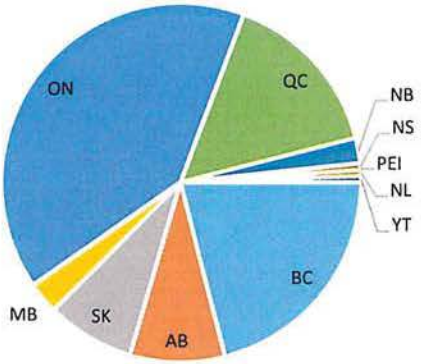
Figure 2 –FINTRAC's Three Stages of the Money Laundering Process

Criminal Involvement and Domestic Scope

Over a five-year period (2015-2019), an average of 25 percent of OCGs were reported to be involved in money laundering activities in Canada. Currently, 176 of the 680[3] assessed OCGs are identified as being involved in money laundering. Given that the majority of crime groups and criminals with illegally obtained funds seek to disguise their proceeds of crime, the actual number of groups participating in money laundering activities is believed to be greater than reported.

The highest reported number of groups involved in this activity are in Ontario, followed by British Columbia and Quebec, with all three collectively representing more than 76 percent of the groups identified nationally as being involved in money laundering. **Figure 3** provides a proportional overview of OCGs involved in money laundering, by province.

Figure 3 – Proportion of OCGs Involved in Money Laundering in 2019, by Province

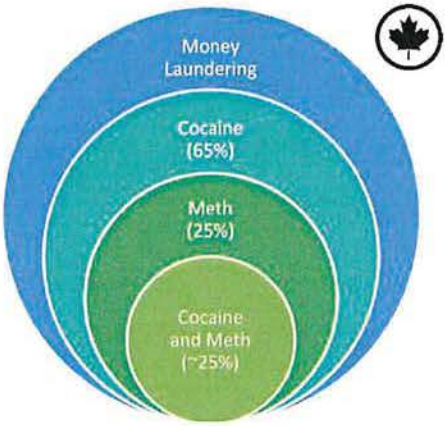


As illustrated in **Figure 4**, there is a significant overlap by these crime groups of involvement in money laundering and in two priority drug markets: 115 money laundering groups (65 percent) are involved in the cocaine market, 45 (25 percent) are involved in the methamphetamine market, and 43 (nearly 25 percent) are involved in both the cocaine and methamphetamine markets.

OCGs involved in money laundering as well as cocaine and methamphetamine are located in western Canada, the Prairie Provinces, Ontario, Quebec, and New Brunswick, and include outlaw motorcycle gang (OMG) chapters and various PMLs. The money laundering activities of groups involved in the importation and distribution of drugs suggest the movement of funds, or settling of debts through other value transfers (such as the exchange or trade of goods or other assets), to source countries of illicit drugs or precursors and chemicals.

Approximately 37 percent of groups involved in money laundering have interprovincial or intra-provincial links (see **Figure 5** on the next page) and operate within multiple jurisdictions in Canada, indicating that their proceeds from crime are crossing multiple policing

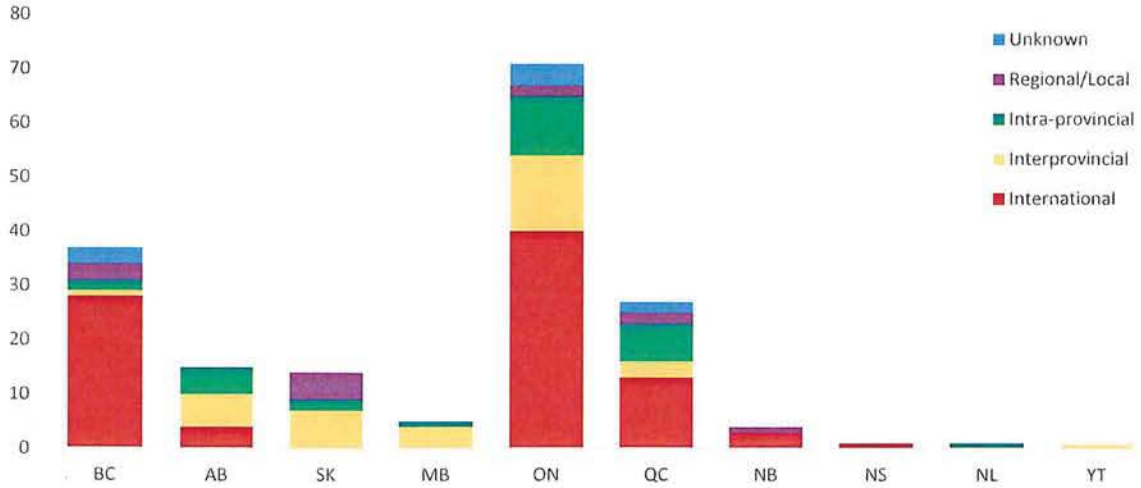
Figure 4 – Overlap in Market Involvement Related to Money Laundering (Domestic Scope)



[3] There are an additional 1200 OCGs that are not currently assessed by the ITA process, given the absence of recent and meaningful information that hinders an accurate and comprehensive assessment of their criminal activities.

jurisdictions. Participants include members of Ontario and Quebec-based OMGs as well as members of mafia-structured crime groups. Various street gangs with interprovincial links are also reportedly involved in money laundering.

Figure 5 – Number of OCGs Involved in Money Laundering per Province, by Geographic Scope*



**No groups in Prince Edward Island have been assessed to be involved in money laundering.*

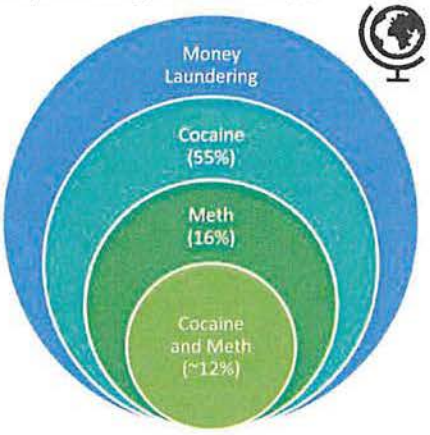
Criminal Involvement and International Scope

Approximately 50 percent (89) of the 176 assessed OCGs maintain international links, with the top five countries being the United States, Mexico, China, Colombia, and Australia. Given that some of these groups are also associated to the cocaine and the methamphetamine markets, it is not surprising to see some of these countries listed as having the most links to OCGs involved in money laundering.

According to FINTRAC, Canada-based money laundering service providers (also known as PMLs) have key ties to Asia, the Middle East, as well as to Latin America. These PMLs are believed to act on behalf of transnational OCGs and use legitimate or fraudulent trade, or the comingling of proceeds of crime with legitimate payments. Additionally, there are money launderers suspected of using MSBs and informal value transfer systems (IVTS's) for cash pickup and transfer schemes that involve money flowing to Canada from Asia and the Middle East.

Similar to those groups with domestic scope, groups with international links involved in money laundering are also involved in two priority drug markets (see **Figure 6**): 49 money laundering groups (55 percent) are involved in the cocaine market, 14 (16 percent) are involved in the methamphetamine market, and 12 (almost 13 percent) are involved in both the cocaine and methamphetamine markets.

Figure 6 – Overlap in Market Involvement Related to Money Laundering (International Scope)



Professional Money Launderers

Of particular concern to law enforcement are OCGs and criminals that launder funds by engaging PMLs who offer their services for a fee. PMLs coordinate operations for OCGs, individual criminals, and also themselves. This type of criminal can include corrupt and dishonest professionals such as accountants, bankers, and lawyers, as well as owners or

affiliates of money services business and trading (import/export) companies. PMLs sell their services to OCGs and other criminals, but are often not part of the criminal activities that generate the proceeds of crime they launder. This permits them to remain insulated from the predicate offences, and makes it difficult for investigators and prosecutors to prove knowledge of the illicit origins of the funds. Some Canadian PMLs are estimated to launder hundreds of millions of dollars CAD per year.

In 2019, the Government of Canada amended the *Criminal Code* related to money laundering offences. Under subsection 462.31(1), "Laundering the Proceeds of Crime," the offence was broadened from requiring knowledge or belief to include recklessness as to whether the property or proceeds being used, transferred, transported, or otherwise dealt with were obtained through the commission of an offence. The previous requirement of either knowledge or belief regarding the origin of the property made prosecuting PMLs very challenging because of their insulation from predicate offences. The change gives law enforcement authorities and prosecutors a new avenue to counter the complex and evolving role of PMLs.

Some groups, based in British Columbia, Ontario, and Quebec, not only launder their own proceeds of crime but also provide laundering services for other crime groups primarily linked to the precursor chemicals and synthetic drugs markets that have links to Asia.

Money Laundering Typologies

Practically every aspect of the legitimate economy and financial services industry can be exploited or misused for money laundering purposes. OCGs employ a wide variety of methods to legitimize criminal profits and circumvent anti-money laundering measures. The most complex schemes can involve all three steps of the previously-mentioned laundering process through exploiting MSBs, using IVTS's, and layering through TBML.

As part of the 2018 *Independent Review of Money Laundering in British Columbia*, Peter German and associates assessed main typologies of the activity, including laundering through casinos, real estate, and luxury vehicles. The findings of the independent review resulted in the creation of the Commission of Inquiry into Money Laundering in British Columbia, also known as the Cullen Commission, which is ongoing in 2020.

Methods of laundering such as through real estate, casinos, private sector businesses, cryptocurrency, and bulk cash smuggling are used by OCGs and PMLs across all levels of sophistication. More sophisticated methods such as TBML or schemes with complicated financial arrangements often require the assistance of PMLs or professional service providers such as accountants, bankers, and lawyers.

The 176 groups identified to be involved in money laundering do so most prevalently through private sector businesses, MSBs / IVTS's, casinos / gambling[4], real estate, and cryptocurrency. OCGs and other criminals may use more than one typology to facilitate money laundering at any given time, depending on the volume of illicit funds needing to be cleaned, and their access to different methodologies.

Private Sector Businesses

Private sector businesses are used for money laundering purposes in numerous ways, including the commingling of proceeds of crime within legitimate business cash inflow, falsifying receipts and invoices, paying employees in cash, the use of corporate accounts to purchase assets (real estate, assets and high-valued goods) to further obscure origin and ownership, the use of nominees and shell companies to distance transactions from beneficial owners, and providing financing or loan services using proceeds of crime. Of the 176 OCGs identified as being involved in money laundering, approximately 28 percent (50) are suspected of using private sector businesses to facilitate laundering or hiding their proceeds of crime.

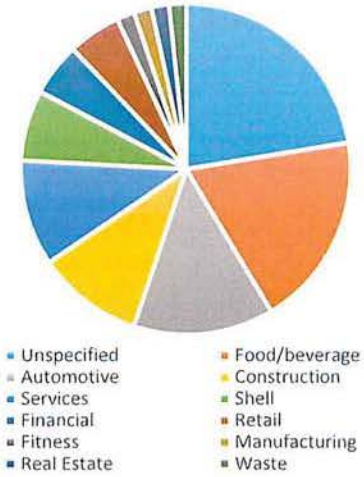
[4] For the purposes of this assessment, legal and illegal gambling methodologies, like the use of casinos and illegal gaming houses, were combined into one category. This is the result of reporting gaps concerning the specific types of gaming being used, so a differentiation could not be made.

The vast scope of Canadian private sector businesses provides organized crime significant opportunities to hide their money laundering activities within legitimate enterprises and concurrently challenges law enforcement due to the difficulty in determining which businesses are criminally involved or complicit. The use of nominee owners also complicates linking businesses to groups.

According to Innovation, Science, and Economic Development Canada's Small Business Branch, as of December 2017, there were 1.18 million employer businesses in Canada, providing employment for approximately 11.9 million people. The majority of these (1.15 million, or 97.9 percent) are small businesses, employing less than 100 people; over half (53.8 percent) employ between one and four employees.

The number of businesses to which OCGs are linked or in which they have influence is believed to be under-reported. Based on the 176 OCGs identified as being involved in money laundering, the top three most common private sector businesses suspected of facilitating money laundering activities are food/beverage services (e.g. restaurants and bars), automotive (e.g. vehicle sales and repair), and construction (e.g. new builds and renovations). **Figure 7** illustrates the types of private sector business used to launder proceeds of crime.

Figure 7 – Private Sector Businesses Used by OCGs Involved in Money Laundering, by Type, 2019



Money Services Businesses

FINTRAC oversees registered MSBs in Canada, defining that category as businesses that offer foreign exchange dealing, money transfers, issues or redeems money orders, traveller's cheques or similar products, or deal with virtual currency (oversight of this latter element effective as of June 1, 2020). These businesses are regulated and must pre-register before commencing operations. As of March 2019, 1101 MSBs are registered with FINTRAC.

There are two types of MSBs in Canada: national companies with numerous agents that have access to hundreds of thousands of locations worldwide and conduct large volumes of transactions and services, and local companies that provide transactions to specific geographic regions, which are relatively small and are often family-owned. Because MSBs are a cash-intensive business, they are able to facilitate the placement of illicit funds into the legitimate financial system. Two of the larger national MSBs in Canada generally transmit money via wire transfer and report having over 5000 and 2500 locations respectively across Canada. In contrast, the smaller, local MSBs have only limited locations, and typically function as part of an IVTS.

IVTS's are alternative remittance systems (also commonly called *hawala*, *hundi*, and *fei ch'ien* networks) used around the world in areas with limited accessibility to traditional banking services. Using ITVS's, clients transfer value without the requirement for the funds to be physically transferred from one country to another. IVTS's are also considered MSBs, must register with FINTRAC, and must implement a compliance regime in order to meet obligations under the *PCMLTFA*.

OCGs exploit legitimate MSBs for money laundering, through infiltration and corruption or by complicit businesses that ignore indications of criminality and accept transactions using suspected proceeds of crime. Of greatest concern are MSBs that are owned or controlled by OCGs, as they can launder significant amounts of funds and can facilitate the international payment of criminal enterprises' illegal transactions for payments related to importing drugs.

Casinos and Gambling

Casinos deal with significant quantities of money and are essentially cash-based businesses; however, they are not considered an MSB. They are vulnerable and at risk of criminal exploitation aiming to legitimize proceeds of crime,

and some are known to be used to launder funds. While casinos are required to report large currency transactions, as well as suspicious transactions, irrespective of size, to FINTRAC, the volume of funds flowing through casinos provides a strong cover for illicit funds.

Eighteen of the OCGs assessed in 2019 are reportedly using casinos or gambling to launder their proceeds of crime. Criminals use casinos to launder funds by buying casino chips with cash, bank drafts, or other financial instruments that represent proceeds of crime. After gambling with the chips, with or without losses, individuals cash out their chips in the form of a deposit to their patron gaming fund account, casino cheque, or cash with a casino receipt, which can provide a veil of legitimacy, as the funds represent gambling winnings if not otherwise identified by the casino (i.e. "return of funds - not gaming winnings").

Regulatory changes were implemented in British Columbia casinos in January 2018 as a way to impede and deter money laundering methods at casinos in that province. This includes changes to the verification of the source of funds valued at $10,000 CAD per 24-hour period, and casino-issued cheques not based on winnings but identified as "return of funds – not gaming winnings." The impact of these regulatory changes is unknown at this time. This method of using casinos to launder money is suspected to have potentially evolved and/or is being used in casinos in other Canadian provinces, although intelligence on these developments has not yet been established.

Real Estate

(This section assesses the use of real estate to facilitate money laundering. For an assessment of real estate fraud, please consult page 23.)

Criminals exploit the real estate market for money laundering purposes by using proceeds of crime to purchase property, often after the illicit funds have transited through the money laundering stages of placement and layering to obscure their criminal source. Real estate is an attractive investment for illicit funds as it can provide a home to live in, a relatively secure high-value investment, and/or a place to conduct further criminal endeavours, including OMG clubhouses, underground casinos, brothels, and drug production and/or trafficking.

Money laundering through real estate uses various mortgage and loan schemes that result in proceeds of crime being used to purchase properties. Methods include purchasing properties or paying down mortgages, refinancing, or other loans with proceeds of crime, and manipulating property values (also considered fraud) and obtaining loans against the overvalued real estate that are paid using proceeds of crime. Purchased real estate is used to launder funds by presenting proceeds of crime as rental income and undertaking renovations. Depending on the sophistication of the transaction, criminals may engage the assistance of corrupt or unwittingly-used professionals, such as appraisers, real estate agents, accountants, lawyers, or notaries, to complete their transaction. The specialized knowledge and skills of these service providers are used to obscure the source of funds and the beneficial ownership of the property.

Inadequate transparency in Canada surrounding beneficial ownership is an important enabler to money laundering through real estate, as the legal ownership of property by companies, partnerships, trusts, and nominees allows the individual(s) with the actual control of the property to be concealed.

TRADE-BASED MONEY LAUNDERING

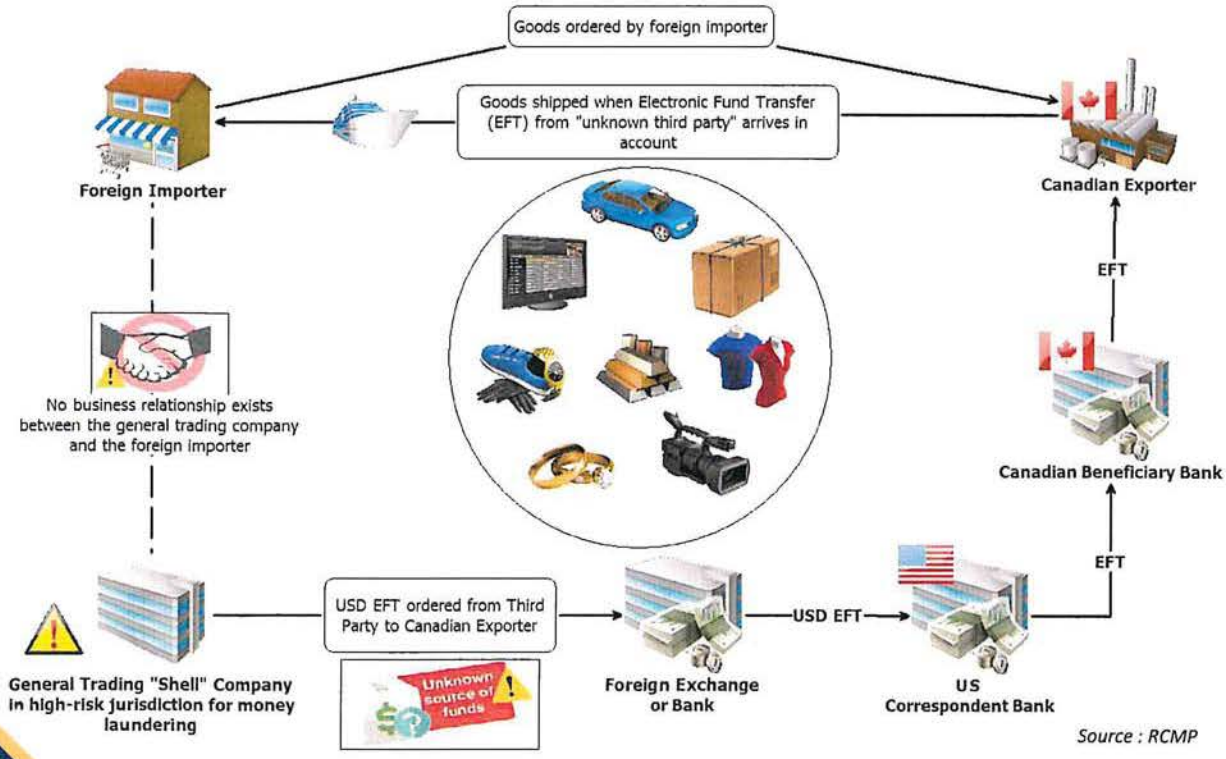
Key Highlights

- Trade-based money laundering (TBML) is used to move proceeds of crime in volumes believed to be in the hundreds of millions of dollars through Canada, but is under-recognized due to the complex international business arrangements that its schemes use.
- Canadian PMLs are engaging in significant TBML activities for international clients, but specifics regarding the scope of the scheme's use by established Canadian OCGs is unknown.
- As anti-money laundering efforts continue to focus on other laundering methods, PMLs are likely to increase TBML schemes as an alternative source of legitimization for proceeds of crime.
- Trade payments from unrelated third party import/export companies located in jurisdictions that are a high-risk for money laundering represent a significant risk in suspected TBML schemes.

Market Analysis

TBML is the process of disguising proceeds of crime and moving value through trade transactions in an attempt to legitimize their illicit origin. Criminals use illicit proceeds to purchase goods to sell in legitimate trade markets, an activity that enables complicated arrangements that provide seemingly-legitimate reasons to justify the transfer of funds across jurisdictions and parties. Through methods including fraudulent invoices and customs declarations, payment through unrelated third-party companies, and underground value transfers, TBML is particularly useful for repatriating money to drug source countries, while simultaneously enabling the circumvention of capital flight restrictions or sanctions. Any kind of goods may be involved, but electronics, vehicles, textiles, and precious metals and stones are frequently observed in TBML schemes. In many cases, no physical goods are exchanged, with fraudulent invoices providing rationale and cover for transnational fund transfers between companies. Though domestic trade can also be used for money laundering purposes, TBML predominately describes international trade exploitation, which takes advantage of complex trade arrangements across multiple jurisdictions (see **Figure 8**).

Figure 8 – Third-Party Payments: Layering and Integration of Foreign Illicit Funds in the Canadian Economy



Source : RCMP

Commercial fraud, which includes TBML, was assessed as a very high threat by Canada's Department of Finance in its 2015 *Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada*. Intelligence from ongoing investigations, FINTRAC disclosures, and open source reporting indicate that domestic PMLs and transnational OCGs have likely increased the use of TBML as a money laundering technique in the past five years.

Capabilities and Vulnerabilities

PMLs are generally insulated from the predicate offences that generate proceeds of crime in Canada or abroad. OCGs and PMLs use many variations of TBML, tailoring their methods to the needs in any scenario. Fraudulent customs information (i.e. customs trade fraud), third party payments (i.e. wire fraud), and the Black Market Peso Exchange (BMPE) are examples of commonly-used TBML schemes. While it can be conducted anywhere, the Canadian trading companies and businesses used in TBML are primarily clustered in major logistics and trade centres, such as Toronto, Vancouver, Montreal, and Halifax.

The common theme in TBML involving falsified customs information is fraud related to invoicing and customs declarations. In a scheme referred to as phantom shipments, money transfers are made to look like trade purchases, with all supporting documentation, but no goods or services are ever shipped or received. In schemes involving over- and under-invoicing, goods are shipped but their values are misrepresented to increase or decrease their value. This misrepresentation provides cover for the transfer of money and, in cases of under-valuation, masks the additional revenue that is made on the sale of the goods. In another simpler variation, high-value goods can be purchased with the proceeds of crime, then exported and re-sold abroad.

The BMPE involves transnational OCGs, such as Mexican or South American drug cartels, repatriating drug profits, often from the United States. There are a variety of methods under this category, generally involving structured cash deposits of USD followed by transactions of Mexican or South American importers buying those US funds from complicit brokers and paying for them in pesos. The importer uses the US funds to purchase goods shipped to their countries, while the broker returns the pesos from the importer to the cartels. An example of a Canadian connection to a BMPE scheme involves suspected illicit proceeds of crime being sent from the US or South America to Canadian trading companies, which in turn use the funds to buy goods from exporters abroad.

CRYPTOCURRENCY

Key Highlights

- Knowledge and use of cryptocurrencies has increased steadily over the past three years among the Canadian public and Canadian OCGs.
- Cryptocurrencies are commonly used as a means of payment for mass-marketing fraud and dark web marketplace purchases, and are also an attractive tool for laundering proceeds of crime.
- Use of anonymizing services and tools, such as mixers and tumblers, to obscure cryptocurrency transaction routing has tripled over the past year.
- Recent amendments to Canadian anti-money laundering regulations will force cryptocurrency exchanges complicit in criminal activity to adopt new methods to avoid data reporting to financial intelligence units, and may result in many operations moving to foreign jurisdictions.

Market Analysis

Cryptocurrencies are decentralized digital assets that can be exchanged for government issued (fiat) currency, transferred from person to person, or exchanged for other virtual currencies. Bitcoin, which composes nearly 70 percent of the market, is the original and most widely-used type, but more than 2500 others exist.

Awareness and interest surrounding the technology has increased steadily since Bitcoin's creation in 2009; in 2019, 89 percent of surveyed Canadians had heard of Bitcoin, up from 62 percent in 2016. It can be used to make purchases in Canada in participating coffee shops, restaurants, electronics retailers, and on some e-commerce websites. Consumers obtain cryptocurrencies by buying them with fiat currency at crypto exchanges, using cryptocurrency ATMs, or via informal peer-to-peer exchanges. Just like the public, criminals in Canada are increasing their use of cryptocurrencies. They are attractive due to the added privacy of transactions and the challenges that law enforcement agencies encounter when trying to identify involved parties.

The use of mixers and tumblers, tools to obscure transaction routing by mixing different streams of potentially identifiable cryptocurrency, increased dramatically in the past year, likely as a result of law enforcement's increasing capabilities for forensic analysis of the cryptocurrency records-keeping system known as a blockchain. Many cryptocurrencies, including Bitcoin, use a public ledger on which all transactions are recorded and visible. Mixing or tumbling is a process through which cryptocurrencies from many users are pooled and transferred, making it much harder for law enforcement to associate transactions with specific individuals. Industry analysis from April 2019 indicates that over 4 percent of all Bitcoin transactions were mixed, an increase of 300 percent compared to data from the prior nine months. Other cryptocurrencies known as "privacy coins" or "anonymity enhancing coins" provide an even greater focus on obscuring transactions by using systems that do not have publically visible ledgers. With the use of mixers, privacy coins, or a combination of both, criminal actors can move large amounts of cryptocurrency with heightened privacy while bypassing the reporting requirements found in the traditional financial sector.

Capabilities and Vulnerabilities

Cryptocurrencies have a significant impact on Canadians when used for criminal purposes. Bitcoin and other currencies are a preferred payment method for perpetrators of mass-marketing frauds. Cryptocurrency transactions are irreversible, challenging recovery efforts after scams are reported. Cryptocurrencies are also fully incorporated into the business model of dark web contraband trafficking. EUROPOL's *2019 Internet Organized Crime Threat Assessment* reported that Bitcoin was the most frequently used cryptocurrency in dark web market transactions in 2019, with the equivalent of over $1 billion USD spent.

As a tool for money laundering, cryptocurrencies allow for transfers of large volumes of funds away from the oversight of the traditional financial sector or the reporting requirements found in other transactions. Part of cryptocurrency's appeal is the pseudo-anonymity inherent in the processes. Though blockchains do not record the names of individuals involved, all transactions leave important clues that can be assessed by law enforcement. Data from Bitcoin's distributed public ledger can be analyzed with a variety of tools that facilitate the identification of both the transfers and the people who conducted them.

Cryptocurrency exchanges are a major method for the placement of proceeds of crime into virtual currencies. Operating both online and in brick-and-mortar locations, these businesses facilitate transactions and the conversion of fiat currency into cryptocurrency, as well as exchanges between different cryptocurrency types. Exchanging cryptocurrencies across multiple types obfuscates the original source of the funds, and can make tracing difficult.

There are more than 730 cryptocurrency ATMs in Canada, up from 205 in 2017. They can be used by criminal actors to deposit illicit cash in exchange for Bitcoin or other supported virtual currencies, and many do not require any form of identification. Cryptocurrency ATMs have varying deposit and withdrawal limits, most often falling below $10,000 CAD. ATM ownership and operation can also be exploited; a criminal actor with control over an ATM can stock it with cash obtained through illegal activities, receiving legitimate electronic payment for the funds disbursed.

Established OCGs across all spectrums, from OMGs to mafia-structured crime groups, as well as the PMLs who support them, are reported to be using cryptocurrency for criminal purposes such as laundering proceeds of crime and facilitating money transfers as payments for drugs and illegal activity. Other groups with links to Asia are likely using Bitcoin to move money through countries as it is popular method to avoid capital flight restrictions.

Cryptocurrency is a popular payment method for mass-marketing fraud. FINTRAC reported a significant increase in suspicious transaction reports submitted in 2017 and 2018 linked to cryptocurrencies and fraud.

Canadian Law Enforcement Implications

The Government of Canada amended the *PCMLTFA* regulations in July 2019 to regulate dealers in virtual currency and update reporting and record-keeping requirements for virtual currency transactions. The changes, which will have phased-in compliance beginning in June 2020, are anticipated to have a significant impact on the operations of cryptocurrency exchanges. Under the new regulations, cryptocurrency exchanges are considered MSBs and are required to register with FINTRAC, implement compliance programs, and report suspicious transactions. Canada's regulatory amendments strengthen its anti-money laundering regime in accordance with Financial Action Task Force guidelines.

The *PCMLTFA* amendments will have a significant impact on how criminals acquire and transfer cryptocurrency. Criminals are keenly aware of "Know Your Customer" (KYC), the collection of identifiable customer information to allow attributable records of financial transactions; in 2018, US Exchange ShapeShift saw a major decrease in users and revenue after it began collecting details to identify customers. With tighter regulations on domestic exchanges, criminals seeking cryptocurrency are likely to use peer-to-peer trading, often advertised online, and PMLs are likely to take advantage of the demand in the newly-regulated space by offering services to replace exchanges. FINTRAC reports from 2015-2018 found that account activity of businesses engaged in suspected cryptocurrency money laundering was inconsistent with the stated nature of their business activities. Businesses claiming to operate in a range of sectors used their accounts as flow-through conduits to buy and sell virtual currency.

Though changes to regulations are a positive step to deal with abuses of cryptocurrencies, many challenges from a law enforcement perspective still exist. By their very design, cryptocurrencies are decentralized, with no central point of contact for access or oversight. As with many crimes with a cyber component, law enforcement authorities face jurisdictional issues when identifying foreign links to cryptocurrency investigations.

MASS-MARKETING FRAUD

Mass-marketing fraud is an umbrella term for fraudulent schemes that use mass-communication media (including telephones, internet, mail-outs, television, radio, and in-person contact) to defraud multiple victims in one or more jurisdictions. Five key categories of schemes are included in this section, including government services schemes, identity theft and phishing, romance schemes, ransomware schemes, and elder-targeted schemes.

Government Services Schemes

Involving impersonation scams and/or deceptive telemarketing, government services schemes consist of an individual or group posing as a government representative to mislead a victim into revealing sensitive financial or personal information in order to steal their money or identity. In many cases, fraudsters resort to extortion to complete their scheme, threatening severe financial or judiciary consequences if victims do not comply immediately and demanding restitution in the form of Interac e-transfer, cryptocurrency (i.e. Bitcoin), prepaid credit card, or gift card. These schemes erode public confidence in government institutions and enforcement agencies and have the potential to fuel distrust among many citizens, particularly those from more vulnerable communities.

Traditionally accomplished via telephone and email, government services schemes are increasingly expanding their tools, including the use of text message or social media platforms (e.g. Facebook Messenger or WhatsApp) to communicate with victims. Among recent trends is the increase in reported schemes whereby criminals spoof a legitimate government phone number when contacting victims in order to lend credence to their claims of legitimacy. **Table 2** highlights some of the more commonly encountered schemes in Canada. Whereas many are contrived to defraud victims of their money, the Service Canada scheme, which has seen a recent increase, is of particular concern, as the unwitting release of SIN data in combination with other personal information, such as name and address, often leads to identity theft.

Table 2 – Notable Typologies of Recent Government Services Scams

Canada Revenue Agency (Tax Return) Misleading victims into paying a false debt; or offering a refund while asking for banking account numbers and other financial details.
Service Canada (Social Insurance Number) Claims that an individual's SIN has been cancelled, compromised, or associated with a criminal act, and requiring a fee to fix the issue; closely associated to identity theft.
Immigration, Refugee and Citizenship Canada (Immigration Scam) Claims that an immigrant or individual working towards citizenship has not correctly completed and submitted immigration documents, and requiring a fee to avoid deportation.

Very few Canadian OCGs have been reported to be involved in government services schemes in the past several years; in 2019, only four OCGs are identified. Canadians are being targeted primarily by fraudsters operating international "boiler rooms," which are organized for the sole purpose of extortion. A joint investigation between the RCMP and law enforcement in India that involved call centres in India effecting the CRA scheme, resulted in the arrests of alleged money mules in Canada and call centre operators in India in March 2020. New citizens or residents working towards becoming citizens are particularly vulnerable to such schemes, as they may be less familiar with legitimate government practices. In 2018, for example, the U.S. disrupted an Internal Revenue Service scheme originating in India whereby fraudsters misrepresented themselves as government officials and threatened victims with arrest and deportation if they failed to make payments. More than 15,000 victims lost hundreds of millions of dollars USD, and more than 50,000 individuals' personal information was misused.

Identity Theft and Phishing

In 2019, almost 2000 Canadians were reported by the CAFC to have been victims of identity theft, with a total dollar value loss of over $506,000 CAD. These figures represent a marked increase from 2017, when just over 1500 Canadians were defrauded, resulting in almost $269,000 CAD in losses. Victims of identity theft come from all spheres of society and all income and age groups.

There are many different schemes used to steal individuals' identities. A popular method involves phishing, whereby criminals communicate with individuals while purporting to be from reputable entities in order to induce the disclosure of personal information (see **Table 3** for variations). Phishing schemes can take the form of a traffic infringement scam, unsolicited service calls, computer repair services, or vacation and travel offers, among others. Reported phishing incidents and associated dollar losses have increased over the past three years, and remains one of the most reported schemes relating to identity theft. Spear phishing has reportedly become the most lucrative type of identity theft scheme in 2019, totalling more than $21.4 million CAD in losses.

One newly-reported trend involves "SIM-swapping," whereby fraudsters misrepresent themselves to a mobile provider and use stolen personal information about a subscriber to report a phone as lost or stolen. The phone is then linked to a new SIM card and device under the fraudster's control, after which they can access various applications and reset account passwords. If an online banking account is linked to a victim's phone number or email address, fraudsters can obtain a new verification code and hijack associated financial accounts.

Table 3 – Notable Typologies of Phishing Attacks

Email Phishing Targets a large, indiscriminate number of people.
Spear Phishing Involves a targeted attack directed at a single person.
Whale Phishing Involves a targeted attack directed at specific high-ranking employees, such as CEOs.

Twelve of the OCGS assessed in 2019 are reported to be involved in identity theft in Canada. The majority are located in British Columbia, and almost half have international connections. One group has members with direct links to Nigeria, which has long been a source of phishing schemes targeting Canadians. In addition to OCGs, other criminal actors are also exploiting their expertise to commit identity theft, such as recent reports of the theft of data by employees of financial companies. In 2019, Desjardins Financial Co-Operative was defrauded when an employee stole the personal data and information of 4.2 million customers. Capital One customers in Canada and the U.S. also had their personal data stolen by a hacker, who was a former Amazon software engineer. While the Desjardins incident highlights the dangers of potential insider threats to financial institutions, the Capital One incident illustrates how vulnerable these entities are to outside rogue or criminal elements.

Romance Schemes

Victims reported more than $24 million CAD in losses relating to romance schemes to the CAFC between 2018 and 2019. Actual losses are likely much higher, as only five percent of incidents are believed to have been reported. Between 15,000 and 20,000 Canadians are believed to have suffered monetary loss to romance schemes in 2018, with less than 1000 occurrences reported.

Typical Romance Scheme

Victims are lured into a false relationship with a fraudster, often through the use of information that they have posted online. Once trust has been established, an emergency situation is concocted whereby the fraudster is in dire need of funds and emotionally extorts money from the victim.

Criminals involved in romance schemes are also frequently involved in other types of fraud. The money laundering transactions created through these schemes and the use of money mules to facilitate crimes indicates that OCGs may be working in concert to commit these schemes, sometimes on an international scale. For example, a Nigeria-based transnational OCG is believed to be stealing between $100 and $300 million dollars USD per year in North America. With a presence in at least 26 countries, including Canada, this OCG is primarily involved in fraud – including romance schemes and counterfeiting operations – and money laundering across Canada. Romance schemes comprise approximately 50 percent of its criminal operations, wherein it recruits young educated males and may operate in stages (luring victims, establishing and maintaining a fraudulent romantic relationship, receiving money from victims). The group also uses their victims as money mules to launder money, usually acquired from another victim or criminal activity, in order to further insulate themselves.

Romance schemes are expected to increase in the coming years, particularly through the continued use of social media (e.g. dating and networking sites). Facebook ranks as the primary site where individuals fall victim to romance schemes, although many others originate on dating sites (e.g. Match.com) and other social networking sites (e.g. Instagram). The increasing number of online social apps creates an ever-growing terrain in which criminals can operate.

Ransomware Schemes

Canadian individuals and institutions (including businesses, universities, banks, hospitals, and government agencies) are estimated to be targeted by ransomware attacks approximately 3200 times a day, according to data from the CAFC. On average, such attacks are estimated to cost between $1 and $3 million CAD per incident, including ransom payments and lost productivity. Although ransomware schemes represent only a very small proportion of extortions reported to the CAFC, losses to this type of fraud can be significant in terms of lost money and information, and reporting is estimated to represent only a fraction of the actual number occurring in Canada.

Ransomware Defined

Criminal actors deploy malicious software to attack computer networks by encrypting files and holding data hostage. Payment to release files is often demanded in the form of Bitcoin.

Institutions, such as government departments and private sector businesses, are often targeted due to the sensitive nature of data being compromised and the resulting large profit to be made.

Most victims pay the ransom, as it is seen to be less costly than restoring their systems; however, ransomed files often become corrupted and unrecoverable, and data loss is common, even if the ransom is paid.

In addition to the potential for data to be stolen, resulting in privacy breaches and privacy concerns, compromised computer systems can also lead to a gamut of other frauds, including identity theft and extortion, and can present a threat to Canadian infrastructure or government operations. In cases involving medical institutions, a ransomware attack holding medical records hostage could result in potentially serious health risks, including death. In a recent example, the Nunavut government was a target of ransomware attacks, where its citizens were without internet, payment and medical appointments. The temporary disruption of the organization's functioning services severely impacted society's public order and individuals, causing economic damage. In another example, a health centre providing services to approximately 13,000 clients in Nova Scotia was attacked by ransomware in 2018-2019, resulting in their computerized systems shutting down for several days and negatively affecting many patients.

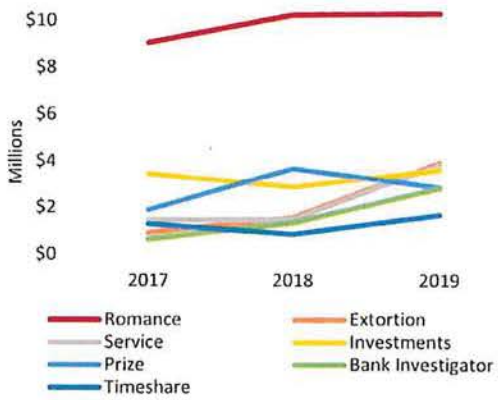
In 2019, the United States was affected by an unprecedented number of ransomware attacks, affecting 966 government agencies, as well as healthcare and education sectors – emergency services were interrupted; police agencies were locked out of their systems; prison doors could not be remotely unlocked; and medical records were lost.

Given the cyber nature of ransomware schemes, criminal actors are not constrained by geographical limitations; they are located in countries across the globe. No Canadian OCGs have yet been reported to be associated to such schemes, although the complexity of investigations into these activities hinders an accurate assessment by law enforcement of their involvement. Ransomware is likely to continue to be a pre-eminent cybercrime threat, as it generates high financial returns.

Elder-Targeted Schemes

Fraud targeting people over the age of 60 (commonly referred to as elders or seniors) is expected to increase in Canada as the population of people over the age of 60 grows. Around the world, the number of elders is growing faster than all other age brackets, and in 2016, Canada's seniors were already estimated to comprise 17 percent of the country's population. The CAFC recorded over 14,000 complaints involving seniors in 2019, representing approximately one quarter of all Canadian victims and totalling more than $35 million CAD lost. The primary fraud typologies resulting in the most financial losses for seniors include romance schemes, extortion, service schemes, investment schemes, bank investigator (impersonation) schemes, prize offers, and timeshare schemes (see **Figure 9**).

Figure 9 – Financial Losses by Seniors, by Pitch and Year



Source: Canadian Anti-Fraud Centre

High-level OCGs, including members of OMGs and mafia-structured organized crime, are indirectly benefitting in such

schemes, involved in a structure where profits are paid up from runners and intermediary OCGs in exchange for "protection." Canadian criminals based in various provinces are part of an international network targeting Canadians using pitches that typically victimize elders, including impersonation schemes (e.g. Canada Revenue Agency, Bank Investigator, and Tech Support schemes). Fraudsters have also started impersonating police and telling victims that they require assistance in an investigation addressing such schemes. Criminals then gain remote access to the victims' computer, and deceive them into transferring thousands of dollars from their bank account as part of the fake investigation.

Canadian OCGs target elders in Canada and the United States, and will likely continue to do so given their consistent success and high profits. American targets will continue to present an attractive and lucrative market because of the larger population and the higher value of the US dollar. The growing proportion of elders and their increasing use of the internet will result in more targets becoming available to elder-targeted schemes in the coming years.

SECURITIES FRAUD

Securities fraud covers a wide-range of illicit activities that involves the deception of investors and the misrepresentation or manipulation of financial markets. Some of the more prominent schemes include illegal distribution, insider trading, and market manipulation (i.e. pump-and-dump), and in particular: frauds via online trading platforms, initial coin offerings, and Ponzi and Pyramid schemes. Securities fraud jeopardizes the integrity and public interest in the capital market by creating unfair or fraudulent acts against investors, corporations, or the public.

The total dollars lost reported to the CAFC has been increasing since 2016; the actual number is believed to be higher than reported. In the past two years, residents in Ontario, Alberta, Quebec, and British Columbia, respectively, reported the most losses.

While securities schemes do not necessarily have as many victims as other types of frauds, they result in some of the highest dollars lost. One single pump-and-dump scheme can generate millions of dollars in losses for victims. For example, three Canadians were charged in January 2020, by the U.S. Securities and Exchange Commission (SEC) for the alleged operation of a $35 million USD pump-and-dump scheme that used at least 45 companies across four continents.

Securities Fraud Terms Defined

Pump-and-dump – a form of fraud in which the price of an owned stock is artificially inflated through false and misleading positive statements, in order to sell the cheaply-purchased stock at a higher price.

Initial coin offering scheme – a means of raising funds over the Internet to finance the launch of a new virtual currency. Investors are offered digital assets or "tokens" whose eventual value and usability are closely tied to the financed project's success. Markets for these assets are less regulated than traditional capital markets, and bring an increased risk of fraud.

Ponzi scheme – a form of fraud in which belief in the success of a nonexistent enterprise is fostered by the payment of quick returns to early investors from money invested by later investors.

Pyramid scheme – a form of fraud whereby members are promised payment or services for enrolling others into the scheme, rather than by supplying investments or sale of products.

Nine OCGs are reported to be involved in securities fraud (specifically in market manipulation), a number that has remained relatively stable over the past several years. Although this number represents only a small proportion of reported OCGs, they are assessed as representing higher levels of threat, indicating that this market may require a higher degree of sophistication, networking, and scope to be successful and avoid prosecution. This may also indicate that securities fraud requires OCGs to have a larger amount of capital to operate successful pump-and-dump schemes within the capital market.

Schemes target both Canadian and international investors. They can include OCGs, private sector businesses, insurance brokers, and investment companies working together to overvalue potential investments and insulate criminality. International criminal networks operate schemes in multiple countries. At its height, the binary options industry (a financial option wherein the payoff is either some fixed monetary amount or nothing at all) in Israel had victims in Canada, the US, Europe, Africa, and the Middle East.

Several Canadian OCGs associated to pump-and-dump schemes are also reported to be involved in money laundering, likely using their private sector businesses and links to the securities industry to launder their proceeds of crime, as

the securities market can offer a 100 percent return or further profit, whereas proceeds laundered through other methods usually results in some loss.

These groups also all have links to other countries, primarily to the United States, Italy, and South America. These international connections, although likely facilitating other criminal activities such as cocaine importation and drug trafficking, may also be used to facilitate securities fraud. To address its transnational nature and minimize jurisdictional impediments to investigating securities fraud, multi-agency task forces such as the Cross Border Market Fraud Initiative (CBMFI) have been created to identify criminal securities fraud activities between Canada and the United States.

Foreign and domestic criminals will continue to target Canadians, given their relatively high average income. Low knowledge of investments among some Canadians will continue to be facilitate securities fraud, especially as more people use the Internet. Securities fraud activities and strategies will continue to adapt to changes in communication media, the global economy, and enforcement, and will continue to evolve with annual market flows and trends, such as misrepresenting investment opportunities in start-up projects in industries relating to gold, green energy, cyber, medicine, and cannabis, as the capital market is seeing increasing interest in these fields. Fraudulent investment opportunities involving cyber, in particular, will continue to expand and pose a high risk to investors, based on a lack of general knowledge on legitimacy and valuation in this complex market.

PAYMENT CARD FRAUD

Payment card schemes are perceived as low risk and highly profitable. They include *card-present fraud* and *card-not-present fraud* (CNP), the latter of which occurs when a fraudulent transaction is made without the physical card and legitimate cardholder present. By stealing card details through virtual (i.e. malware, phishing) and physical technologies (i.e. card skimmers, false pin pads), criminals are able to make fraudulent online and in store purchases.

CNP is now the most prevalent form of payment card fraud. The implementation of card-chip technology on physical cards resulted in a shift toward online exploitation, as CNP fraud – especially relating to credit cards and gift cards – can be completed anonymously via the internet.

Fraudulent losses relating to credit cards are significantly higher than those relating to debit cards. In the past decade, there has been a 71 percent increase in the number of Canadian credit card accounts reporting at least one case of fraud. According to the Canadian Bankers Association, financial institutions reimbursed $862 million to Canadian credit card customers in 2018. However, in the same year, only slightly more than $6 million CAD in financial losses from credit card fraud – less than one percent – was reported to the Canadian Anti-Fraud Centre. This gross under-reporting to law enforcement presents challenges in investigating and targeting the criminals involved.

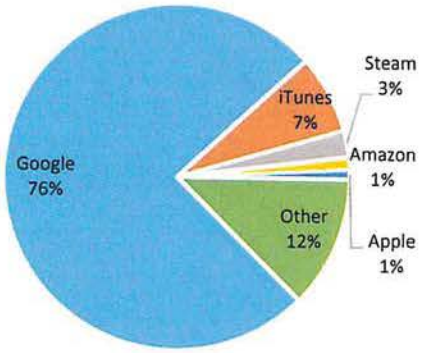
Twenty-two OCGs are reported to be involved in payment card fraud, a number that has remained relatively stable over the past five years. These groups are also all involved in other criminal markets, including illicit drugs, theft, other frauds, and money laundering, and may be using proceeds from payment card fraud to finance their other criminal activities. They are primarily based in Ontario and British Columbia, although, given the ability to target victims from any region in the world with the use of the internet, these groups have the potential to commit payment card fraud outside of their respective areas. Of these OCGs, 82 percent have an interprovincial scope and 50 percent have an international one, albeit primarily related to their illicit drug activities.

Gift card and prepaid credit card fraud will likely increase as a way for OCGs to target victims and launder proceeds of crime, as they are an anonymous and highly-liquid alternative. For example, in the first half of 2019, almost $700,000 was reported to be defrauded from residents of Edmonton, Alberta, from gift card frauds alone (see **Figure 10** on the next page for a proportional breakdown of the gift card type). Victims of the schemes were contacted by phone, email, and text, through common mass marketing fraud methods including phishing, government services scams (specifically, CRA), computer hacks, account takeovers, prize scams, and romance scams. These schemes originated from Africa,

Malaysia, Turkey, the UK, and India, highlighting the international capabilities of payment card fraud. Moreover, gift cards can also be traded for Bitcoins, which can then be sold for cash on online international exchange sites into multiple currencies, providing OCGs and criminal entrepreneurs an alternative to launder their money. (Consult the cryptocurrency section on page 16.)

As technology advances and e-commerce grows, security efforts to identify and target perpetrators of payment card fraud will remain a challenge. With the rise of the dark web and the emergence of more internet-connected and wireless devices, it will be increasingly difficult for law enforcement to successfully identify and prosecute virtual and anonymous fraudsters. Organizations worldwide are likely to see an increase in spending on cybersecurity in an attempt to prevent card data breaches.

Figure 10 – Proportion of Gift Card Fraud in Edmonton (Jan-June 2019), by business



Source: Edmonton Police Service

Whereas security implementations, such as chip technologies on credit cards, provide some security against physical technologies used in payment card fraud, skimming will remain a threat as long as cards with magnetic stripes and tap-and-pay are being used. Due to the virtual nature of payment card fraud, it will also remain difficult to enforce global initiatives to target cross-border transactions, as security policies and regulations differ from country to country.

REAL ESTATE FRAUD

Fraudulent real estate schemes include *fraud for shelter*[5] and *fraud for profit*. The latter, which can represent lucrative returns for OCGs, includes illegal property flipping, overvaluation, mortgage fraud, and title fraud. Enablers include the use of shell companies and straw buyers to conceal acquisitions and ownership, and the use of shadow lenders (unregulated by the Canadian banking system) to avoid detection. Real estate fraud also often involves collusion by industry professionals, such as lenders, real estate agents, lawyers, and underwriters to help construct, facilitate, and obscure the fraud. OCGs involved in real estate fraud target major Canadian banks, real estate investors, homeowners, or renters.

Eight OCGs – the majority of which are concentrated in British Columbia and Alberta – are reported to be involved in mortgage fraud, representing a slight increase from previous years. Six of these groups are also involved in laundering proceeds of crime, including money laundering through real estate. Of note, as highlighted in **Table 4**, several of these groups have expertise in the real estate market or collude with professionals in the industry to accomplish their fraudulent activities. Given the propensity for organized crime to launder money through Canadian real estate, real estate frauds will continue to occur, as tactics such as overvaluation of property and property-flipping help to facilitate money laundering.

Table 4 – Notable Examples of OCG Involvement in Real Estate Fraud

Use of a shell company and complicit lawyer to facilitate paperwork for mortgage fraud.
Mortgage broker completes fraudulent applications and obtains housing intended for criminal purposes.
Mortgage broker finances mortgages on properties used for insurance frauds.
Targets rental properties with absent landlords and uses a complicit notary to approve the fraudulent sale of the home.
Mortgage broker acquires high-risk mortgages for group members used for criminal purposes, including money laundering.

Real estate fraud can account for significant dollar losses. One such scheme in Alberta that spanned several years resulted in losses totalling 30 million dollars CAD for the Bank of Montreal, because of fraudulent mortgages generated by a group of criminal actors. Title fraud (using stolen personal information or forged documents to transfer a home's title without the owner's knowledge), although infrequent in Canada, can also result in significant dollar losses,

[5] Equifax Canada reported a 52 percent increase in mortgage fraud from 2013 to 2017. The majority of this increase can likely be attributed to *fraud for shelter* schemes perpetrated by homebuyers providing false information on mortgage applications to secure loans. Such schemes are becoming more prevalent, given increasing costs of housing in Canada and more stringent lending standards by financial institutions. Because this type of fraud is not profit-driven, is represents minimal organized crime involvement.