

Overview Report: Miscellaneous Documents

A. Scope of Overview Report

1. This overview report appends a number of reports and documents which Commission counsel are putting forward for the benefit of the Commissioner and participants. They are as follows and have been added as appendices below:

1.	The 2021 Crypto Crime Report – Feb 14, 2021	https://blog.chainalysis.com/reports/cryptocurrency-money-laundering-2021
2.	Ending the Shell Game: Cracking down on the Professionals who enable Tax and White Collar Crimes (OECD Report)- 2021	http://www.oecd.org/tax/crime/ending-the-shell-game-cracking-down-on-the-professionals-who-enable-tax-and-white-collar-crimes.htm?utm_source=Adestra&utm_medium=email&utm_content=Read%20more&utm_campaign=Tax%20News%20Alert%2011-02-2021&utm_term=ctp
3.	The Challenges of Implementing Anti-Money Laundering Regulation: An Empirical Analysis – Dr. Illaria Zavoli and Dr. Colin King	https://onlinelibrary.wiley.com/share/author/JZCV4KEI2XGDU MK6IVI3?target=10.1111/1468-2230.12628
4.	CAN-001303	Money Laundering in the Real Estate Sector: Media Reference Which Cites “Secret Police Study” – Prepared for Kevin Hackett - March 14, 2019
5.	CAN-001769	FINTRAC’s Update on the Real Estate Sector: Meeting with the Canadian Real Estate Association Presentation – August 7, 2019
6.	A Guide for Developing a Notary Practice Risk Assessment Program – July 2018	NA
7.	Public Consultations on Strengthening Corporate Beneficial Ownership Transparency in Canada: What We Heard – April 6, 2021	https://www.ic.gc.ca/eic/site/142.nsf/eng/00002.html
8.	Future of Financial Intelligence Sharing	NA

Cullen Commission of Inquiry into Money Laundering in BC

	(FFIS): Canada in Context – Canadian Legislation, Supervision and Operational Processes for Information-Sharing to Detect Money Laundering and Underlying Crime, set in the Context of International Practices – Feb 19, 2021	
9.	Compiled Money Laundering-Related Statistics for Cullen Commission from FINTRAC	NA
10.	Additional Statistics from FINTRAC on Money Laundering Crime Data	NA
11.	Guide on Using Money Laundering and Proceeds of Crime Data from Uniform Reporting Survey (UCR) and the Integrated Criminal Courts Survey (ICCS)	NA
12.	ICCS Data Table	NA
13.	Additional Statistics from Canada, Updated Feb 18 th , 2021	NA
14.	Additional Statistics on Money Laundering Cases 2008-2018	NA
15.	CAN-001812	FINTRAC Report to the Minister of Finance on Compliance and Related Activities – September 30, 2020

Appendix 1

Chainalysis Crypto Crime Report- February 14, 2021

The 2021 Crypto Crime Report

Everything you need to know about ransomware, darknet markets, and more

February 16, 2021

Table of Contents

Introduction	3
Money Laundering	8
Ransomware	25
Darknet Markets	42
Scams	70
Stolen Funds	80
Terrorism and Extremism Financing	92
Conclusion	106



Introduction

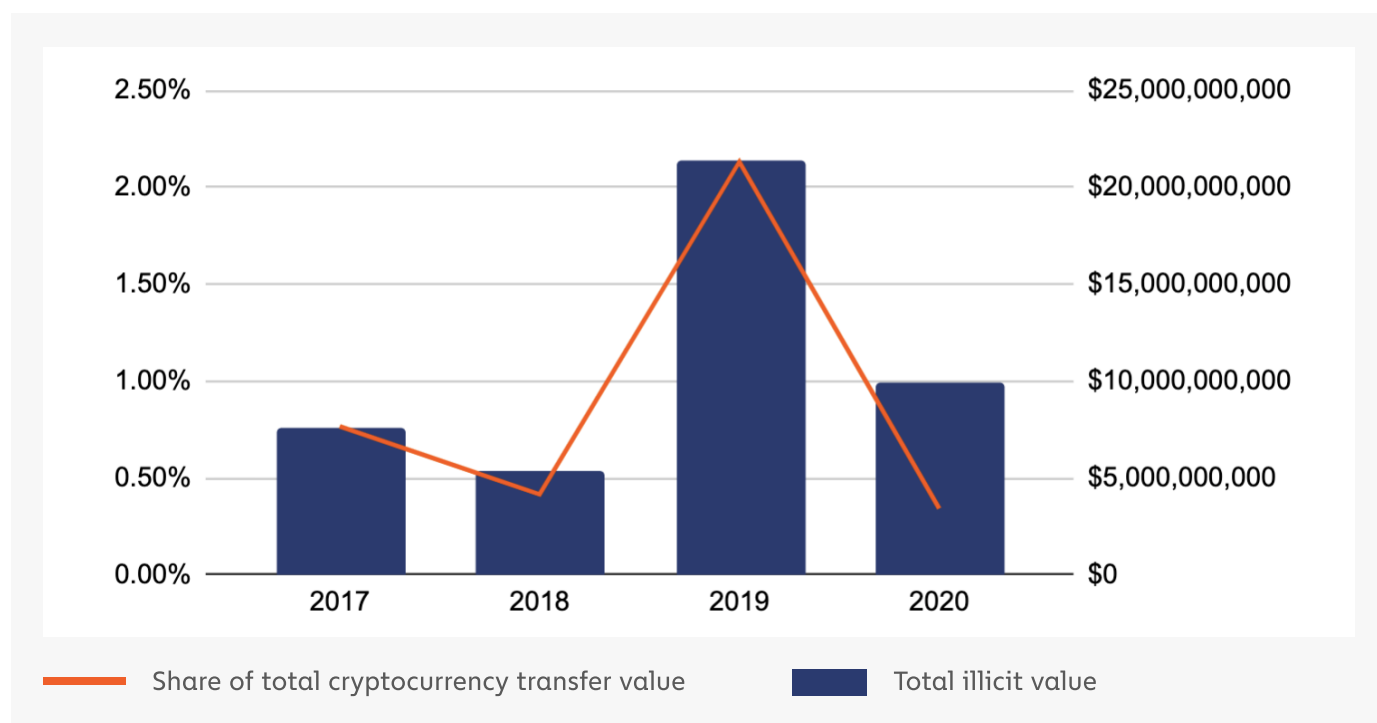
2020 Crypto Crime Summarized: Scams and Darknet Markets Dominate by Revenue, But Ransomware Is the Bigger Story



2020 was an incredible year for cryptocurrency. Despite the devastation wrought by the worldwide Covid-19 pandemic, Bitcoin has shattered its previous price records, largely driven by the increased [demand from institutional investors](#) that many in the cryptocurrency community have long speculated would drive the asset to new heights.

However, cryptocurrency remains appealing for criminals, primarily due to its pseudonymous nature and the ease with which it allows users to instantly send funds anywhere in the world, despite its transparent and traceable design. But the good news is that cryptocurrency-related crime fell significantly in 2020.

Total cryptocurrency value sent and received by illicit entities vs. Illicit share of all cryptocurrency activity | 2020





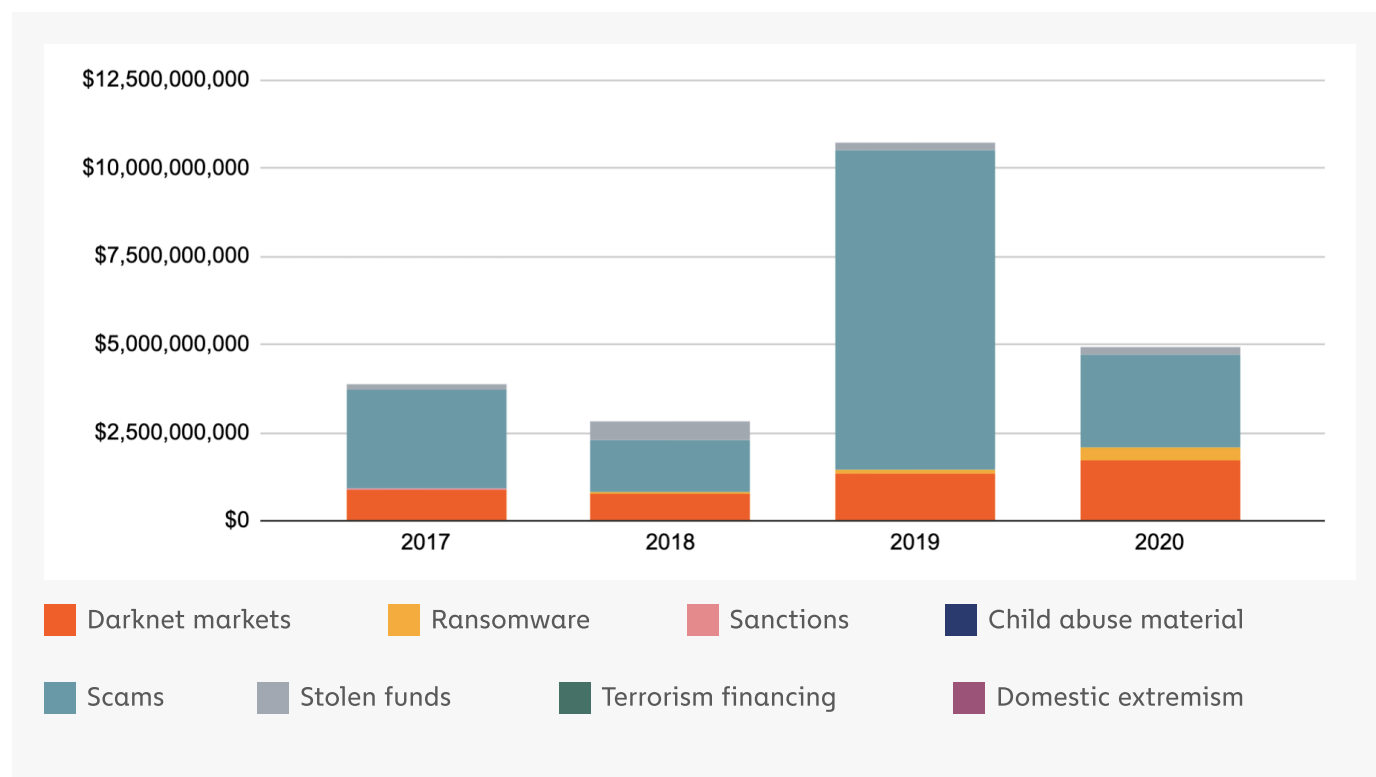
In 2019, illicit activity represented 2.1% of all cryptocurrency transaction volume or roughly \$21.4 billion worth of transfers. In 2020, the illicit share of all cryptocurrency activity fell to just 0.34%, or \$10.0 billion in transaction volume. One reason the percentage of illicit activity fell is because overall economic activity nearly tripled between 2019 and 2020.

We should note that at the time of writing last year's report, we reported 2019's illicit share of cryptocurrency activity to be 1.1%. The reason for the change is the identification of more addresses associated with illicit activity that was active in 2019. Most of those addresses were related to scams that had yet to be identified as such, primarily related to the PlusToken scam. Some are related to previously unreported ransomware attacks. For that reason, we should expect 2020's reported illicit activity numbers to rise over time as well.

Regardless, 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 to the amount of illicit funds involved in traditional finance.

What kinds of crime drove that 0.34% of cryptocurrency transactions associated with illicit activity in 2020?

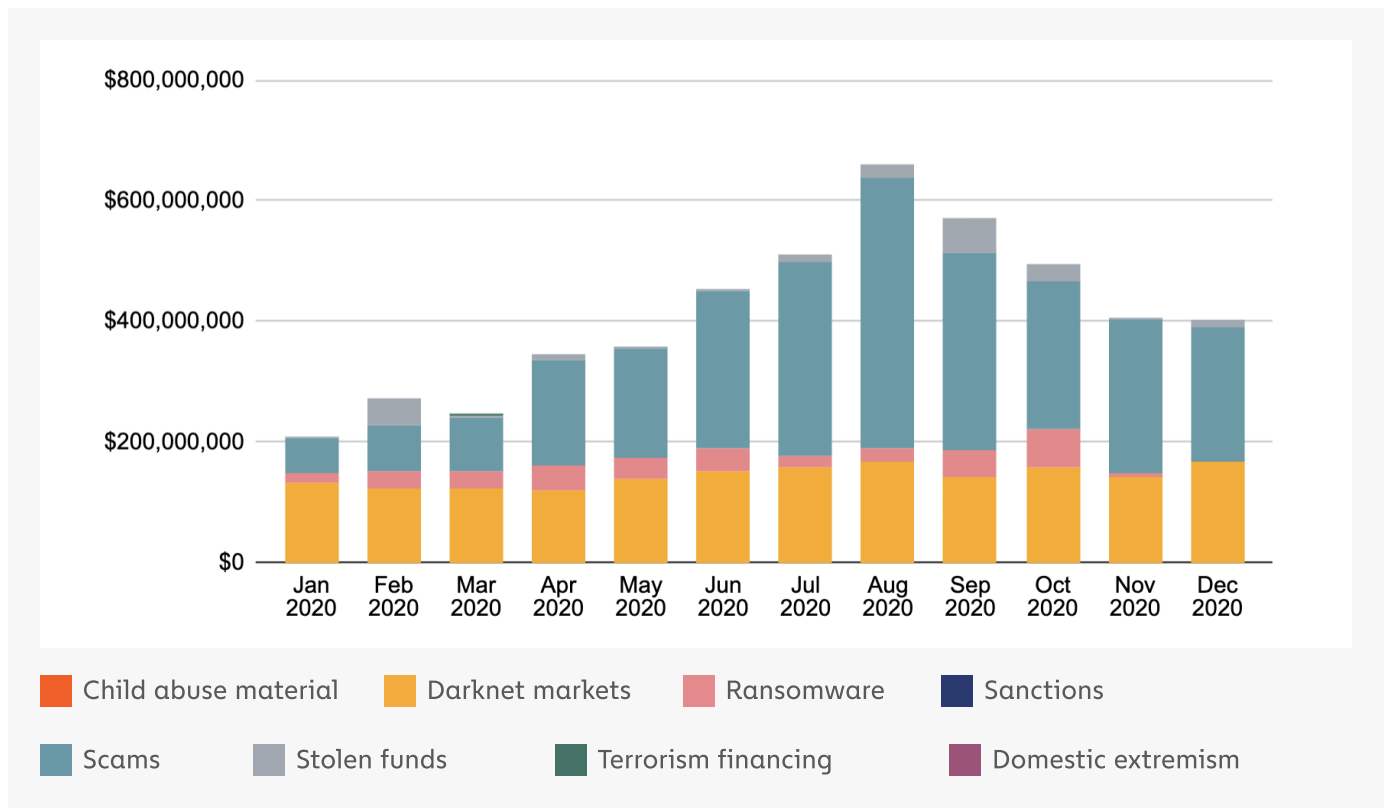
Total cryptocurrency value received by illicit entities | 2017 - 2020





The graph above shows which crime types received the most cryptocurrency in aggregate from 2017 through 2020. Note that this graph differs from the one above it in that it only tracks cryptocurrency received, which we generally associate with criminal revenue, rather than cryptocurrency sent from illicit addresses, which we generally associate with money laundering. The graph below shows the monthly amount received by different types of criminal entities on a monthly basis throughout the year.

Total cryptocurrency value received by illicit entities | 2020

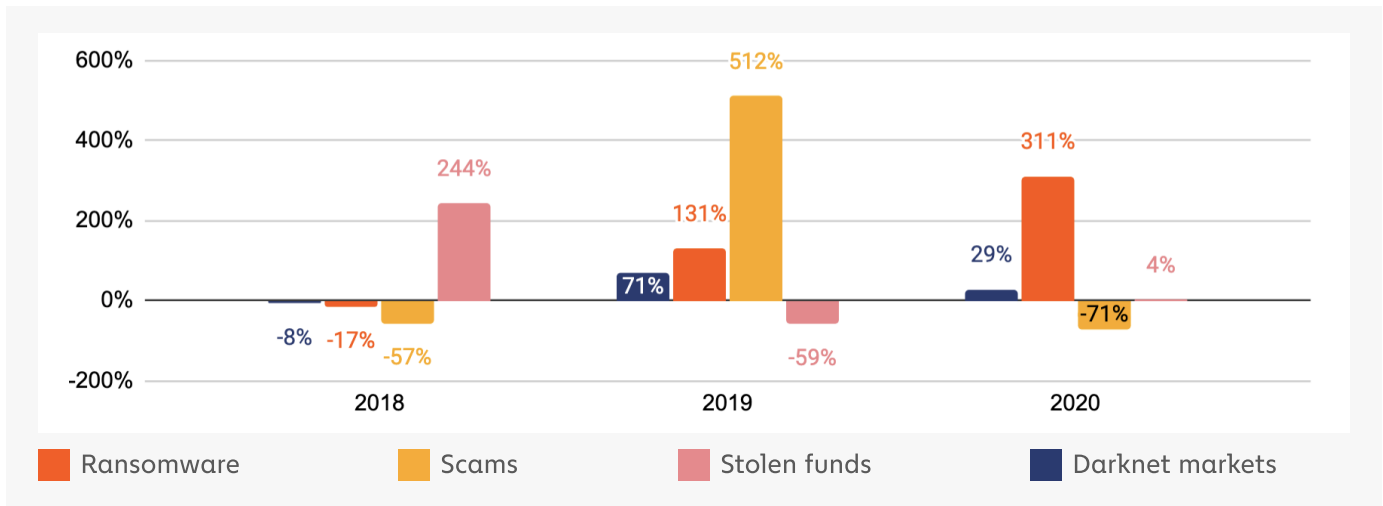


As was the case in 2019, scams made up the majority of all cryptocurrency-related crime, at 54% of illicit activity, representing roughly \$2.6 billion worth of cryptocurrency received. However, both the raw value and share of all criminal activity represented by scams is much smaller than in 2019, as there were no scams in 2020 comparable to those like the enormous [PlusToken Ponzi scheme](#), which took in over \$2 billion from millions of victims. Darknet markets were once again the second-largest crime category, accounting for \$1.7 billion worth of cryptocurrency activity, up from \$1.3 billion in 2019.

However, the big story for cryptocurrency-based crime in 2020 is ransomware. That may sound counterintuitive, as ransomware accounted for just 7% of all funds received by criminal addresses at just under \$350 million worth of cryptocurrency. But that figure represents a 311% increase over 2019. No other category of cryptocurrency-based crime rose so dramatically in 2020, as Covid-prompted work-from-home measures opened up new vulnerabilities for many organizations.



Crime categories by percentage increase in cryptocurrency received, | 2018 - 2020



Keep in mind that ransomware estimates should always be considered lower bounds due to underreporting. The 2020 figure for total ransomware payments will likely grow as we identify more addresses associated with different strains, particularly in the later months of the year. Looking beyond the numbers, we also must note that ransomware is uniquely destructive in that attacks can cripple local governments and businesses for weeks, including several hospitals last year in the midst of the pandemic. When we consider the total economic losses not just from payments, but from businesses and governments being taken offline in attacks, some experts estimate that ransomware cost \$20 billion in economic losses in 2020.

In this report, we'll delve into not just the data on cryptocurrency-based crime, but the story behind the numbers as well. We'll analyze multiple trends, including:

- Why the ransomware ecosystem may be smaller than it appears at first glance, and what that means for law enforcement
- How a small group of shady cryptocurrency services, mostly operating on top of large exchanges, conduct most of the money laundering that cybercriminals rely on to make cryptocurrency-based crime profitable
- DeFi platforms' unique vulnerability to hacking, as well as how cybercriminals such as those of the North Korea-affiliated Lazarus Group utilize DeFi platforms for money laundering
- Why so many darknet markets went offline in 2020
- And more!

By understanding these trends, law enforcement, regulators, and the private sector can work together to ensure cryptocurrency-based crime continues to fall. Thank you for reading, and keep in mind that you can reach out to Chainalysis with any questions at contact@chainalysis.com.



Money Laundering

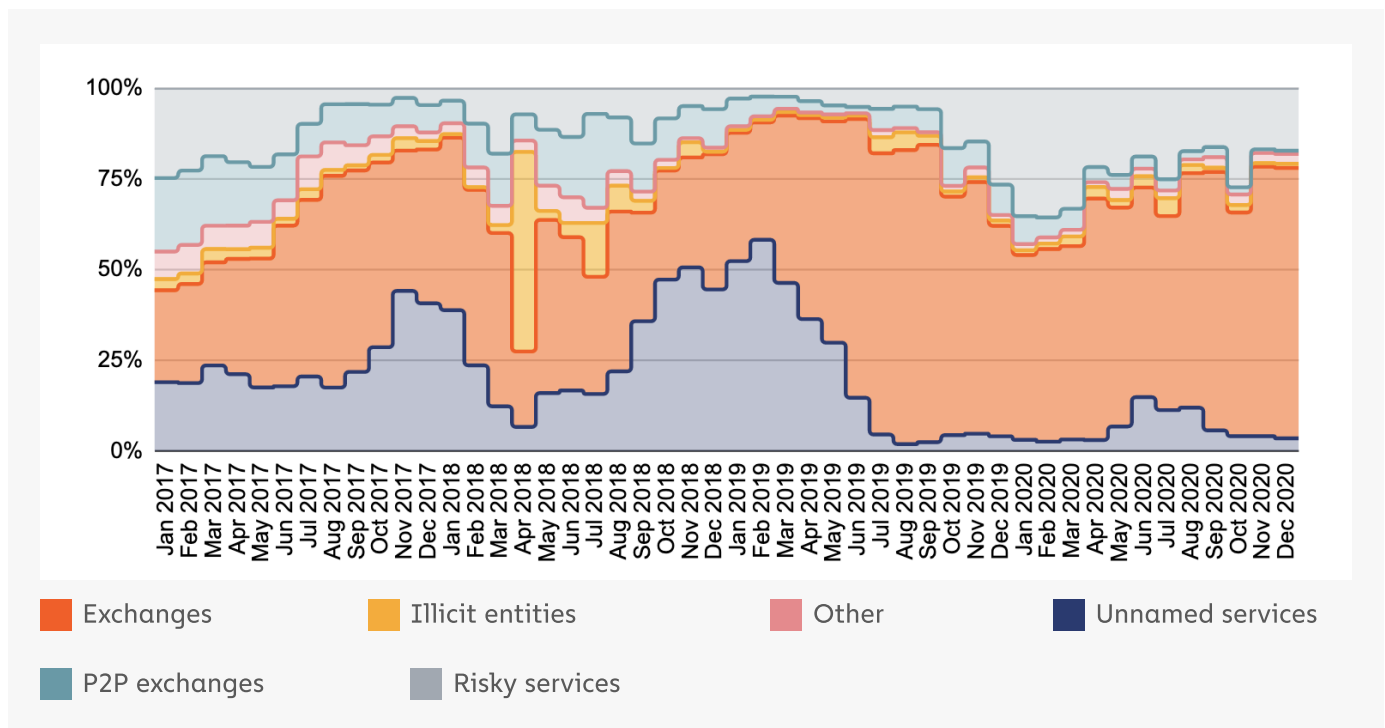


270 Service Deposit Addresses Drive 55% of Money Laundering in Cryptocurrency

Money laundering is the key to cryptocurrency-based crime. The primary goals of cybercriminals who steal cryptocurrency, or accept it as payment for illicit goods, are to obfuscate the source of their funds and convert their cryptocurrency into cash so that it can be spent or kept in a bank. Of course, thanks to the efforts of law enforcement and compliance professionals around the world, cybercriminals can't simply send their ill-gotten cryptocurrency to an exchange and cash out as a normal user would. Instead, they rely on a surprisingly small group of service providers to liquidate their crypto assets. Some of these providers specialize in money laundering services while others are simply large cryptocurrency services and money services businesses (MSBs) with lax compliance programs. Investigators could significantly damage cybercriminals' ability to convert cryptocurrency into cash by going after these money laundering service providers, thereby reducing the incentives for cybercriminals to use cryptocurrency in the first place.

Who are these money laundering service providers? First, let's look at the services that have received funds from criminal sources over the last few years.

Destination of all cryptocurrency sent from illicit addresses, monthly | Jan '17 - Dec '20



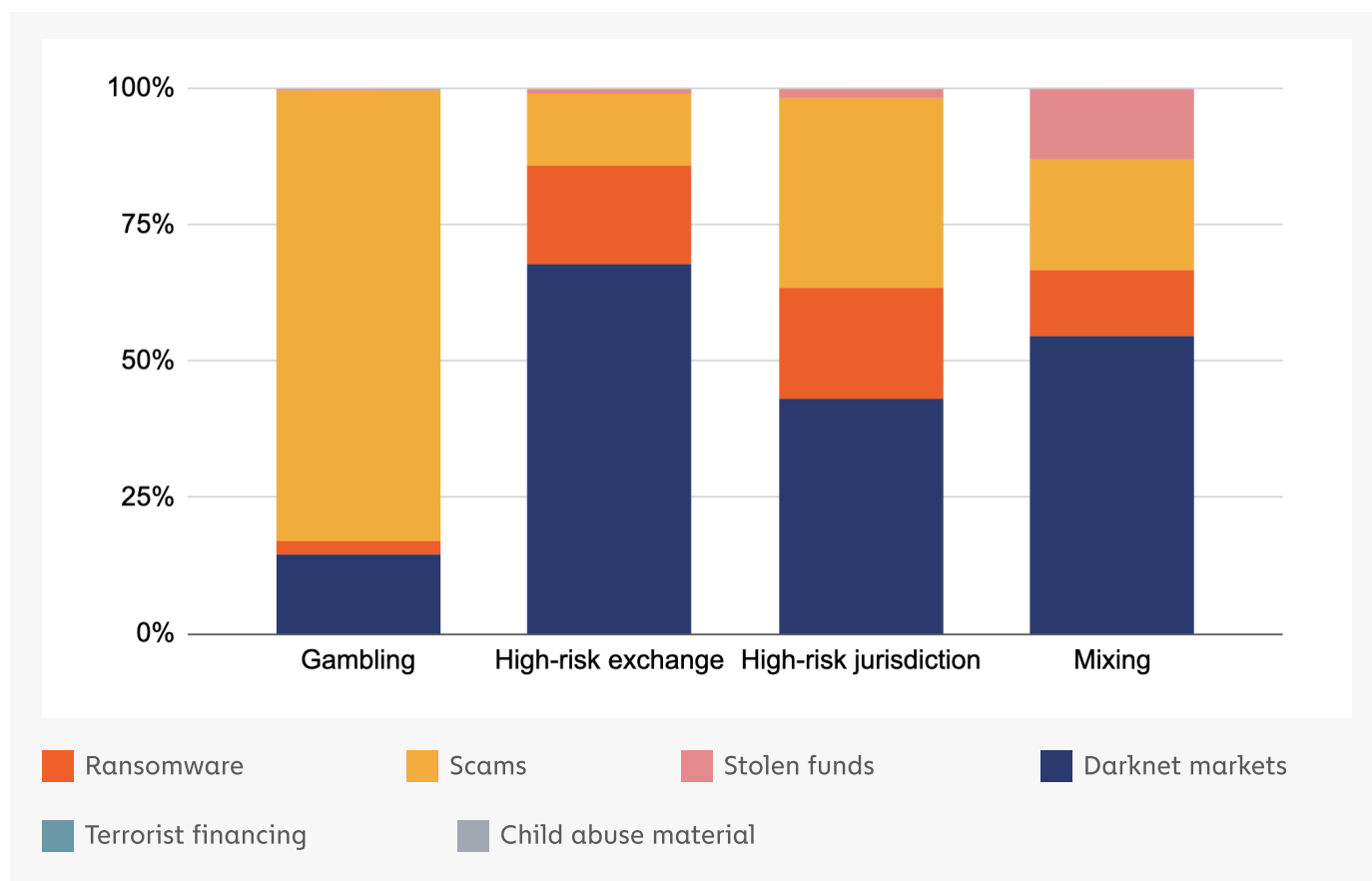
Currencies included: BAT ,BCH, BTC, ETH, LTC, MKR, OMG, PAX, TUSD, USDC, USDT



Historically, mainstream exchanges have been the primary destination of illicit cryptocurrency, and that didn't change in 2020. In fact, the share of all illicit cryptocurrency received by exchanges grew slightly in 2020.

We also see significant volume moving from illicit addresses to services we categorize as “risky,” including high-risk exchanges, gambling platforms, mixers, and services headquartered in high-risk jurisdictions. Interesting trends arise when we look at the specific risky services receiving funds from different types of cryptocurrency-based crime.

Risky services receiving illicit funds by crime type | 2020



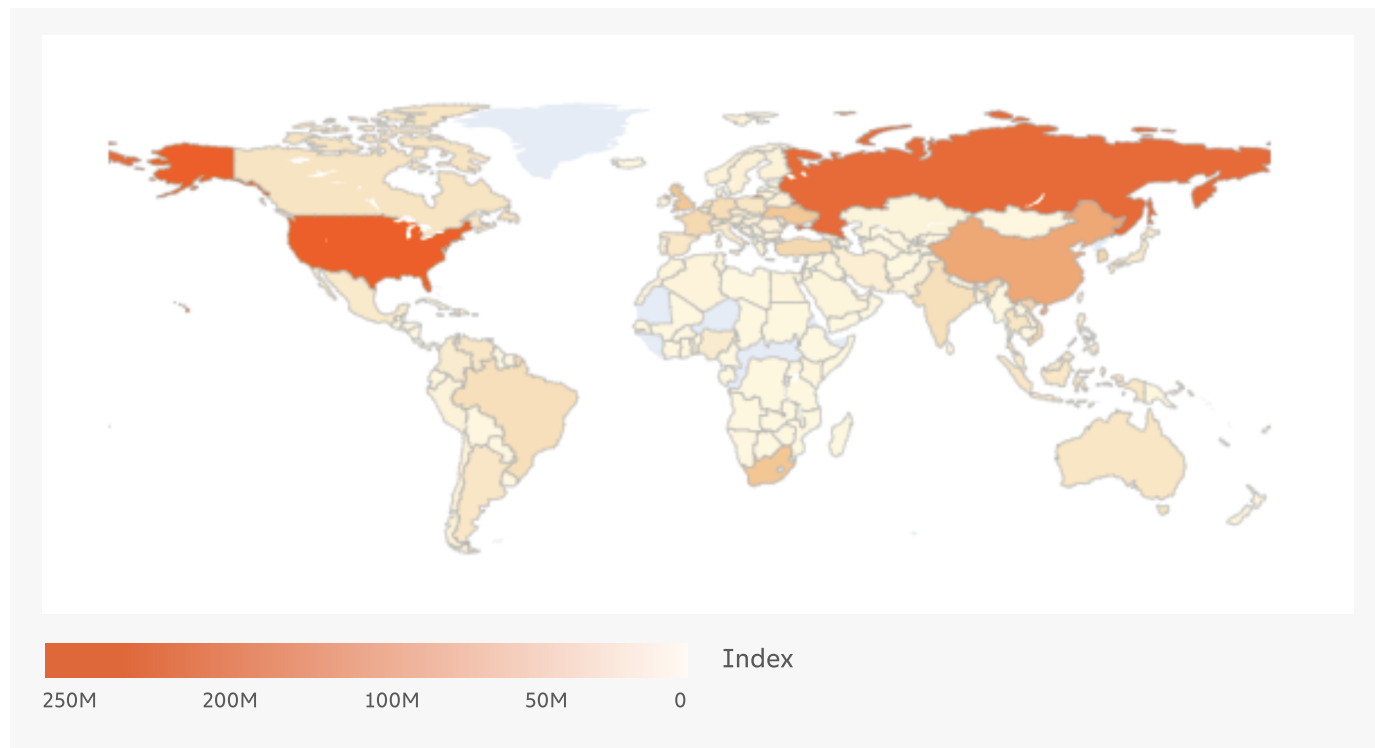
Currencies included: BCH, BTC, ETH, LTC, OMG, PAX, USDC, USDT

The most popular risky service categories for money laundering are similar for each crime category, with scams being the biggest exception. Scammers are much more likely than other cybercriminals to move funds to gambling platforms — a trend that began in 2020 and is best exemplified by the Mirror Trading International scam we cover elsewhere in this report — and to services headquartered in high-risk jurisdictions.

We can also see interesting trends when we look at money laundering through a geographic lens.



Destination of Funds Leaving Illicit Services | 2020



Currencies included: BAT, BCH, BTC, ETH, LTC, MKR, OMG, PAX, TUSD, USDC, USDT

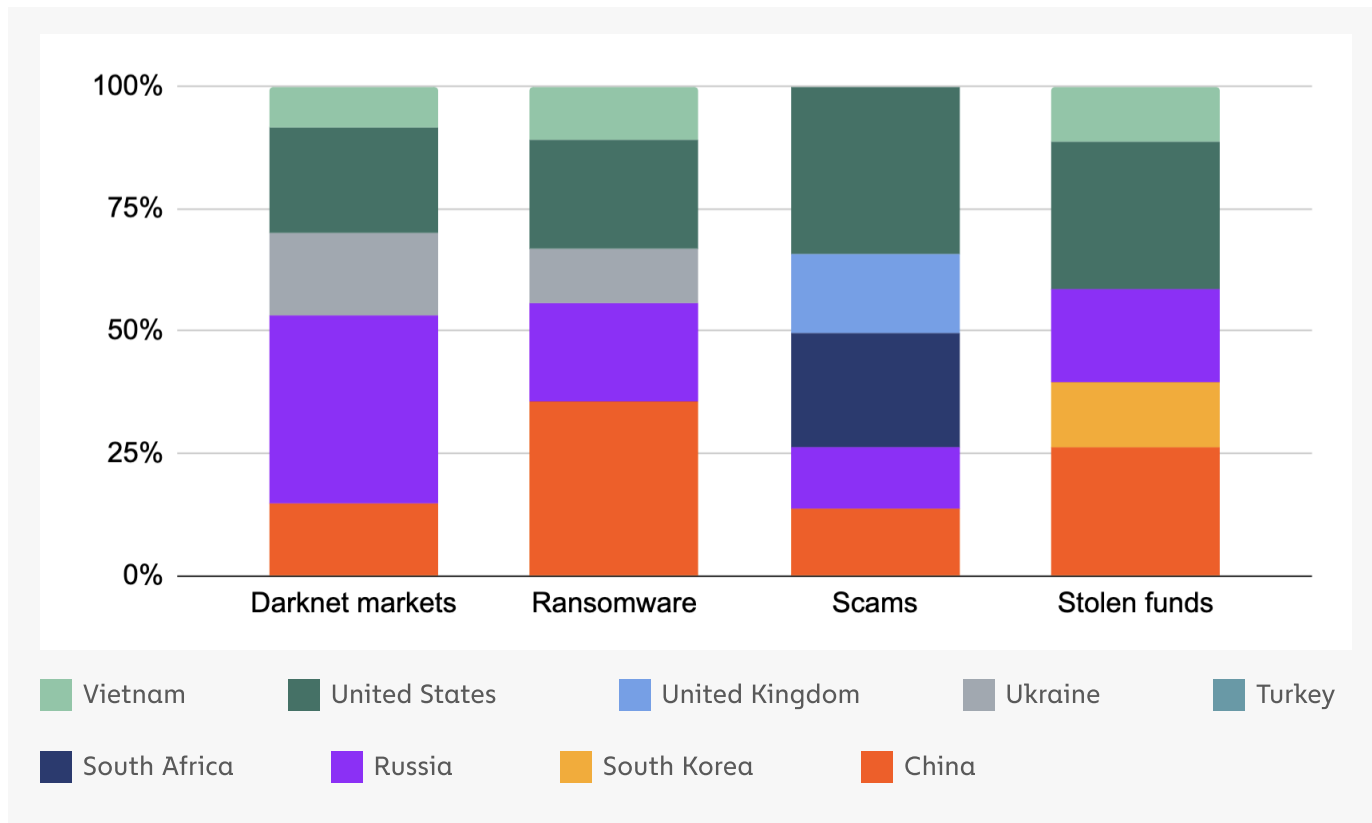
The following countries receive the highest volume of cryptocurrency from illicit addresses, based on the breakdowns of the locations of the users for the services receiving those funds:

- United States
- Russia
- China
- South Africa
- United Kingdom
- Ukraine
- South Korea
- Vietnam
- Turkey
- France



However, patterns emerge when we look at the geographic destination of funds by crime category:

Top 5 countries estimated to receive illicit funds by crime type | 2020



Note: Country estimations based on web traffic of services receiving illicit funds

The first trend that stands out is Russia's receipt of a disproportionately large share of darknet market funds, which is mostly due to Hydra. Hydra is the world's largest darknet market by revenue, and exclusively serves Russia and other Russian-speaking countries in Eastern Europe. China also stands out for receiving a disproportionate share of funds sent from addresses associated with stolen funds and ransomware. Some of this may come from cryptocurrency theft and ransomware activity associated with Lazarus Group, a cybercriminal syndicate linked to the North Korean government. A recent [Department of Justice complaint](#) identified two Chinese nationals who worked with Lazarus Group operatives to launder cryptocurrency that the group stole from exchanges. Other China-based cryptocurrency users could be engaged in similar activity. Finally, the United States is slightly overrepresented in funds received from addresses associated with scams and stolen funds.



Who are the money laundering service providers?

As we discuss above, most funds sent from illicit addresses make their way to deposit addresses at mainstream exchanges or at services we categorize as "risky," including high-risk exchanges (e.g. exchanges with lax or nonexistent compliance programs), mixers, gambling platforms, or services headquartered in high-risk jurisdictions. Some of the deposit addresses receiving illicit funds are likely controlled by the cybercriminals sending the funds in the first place. But we know from our law enforcement partners and our own investigations that many of these deposit addresses belong to third-party services who, sometimes explicitly or implicitly, provide money laundering services to cybercriminals.

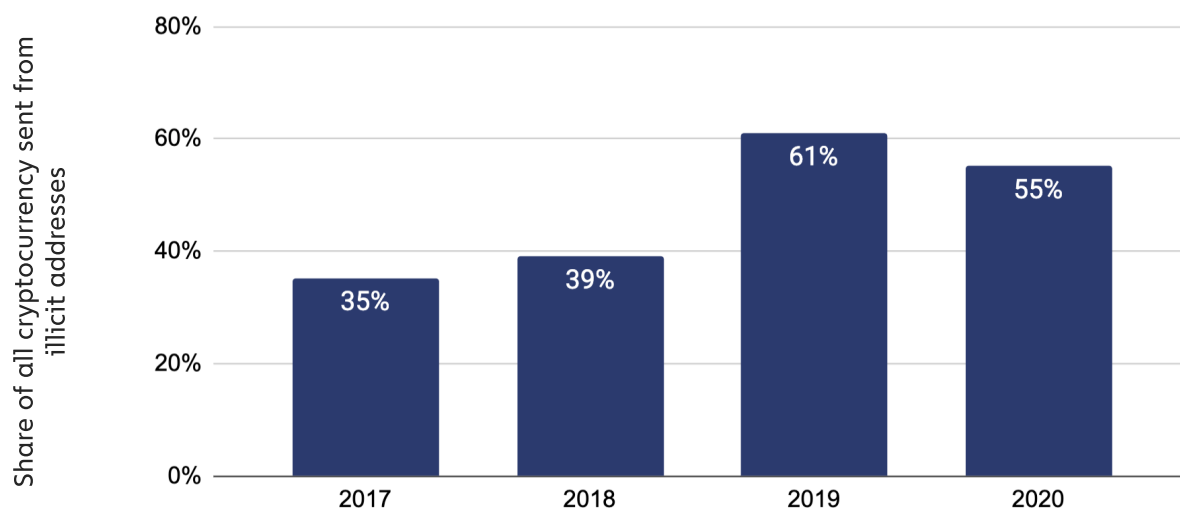
These third-party services largely fall into a broad category called "nested services." Nested services operate within one or more larger exchanges, tapping into those exchanges' liquidity and trading pairs. From a blockchain analysis standpoint, this means that by default, nested services' transactions will show up as having been conducted on the underlying platform that hosts the nested service. Common examples of nested services include Over the Counter (OTC) brokers and instant exchangers. There's 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. 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.

Below, we'll share what we know about the deposit addresses facilitating money laundering, starting with the services hosting them.

Cryptocurrency sent from illicit addresses tends to wind up at just a few services. Below, we show the share of all illicit funds going to the five services receiving the most illicit funds each year since 2017, both overall and broken down by crime type. The top two services receiving illicit funds have remained constant over the three years we studied, with some change in the third, fourth, and fifth spots. Together, the top two take in more than the other three do combined in any given year. Overall in 2020, these top five services received 55% of all funds moved from illicit addresses.

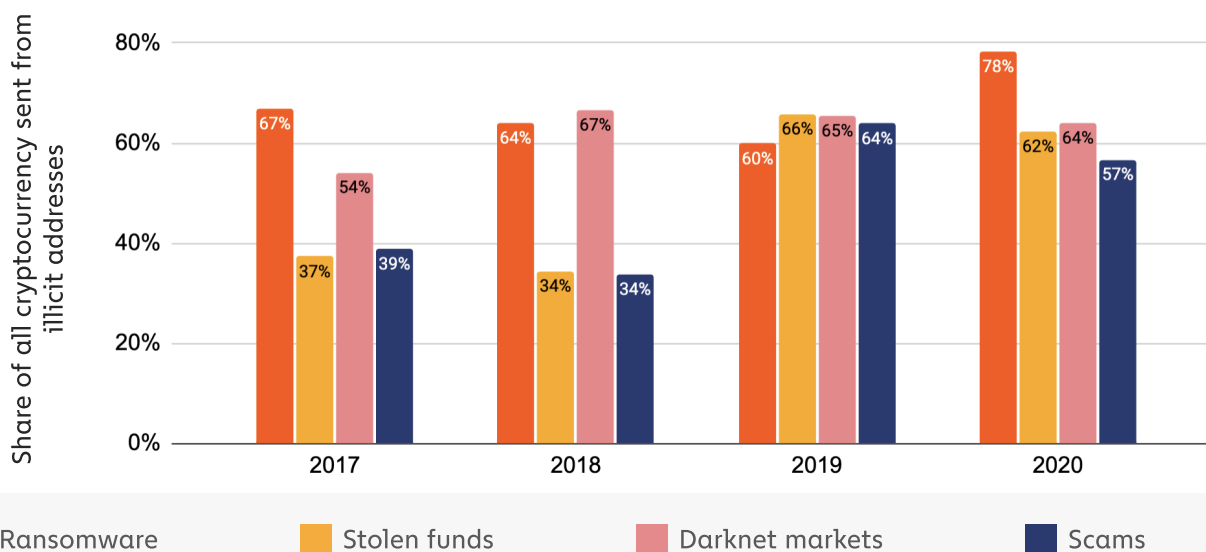


Share of all illicit funds going to top 5 illicit fund receiving services, | 2017 - 2020



Currencies included: BAT, BCH, BTC, ETH, LTC, MKR, OMG, PAX, TUSD, USDC, USDT

Share of all illicit funds going to top 5 illicit fund receiving services by crime type | 2017 - 2020



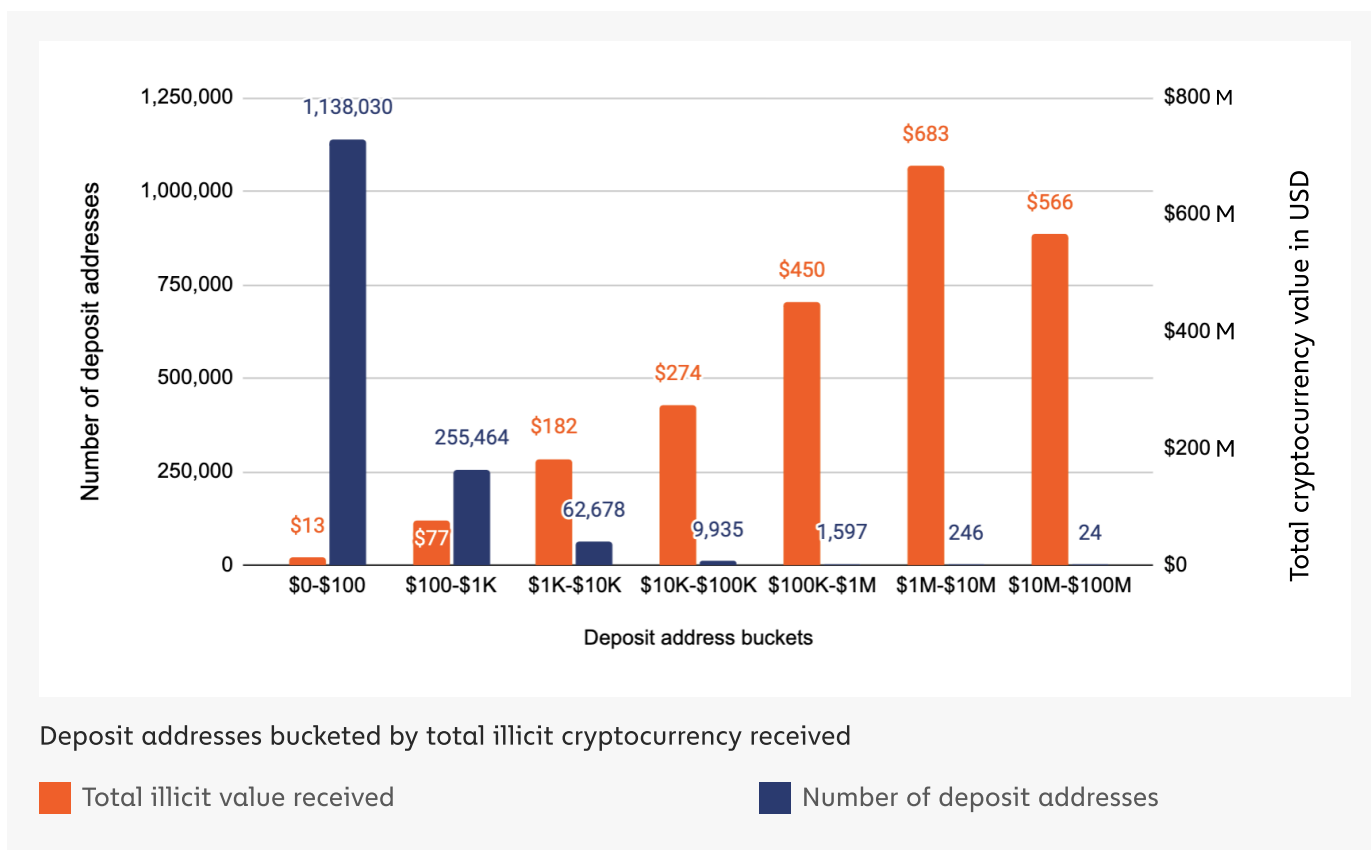
Currencies included: BAT, BCH, BTC, ETH, LTC, MKR, OMG, PAX, TUSD, USDC, USDT



Notably, addresses associated with ransomware have the highest share of sending activity concentrated to the top five services, at 78% in 2020.

But what happens if we go one level deeper from the services and look at the individual deposit addresses? In the graph below, we look at all service deposit addresses that received any illicit funds in 2020, broken down by the range of illicit funds received.

All illicit cryptocurrency received by service deposit addresses | 2020



Currencies included: BTC

How to read this graph: This graph shows service deposit addresses bucketed by how much total illicit cryptocurrency value each address received individually in 2020. Each blue bar represents the number of deposit addresses in the bucket, while each orange bar represents the total illicit cryptocurrency value received by all deposit addresses in the bucket. Using the first bucket as an example, we see that 1,138,030 deposit addresses received between \$0 and \$100 worth of illicit cryptocurrency, and together all of those deposit addresses received a total of \$13 million worth of illicit cryptocurrency.

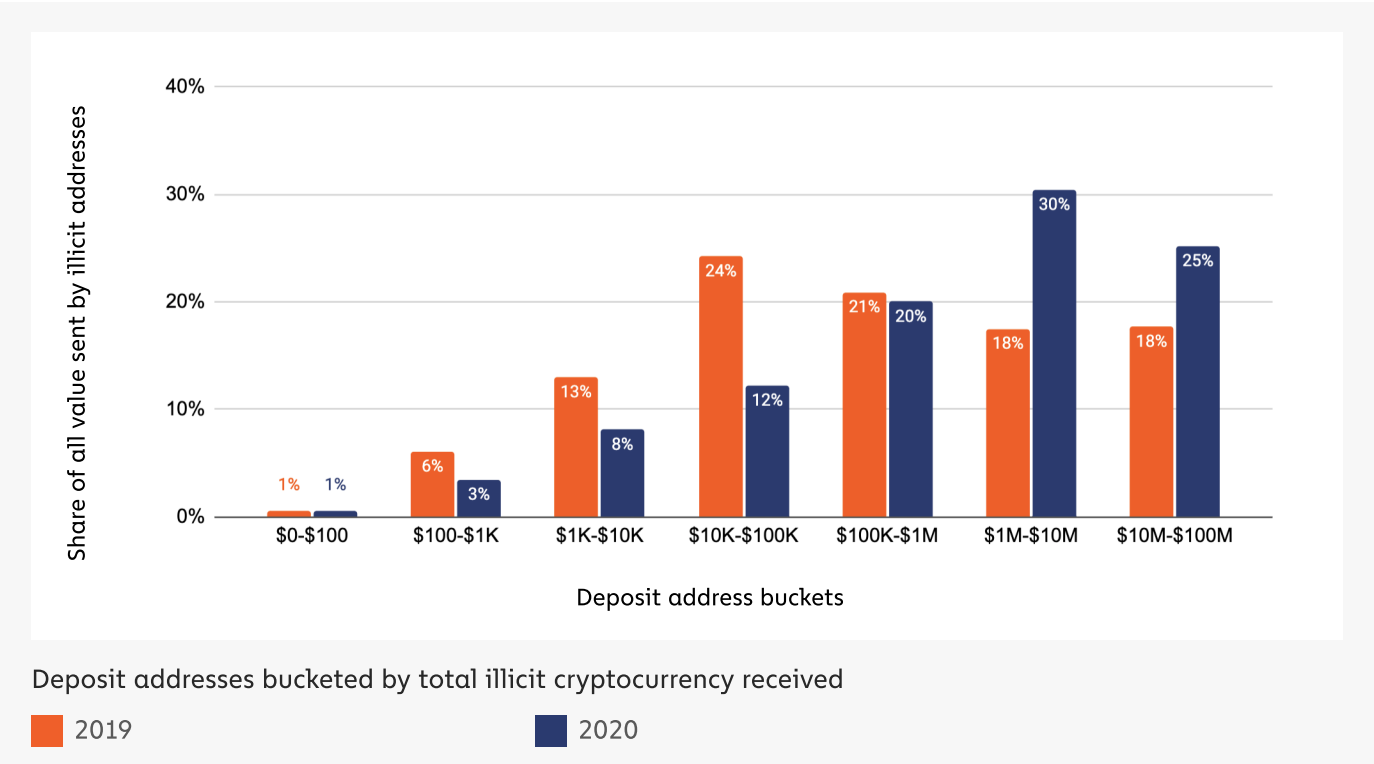
Money laundering activity is even more concentrated at the deposit address level. In fact, the data above shows that a group of **just 1,867 deposit addresses received 75% of all cryptocurrency value sent from illicit addresses in 2020. A smaller group of 270 deposit**



addresses received 55%. Thinking in terms of raw value rather than percentages, those 270 addresses collectively received \$1.3 billion worth of illicit cryptocurrency in 2020, and a smaller group of just 24 received over \$500 million worth of illicit cryptocurrency in 2020.

This level of concentration is greater than in 2019. Below, we look at how the shares of all illicit cryptocurrency received by deposit addresses in each of the buckets shown above changed from 2019 to 2020.

Share of all illicit value received by deposit addresses in each bucket, 2019 vs. 2020



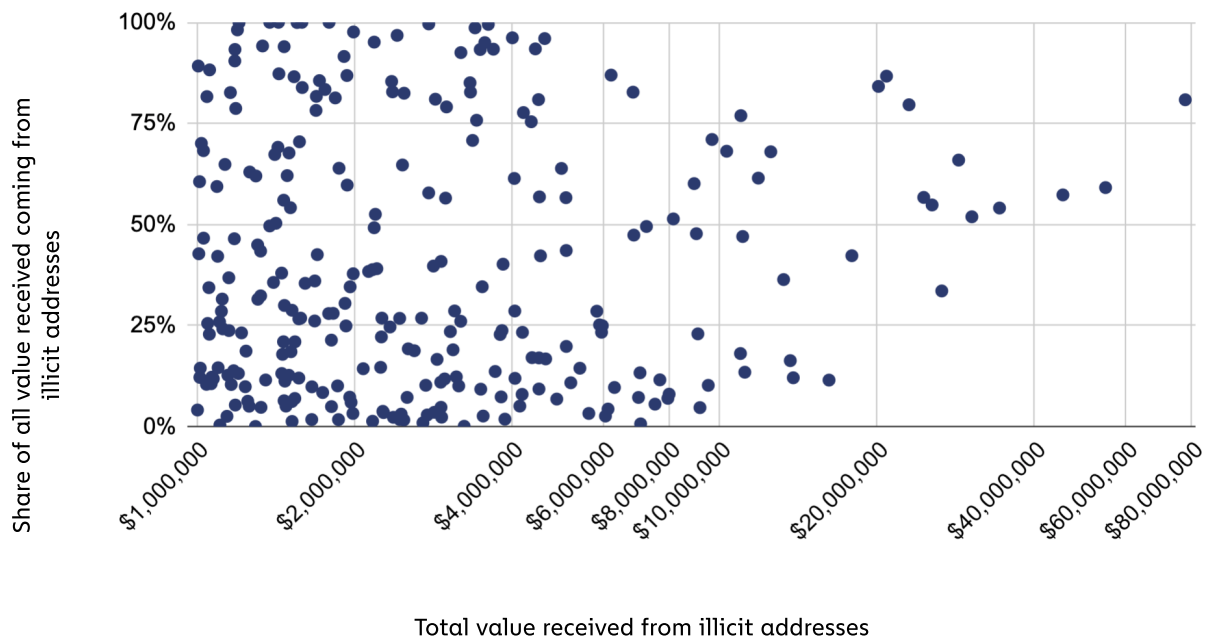
Currencies included: BTC

In particular, we see a much greater share of illicit cryptocurrency going to addresses taking in between \$1 million and \$100 million worth of cryptocurrency per year.

We believe the growing concentration of deposit addresses receiving illicit cryptocurrency reflects cybercriminals' increasing reliance on a small group of OTC brokers and other nested services specializing in money laundering. In order to investigate further, we decided to look more closely at the 270 deposit addresses that received more than \$1 million worth of cryptocurrency from illicit addresses in 2020. In the scatter chart below, we plot those addresses based on the total amount they've received from illicit addresses, versus the share those illicit funds make up of the addresses' total amount received.



Deposit addresses receiving over \$1M worth of illicit cryptocurrency in 2020: Total illicit value received vs. illicit share of all value received



Currencies included: BTC

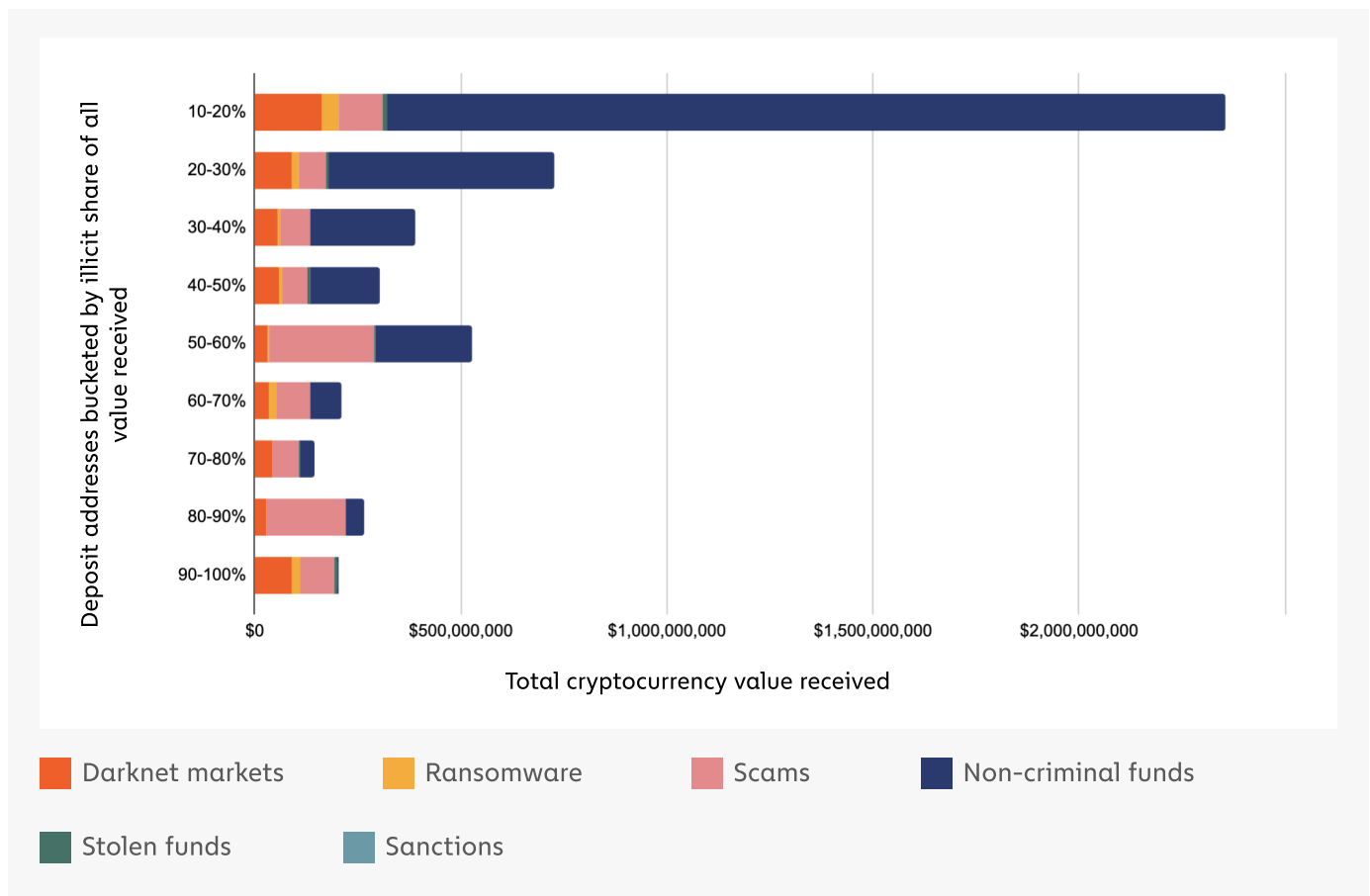
An interesting trend emerges when we look at the 270 deposit addresses that facilitate the most money laundering shown above. Though they individually and collectively may facilitate a great deal of money laundering, legitimate activity also makes up a significant share of total transaction volume for many of these deposit addresses, especially those that received less than \$25 million in cryptocurrency from illicit addresses. In fact, illicit addresses account for under 10% of total cryptocurrency received for many of these addresses, even more so below the \$10 million mark. This suggests that the money laundering those addresses facilitate could simply be inadvertent and due to shortcomings in the compliance programs of the nested services controlling them.

However, we see no such evidence for any of the deposit addresses receiving over \$25 million worth of cryptocurrency from illicit addresses. All of those deposit addresses receive at least 34% of their total funds from illicit sources, with that figure rising above 50% for most of them. It would be difficult to believe that these services are receiving such a high percentage of funds from illicit addresses by accident — those of them that represent nested services could likely not survive as businesses without those funds — so we characterize those addresses as primarily serving cybercriminals.



Below, we expand our set of deposit addresses to include all that received any funds from illicit addresses in 2020, and break them down by the share of all funds they receive that comes from illicit addresses. We see that the wallets receiving the most illicit funds overall are those for whom illicit funds make up the biggest percentage of all funds received. In other words, the small group of actors laundering the most money seem to specialize in it.

Total cryptocurrency value received by deposit addresses grouped by illicit share of all funds received | 2020



Currencies included: BTC

55% of all illicit funds moving to services end up at deposit addresses for which illicit addresses supply 50% or more of all funds. That figure rises to 71% for deposit addresses with 30% or more of all funds received coming from illicit addresses. In other words, a significant share of money laundering in cryptocurrency isn't flying under the radar at big services who can't sift through transactions to spot it, but is being actively facilitated by nested services for whom money laundering is a key part of the business model. **Law enforcement could significantly hamper cybercriminals' ability to convert cryptocurrency into cash by identifying and prosecuting the owners of these deposit addresses.** In addition, this shows that the services hosting these deposit addresses, most of which belong to nested services, need to be more diligent in their transaction monitoring. They too could make the cryptocurrency ecosystem safer by cracking down on the worst offenders.



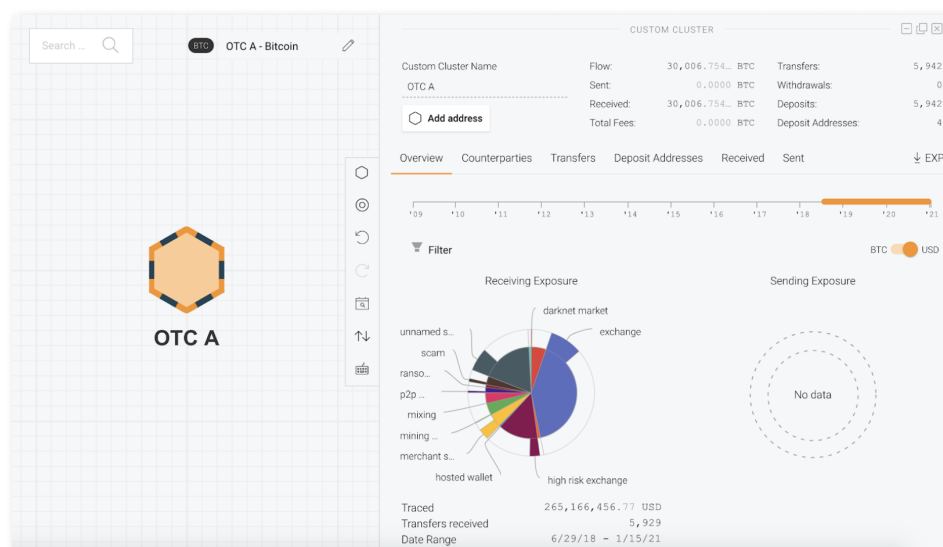
We should also note that even the non-illicit share of funds received for some of these addresses should be treated with suspicion, as they could represent money laundering associated with offline criminal activity — in other words, bad actors criminally-obtained exchanging fiat money for cryptocurrency in an effort to hide it. We'll explore this element of cryptocurrency money laundering in our case studies at the end of this section.

Overall, what the data makes clear is that most illicit funds travel to service deposit addresses for whom money laundering makes up a huge portion of their activity, to the point that many of them appear to have no other purpose. A smaller but still significant portion also goes to deposit addresses doing a high volume of legitimate transactions, which could allow the illicit activity to fly under the radar, reinforcing the need for compliance professionals and investigators to stringently assess all deposit addresses — especially those of nested services.

Case study: Russia-based money laundering ring helps ransomware attackers and darknet market vendors cash out

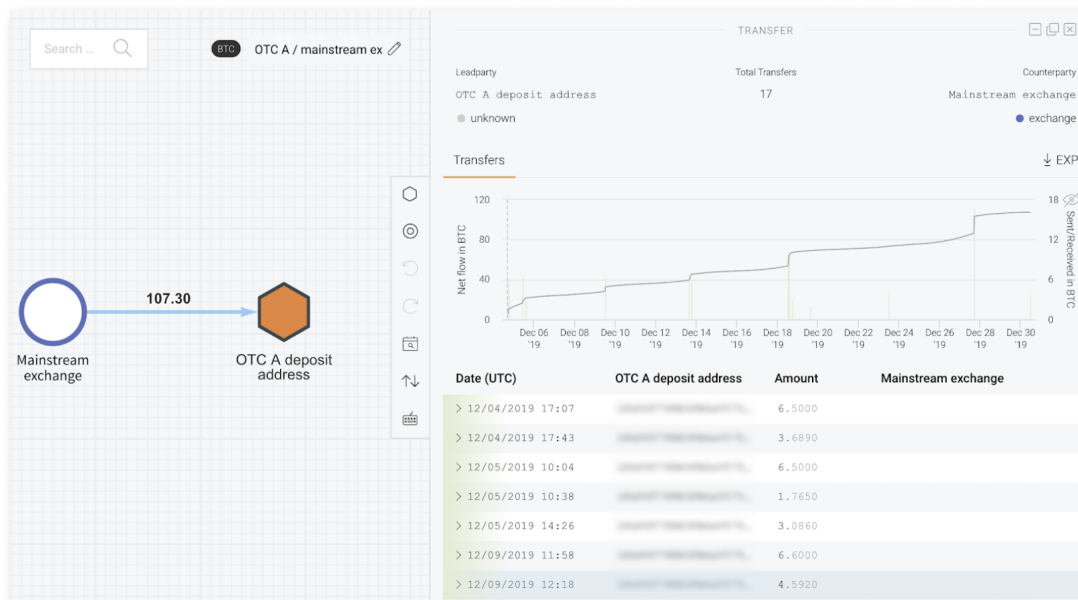
By examining the activity of deposit addresses with significant exposure to illicit addresses, we can learn more about how cybercriminals launder funds through different services, often switching between cryptocurrencies. Below, we'll break down the activity of what appears to be a money laundering ring helping cybercriminals convert large sums of cryptocurrency into cash.

This money laundering ring involves multiple services. The first is a large, Russia-based OTC broker that nests primarily at two highly popular exchanges, which we'll refer to as **OTC A**. We've attributed seven deposit addresses at those two exchanges to OTC A, three of which are within the group of 270 that received more than \$1 million in illicit funds in 2020. Below, we break down OTC A's Bitcoin received, much of which comes from illicit addresses.

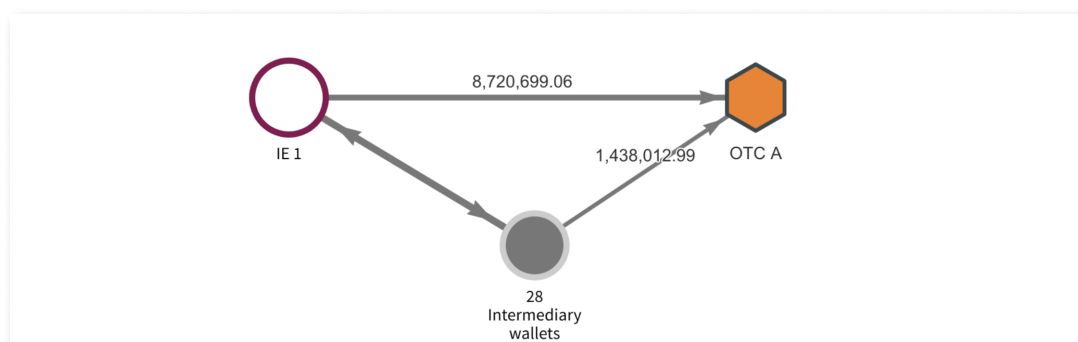




OTC A has received over \$265 million worth of cryptocurrency since becoming active in 2018. More than \$2 million worth has come from ransomware strains such as Maze and Ryuk. Additionally, it's received \$13.9 million worth of cryptocurrency from darknet markets – primarily Hydra – and \$8.1 million worth of cryptocurrency from several scams. Overall, 9.29% of all Bitcoin received by OTC A comes from illicit addresses. OTC A also receives substantial funds without previous transaction history from other exchanges, meaning the funds were initially deposited in fiat form. We believe some of these may be linked to off-chain crime, meaning crime whose proceeds aren't initially derived in cryptocurrency. Below, we see an example of some of those funds – OTC A has received over 107 Bitcoin from a mainstream exchange that was converted directly from fiat.



It's possible that OTC A helps cybercriminals convert at least some of the Bitcoin they send into cash. However, our data also shows that OTC A makes significant transactions in Tether ERC-20 tokens (USDT_ETH). More specifically, it exchanges a good deal of USDT_ETH with another Russia-based service, this one an instant exchanger. We'll refer to it as Instant Exchanger 1, or IE 1. IE 1 allows users to exchange between cryptocurrencies like Bitcoin, Ether, and Tether, and a variety of different electronic fiat currencies powered by e-wallet providers like Perfect Money.





According to Reactor, OTC A has received significant sums of USDT_ETH from IE 1 — \$8.7 million worth directly, and another \$1.4 million through a network of 28 intermediary wallets. We don't know if OTC A sends Tether (or Bitcoin for that matter) to IE 1 — since all of OTC A's deposit addresses are hosted at larger services, it's impossible to trace the cryptocurrency they send. But it's worth noting that the intermediary wallets sitting between OTC A and IE 1 both send and receive large amounts of USDT_ETH to and from IE 1. Based on that, we believe it's possible that OTC A also sends large sums of USDT_ETH to IE 1 on behalf of cybercriminal clients, allowing them to cash out at IE 1.

This is just one example of how funds can be moved from illicit addresses to OTC brokers and other types of nested services.

Case study: Drug ring operating in the UK and Australia Shows How Cryptocurrency Can Be Used to Launder the Proceeds of Offline Crime

Nearly all of the illicit activity we cover in this report consists of cybercrime we'll refer to as "cryptocurrency native", meaning crime that is practically dependent on cryptocurrency or inherently intertwined with it. Take darknet markets, for example. Darknet markets as we know them run entirely on cryptocurrency, with millions of dollars' worth flowing through their centralized networks of wallets every day. Since these services actively solicit new customers online, it's not all that difficult for us to identify their cryptocurrency addresses and track their transaction activity.

But many investigators have wondered how often criminals engaged in traditional, non-cryptocurrency native crime — traditional drug trafficking, for example — are laundering their ill-gotten funds by converting them into cryptocurrency and sending them around the world. In these cases, the funds on-ramp into cryptocurrency directly from fiat rather than move from known illicit addresses, so it's harder to both investigate this activity in individual cases or to size it in the aggregate.

However, we do know that it's happening. Below, we'll share a case study of how a drug trafficking ring operating in the UK and Australia incorporated cryptocurrency into its money laundering strategy.



How the Harrod's drug trafficking ring used cryptocurrency

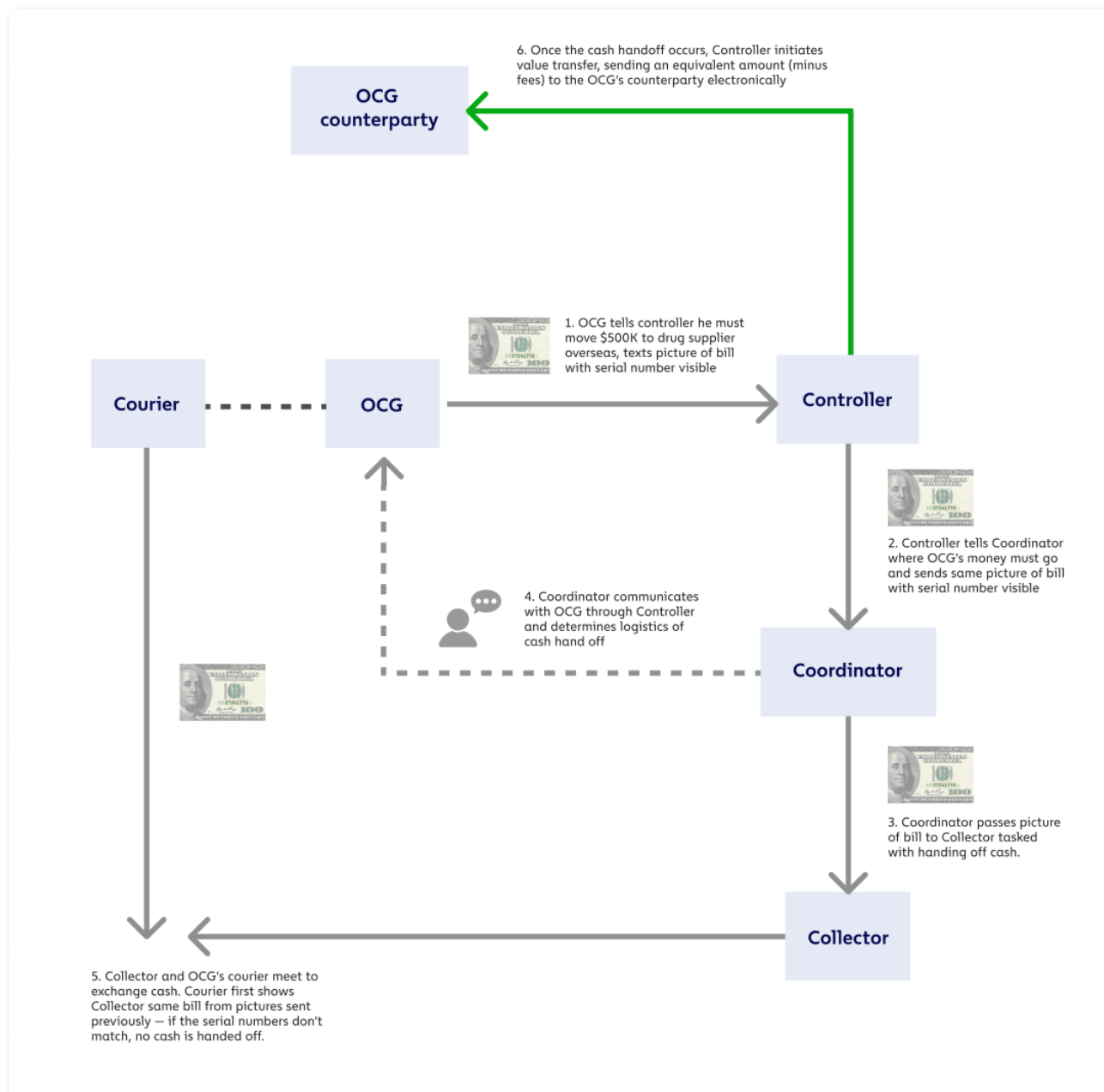
In 2019, police arrested multiple members of a drug trafficking ring operating in the UK and Australia. Notably, the traffickers in this case were inserting cocaine into items at the [department store Harrod's](#), then having the unwitting staff send those items to addresses in Australia where co-conspirators could collect them.

However, our focus is on the methods they used to send drug money overseas to suppliers. The Harrod's ring followed a common strategy that many criminal enterprises use:

1. The **organized crime group (OCG)** contacts a **controller** who is in charge of a money laundering operation, and tells the controller how much illicit cash they need to move, the **counterparty** receiving it, and where that counterparty is located. In the Harrod's case, the OCG was a drug trafficker in the UK who would tell the controller they need to move funds — usually a sum in the hundreds of thousands — to their drug supplier.
2. The controller will then contact one of the many **coordinators** they work with whose job it is to ensure the money gets to the correct counterparty.
3. The OCG will text a picture of a bill to the controller with the serial number visible. The controller will pass this image on to the coordinator, who passes it to the **collector** tasked with physically receiving the cash. (We'll explain why later.)
4. Through the controller, the coordinator will communicate to the OCG the location where the cash will be handed off. The two parties will share other details, such as the make and model of the vehicles the individuals making the exchange will be driving. This is done to limit the risk of the meeting being infiltrated by police.
5. The OCG will then pass the bill from the picture in step 4, along with the cash to be transferred, to a **courier**. The courier then meets the collector at the designated place and time.
6. Upon meeting, the courier will pass the bill from the picture to the collector. The collector then checks to make sure the serial number matches the one in the picture he received. The transaction will not take place if they do not match. This is done to ensure to the collector that the courier, whom he's never met, is the correct person.
7. If the serial numbers match, the courier will hand the full amount of cash to be transferred to the collector.

8. The collector will communicate to the controller that the cash has been handed over. At that point, the controller conducts a **value transfer process**, whereby money is transferred electronically to a coordinator in the OCG counterparty's location. Traditionally, the electronic transfer is done through banks or traditional money services businesses (MSBs).
9. The controller and new coordinator then arrange for the same process described in steps 1-7 to be conducted in reverse in the OCG counterparty's location so that the counterparty receives an equivalent amount of cash – importantly, not the same cash handed over in the OCG's location.

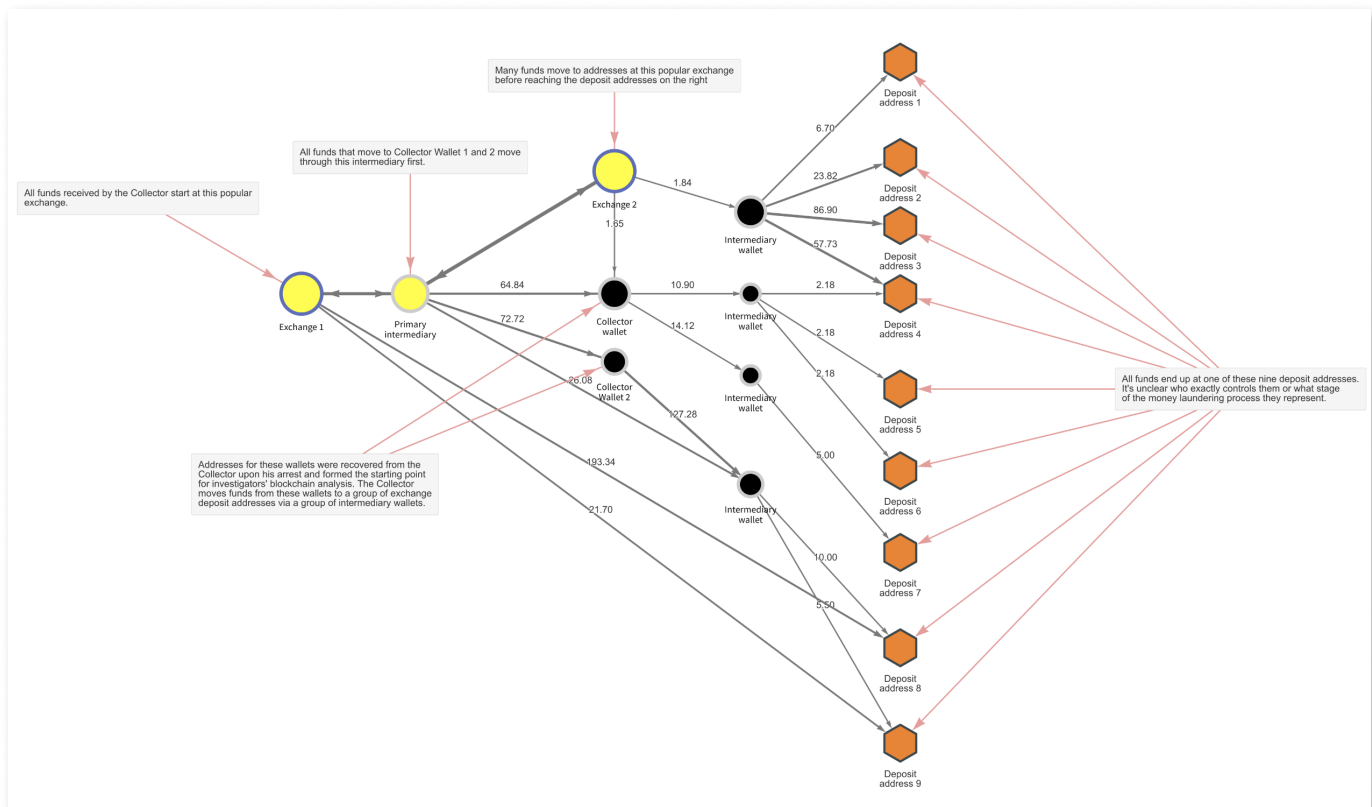
We've condensed these steps in the diagram below:





The Harrod's drug ring followed this exact process, but with one twist: the value transfer process was conducted using cryptocurrency transactions rather than bank or MSB transfers.

Notably, the collectors were the ones responsible for carrying out the cryptocurrency transactions. Police tracking the Harrod's drug ring's activity arrested one of these collectors after a cash handover, recovered the cash, and discovered evidence on his person identifying bill serial numbers described above, as well as a list of several Bitcoin addresses. Below is a Reactor graph showing some of the collector's Bitcoin transactions related to the money laundering ring's activity.



The coordinator on the UK side of the operation fled following the collector's arrest, but returned several months later and was then arrested. Police recovered from him a hardware cryptocurrency wallet, whose transaction history showed £8 million worth of cryptocurrency being moved to a popular exchange within a six-month period. Because these funds entered the cryptocurrency ecosystem as fiat currency, blockchain analysis alone would never allow an investigator or compliance officer to identify them as risky.

The Harrod's drug ring case shows how important it is for law enforcement investigators — even those not responsible for cybercrime — to understand how cryptocurrency and blockchain analysis work.



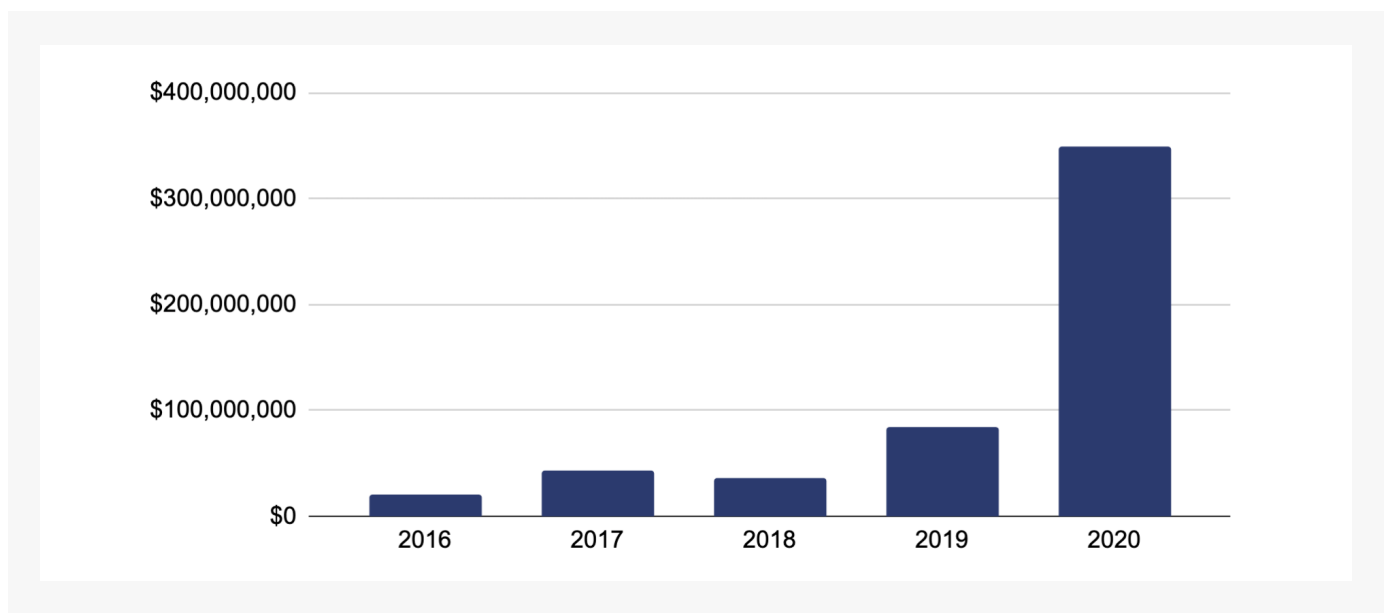
Ransomware



Ransomware Skyrocketed in 2020, But There May Be Fewer Culprits Than You Think

2020 will forever be known as the year of Covid, but when it comes to crypto crime, it's also the year that ransomware exploded.

Total cryptocurrency value received by ransomware addresses per year | 2016 - 2020



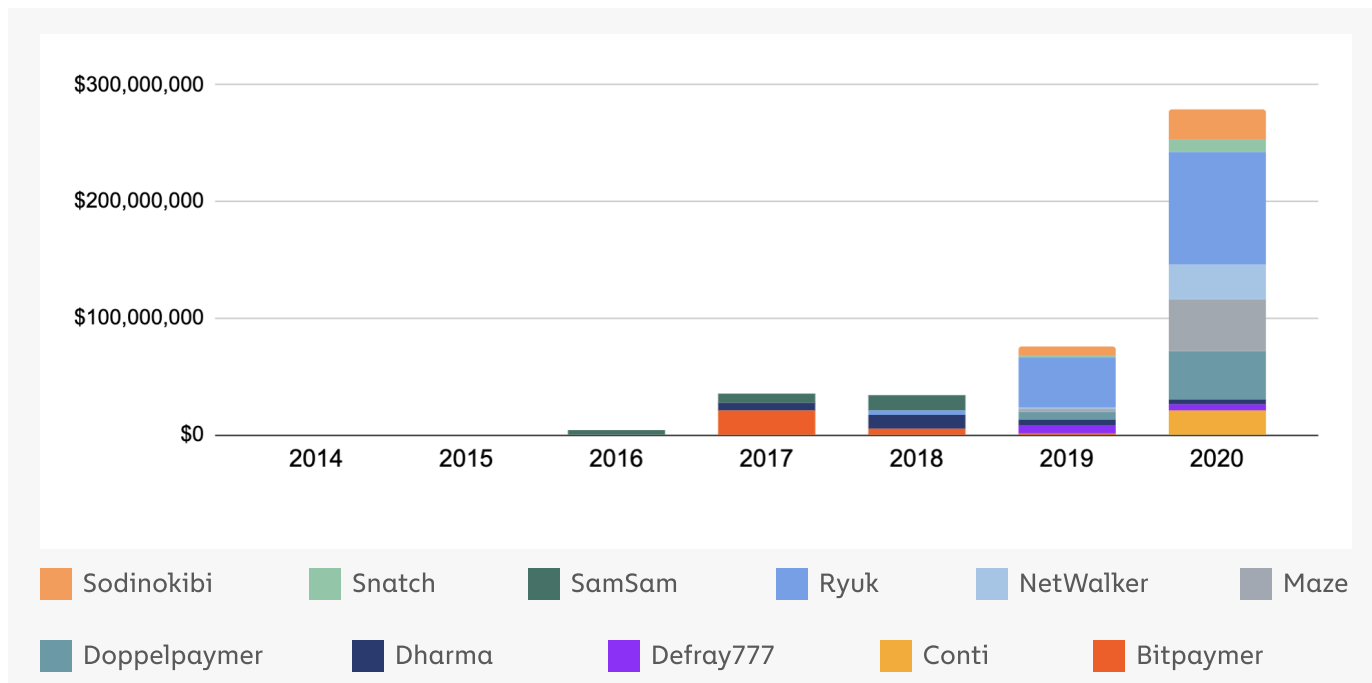
Currencies included: BCH, BTC, ETH, USDT

Blockchain analysis shows that the total amount paid by ransomware victims increased by 311% this year to reach nearly \$350 million worth of cryptocurrency. No other category of cryptocurrency-based crime had a higher growth rate. Keep in mind that this number is a lower bound of the true total, as underreporting means we likely haven't categorized every victim payment address in our datasets.

2020's ransomware increase was driven by a number of new strains taking in large sums from victims, as well as a few pre-existing strains drastically increasing earnings.



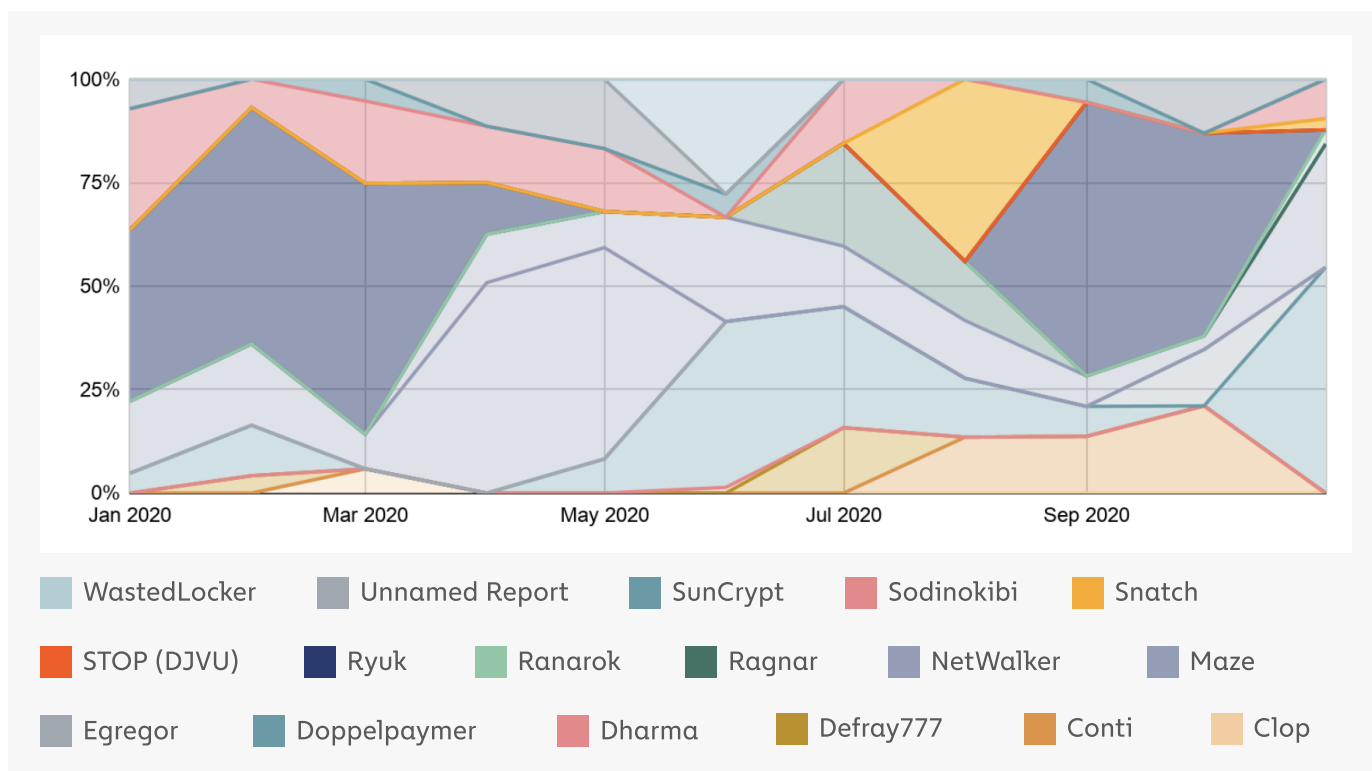
Top 10 ransomware strains by revenue by year | 2014 - 2020



Currencies included: BCH, BTC

Ransomware strains don't operate consistently, even month-to-month. Below, we see that the top-earning strains have ebbed and flowed throughout 2020.

Ransomware lifecycles: Top monthly strains by share of all ransomware revenue | 2020



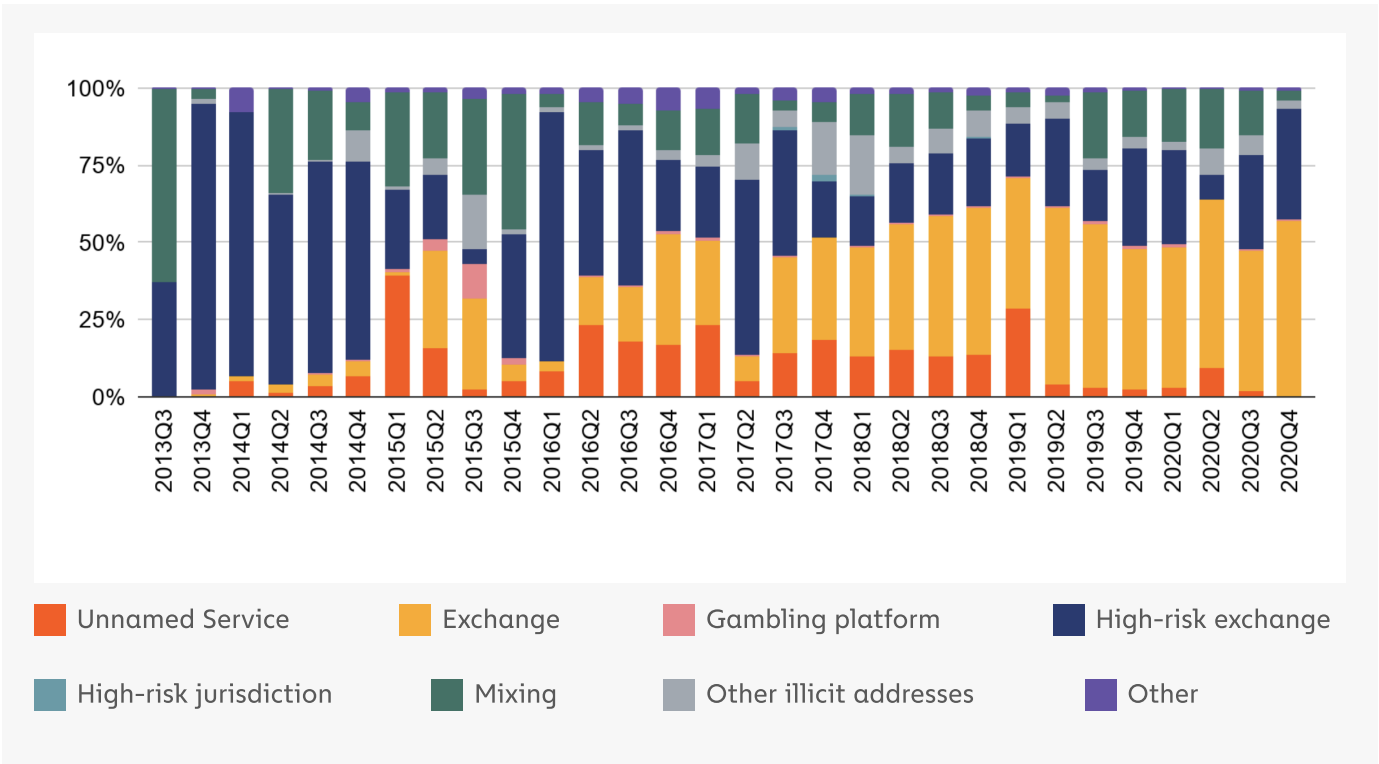
Currencies included: BTC



The number of strains active throughout the year may give the impression that there are several distinct groups carrying out ransomware attacks, but this may not be the case. As we explored in last year's Crypto Crime Report, many strains function on the [RaaS model](#), in which attackers known as affiliates "rent" usage of a particular ransomware strain from its creators or administrators, who in exchange get a cut of the money from each successful attack affiliates carry out.

Many RaaS affiliates migrate between strains, suggesting that the ransomware ecosystem is smaller than one might think at first glance. In addition, many cybersecurity researchers believe that some of the biggest strains may even have the same creators and administrators, who publicly shutter operations of one strain before simply releasing a new, very similar strain under a new name. With blockchain analysis, we can shed light on some of these connections by analyzing how addresses associated with different ransomware strains transact with one another.

Destination of funds leaving ransomware wallets | Q3 2013 - Q4 2020



Currencies included: BTC, BCH, ETH

Ransomware attackers move most of the funds taken from their victims to mainstream exchanges, high-risk exchanges (meaning those with loose to non-existent compliance standards), and mixers. However, as we'll explore later in the section, the money laundering infrastructure ransomware attackers rely on may be controlled by just a few key players,



similar to the ransomware strains themselves. We'll explore the interconnectivity within the ransomware ecosystem below. But first, we'll look at an under-discussed issue ransomware victims face in addition to the loss of money and data: Sanctions risk.

Sanctions risk in ransomware

In October 2020, perhaps prompted by the massive uptick in ransomware attacks rocking both the public and private sector, the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) [released an advisory alert](#) warning that making ransomware payments could be a sanctions violation for victims or companies that facilitate payments for victims. The facilitation point is important, as there's a robust industry of consultants who help ransomware victims negotiate with and pay ransomware attackers. The alert cited examples of ransomware creators and attackers who have been put on the OFAC sanctions list, such as the [two Iranian nationals](#) who laundered proceeds from the SamSam ransomware strain. October's alert bolsters [previous government guidance](#) not to pay ransomware attackers, as this incentivizes future attacks. However, this alert goes a step further in warning that ransomware victims and consultants who help them make payments could face the heavy penalties associated with sanctions violations.

But how big is the sanctions violation risk in ransomware? We looked back at all ransomware payments Chainalysis has tracked since 2016 and calculated the percentage of payment volume that was associated with sanctions risks.

We counted all ransomware payments that meet any of the three criteria below as constitutive of sanctions violation risk:

- Payments to addresses identified by OFAC as belonging to sanctioned individuals (note: this includes payments made before the addresses' owners were actually sanctioned.).
- Payments to addresses connected to ransomware strains whose creators have been sanctioned by OFAC.
- Payments to addresses connected to ransomware strains associated with cybercriminals based in heavily sanctioned jurisdictions such as Iran and North Korea.

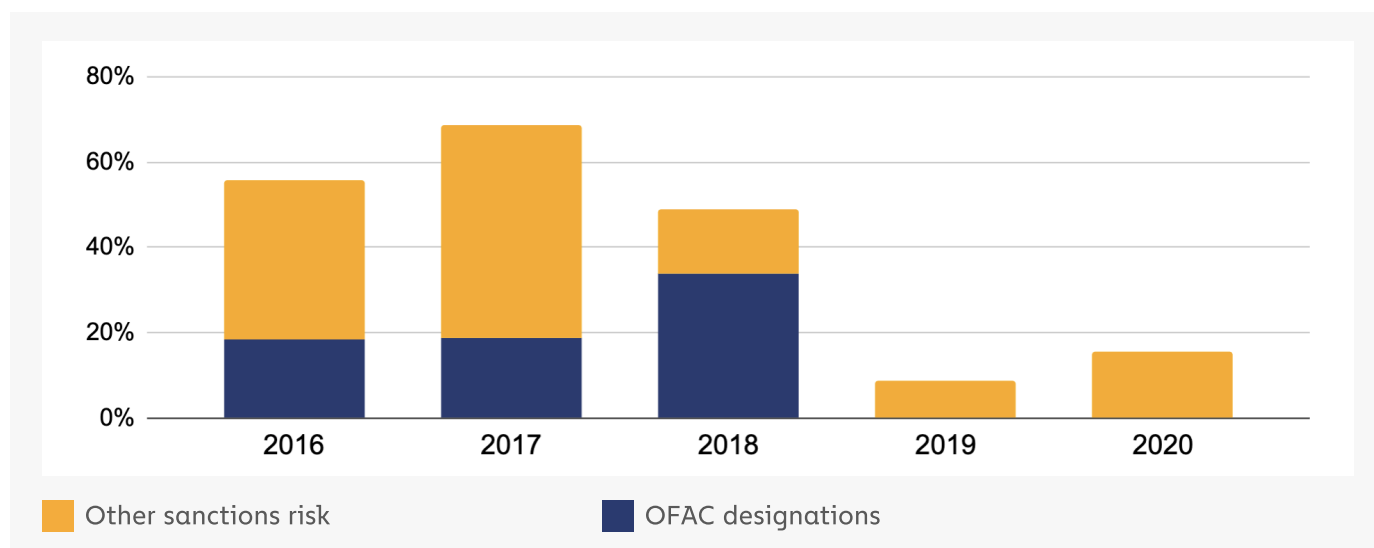


Those criteria cover the following ransomware strains:

Strain	Description
SamSam	OFAC designated cryptocurrency address
Ouroboros	Linked to Iranian Actors
VoidCrypt	Linked to Iranian Actors
Sorena	Linked to Iranian Actors
Pay2Key	Linked to Iranian Actors
WannaCry 1.0, WannaCry 2.0	Linked to North Korean Actors
NotPetya	Associated with sanctioned actors in Russia.
CryptoLocker	Associated with sanctioned actors in Russia.
Bitpaymer	Speculated to be associated with sanctioned group Evil Corp.
Locky	Speculated to be associated with sanctioned group Evil Corp.
Doppelpaymer	Speculated to be associated with sanctioned group Evil Corp.
WastedLocker	Speculated to be associated with sanctioned group Evil Corp.
Clop	Disputed, but speculated to be associated with Evil Corp.

Based on those designations, we found that **15% of all ransomware payments made in 2020** carried a risk of sanctions violations. This was quite low compared to some previous years.

Share of all ransomware payments associated with OFAC designations and other sanctions risk | 2016 - 2020



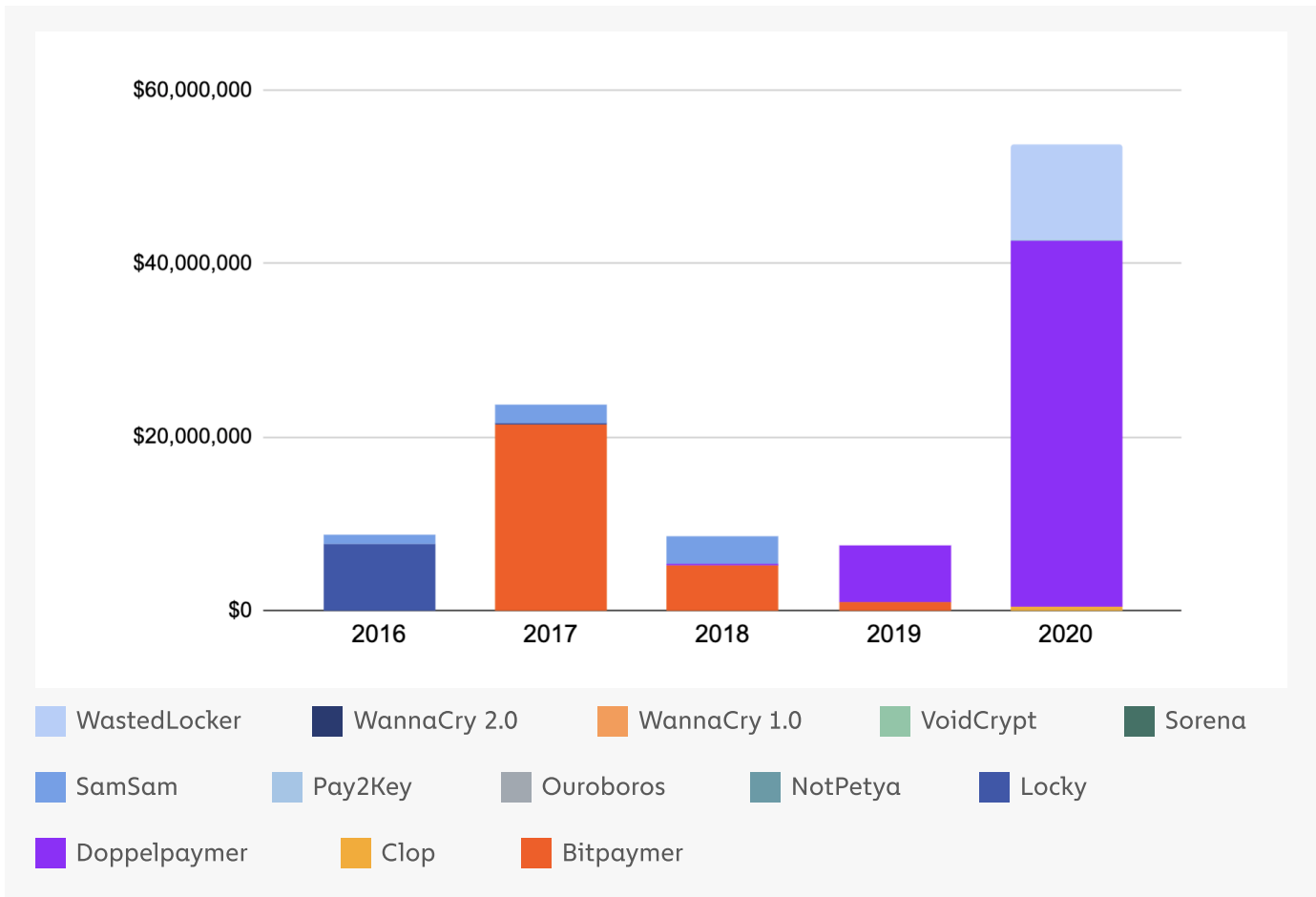
Please note that all payments to addresses associated with OFAC-sanctioned individuals or groups noted on this chart took place before those individuals or groups were added to the OFAC sanctions list.

Currencies included: BCH, BTC, ETH, USDT



While the rate of sanctions risk in ransomware payments has declined from much higher figures in 2018 and prior, keep in mind how much ransomware payments overall increased in 2020. That means the dollar figure for ransomware payments with sanctions risk skyrocketed last year. Below, we show the yearly volume of ransomware payments that constitute sanctions violation risk, broken down by strain.

Total value received by ransomware addresses associated with sanction risk by ransomware strain | 2016 - 2020



Currencies included: BCH, BTC

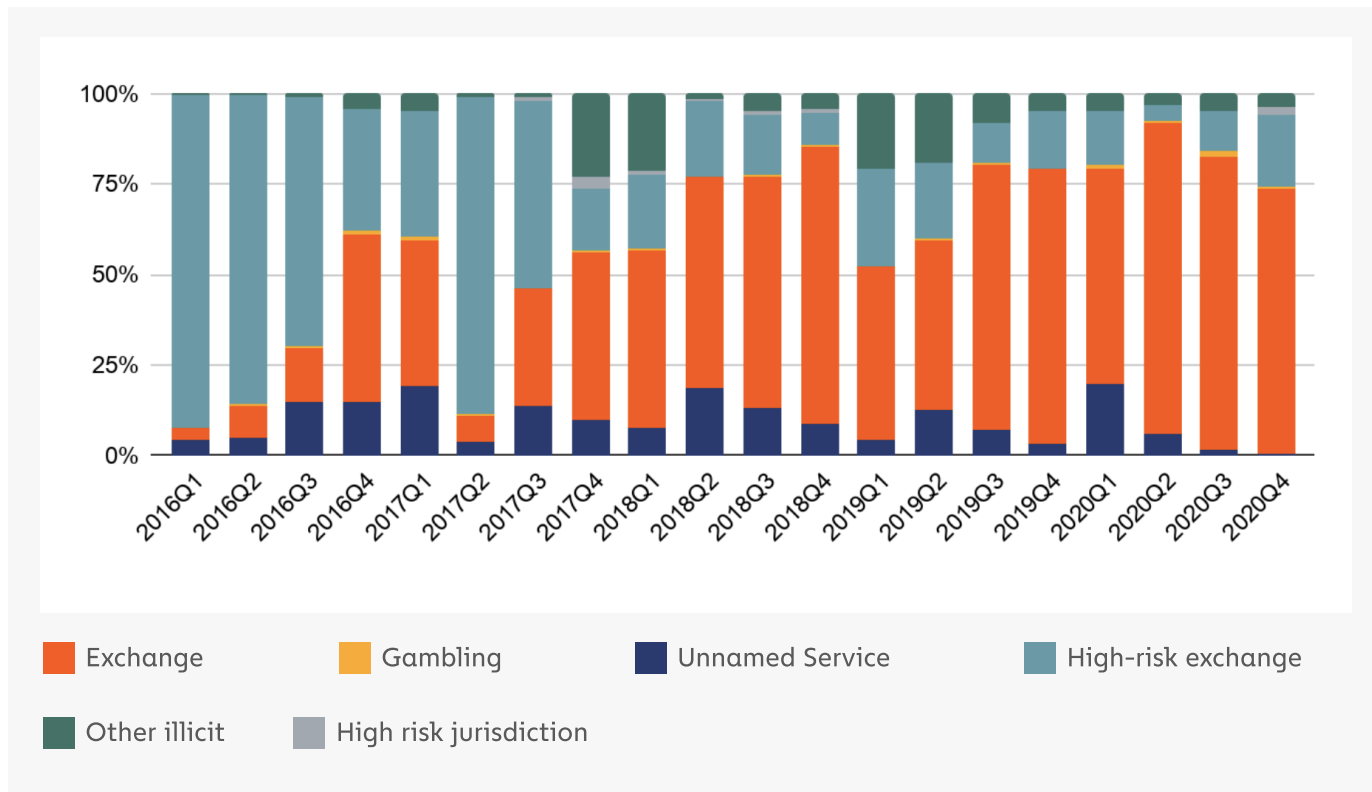
Overall, more than \$50 million worth of cryptocurrency that victims paid out to ransomware addresses that we've identified carried sanctions risk in 2020, nearly all of which was composed of payments to Doppelpaymer and WastedLocker specifically. In previous years, Bitpaymer, SamSam, and Locky have also been responsible for a high volume of ransomware payments associated with sanctions risk.

It's also worth noting that exchanges and other cryptocurrency businesses could be at risk for any funds they receive from ransomware addresses in general, but especially those associated with sanctions risk.



Destination of funds leaving ransomware wallets with sanction risk

| Q4 2014 - Q4 2020



Overall in 2020, mainstream exchanges received more than \$32 million from ransomware strains associated with sanctions risks.

Dealing with a ransomware attack is hard enough without victims having to worry about penalties and reputational damage down the line if it turns out they committed a sanctions violation for paying a ransom. We encourage all ransomware victims to work with a lawyer specializing in sanctions and financial crime before paying off an attacker, and to report the attack to law enforcement.

Blockchain analysis shows connections between four of 2020's biggest ransomware strains

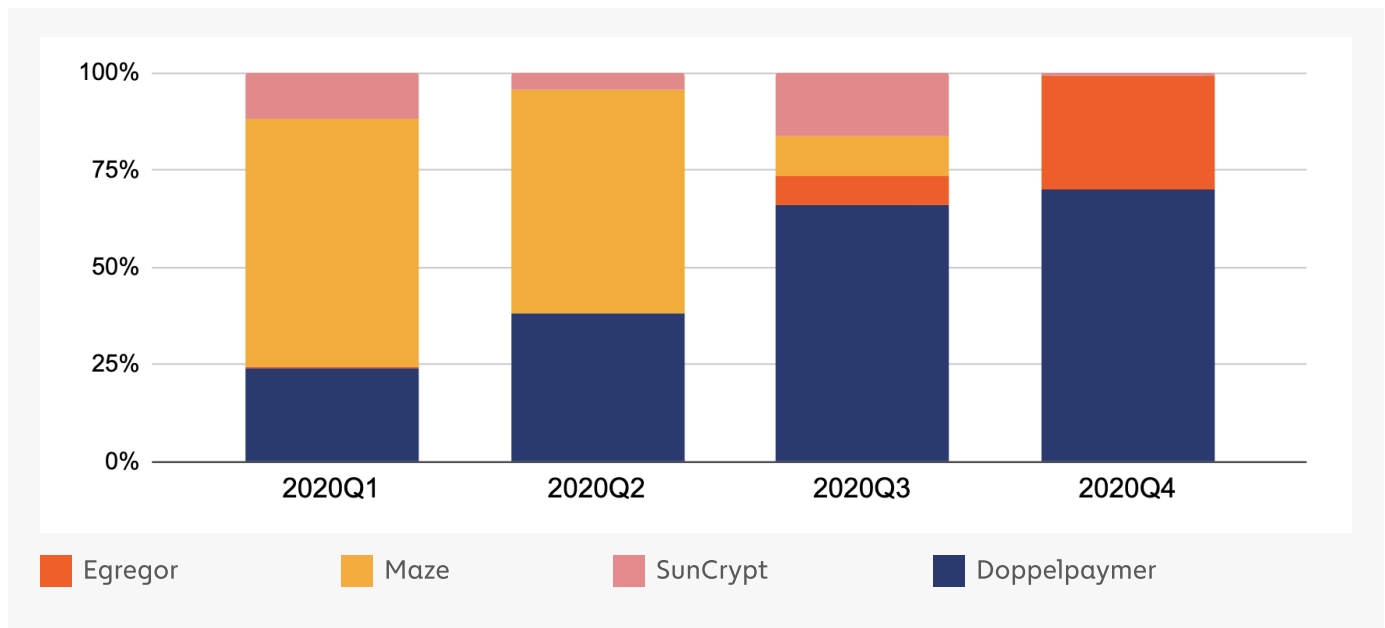
As we mention above, there may be fewer cybercriminals responsible for ransomware attacks than one would initially think given the number of individual attacks, distinct strains, and amount stolen from victims. Cybersecurity researchers point out that many RaaS affiliates carrying out attacks switch between different strains, and many believe that seemingly distinct strains are actually controlled by the same people. Using blockchain analysis, we'll investigate potential connections between four of 2020's most prominent ransomware strains: Maze, Egregor, SunCrypt, and Doppelpaymer.



The four ransomware strains were quite active last year, attacking prominent companies such as [Barnes & Noble](#), [LG](#), [Pemex](#), and [University Hospital New Jersey](#), amongst others. All four use the RaaS model, meaning that affiliates carry out the ransomware attacks themselves and pay a percentage of each victim payment back to the strain's creators and administrators. All four also use the "[double extortion](#)" strategy of not just withholding victims' data, but also publishing pieces of it online as an extra incentive for victims to pay the ransom.

Below, we see the four strains' 2020 revenue broken out quarterly.

2020 Ransomware revenue by quarter: SunCrypt, Maze, Egregor, and Doppelpaymer



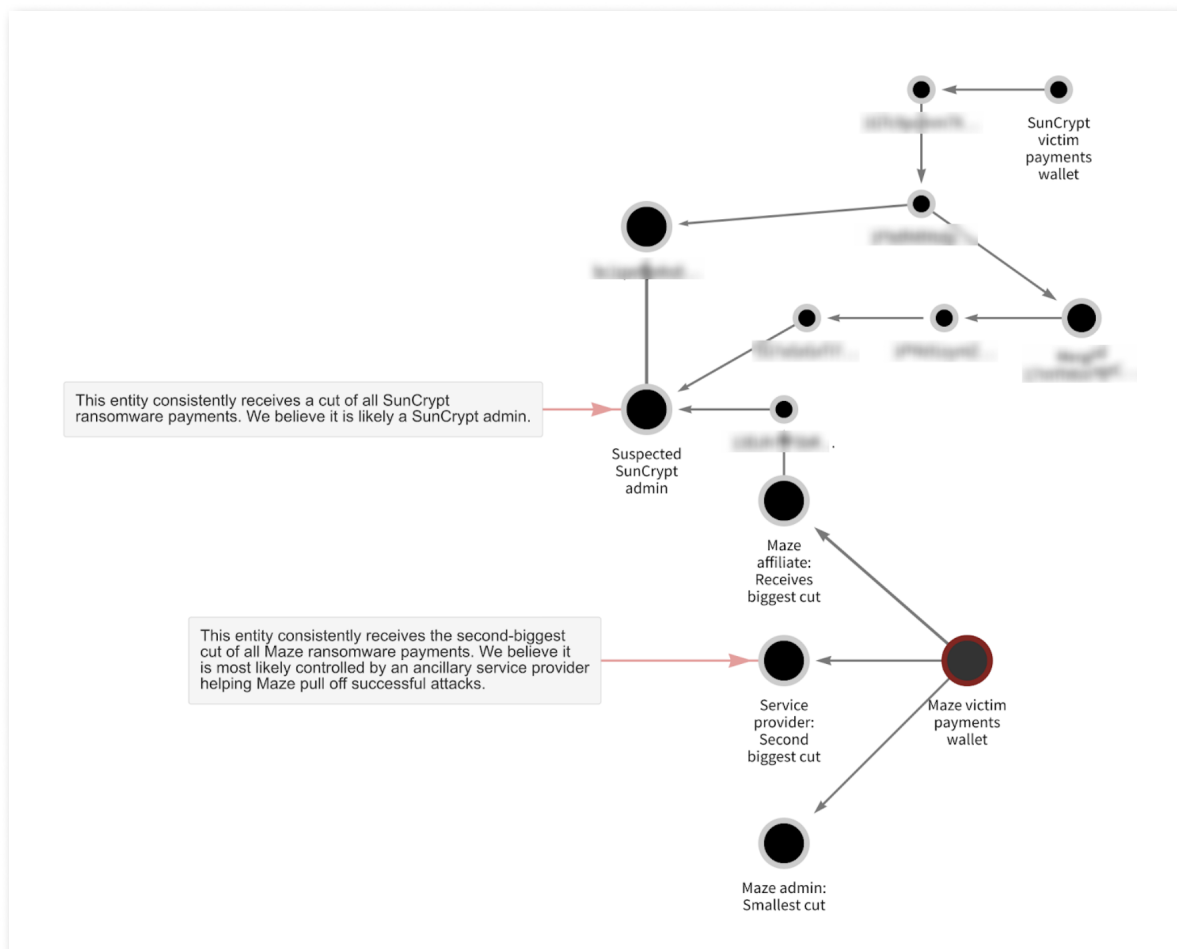
Note that Egregor only became active just before Q4 2020 (mid-September to be specific), soon after the Maze strain became inactive. Some cybersecurity researchers see this as evidence that Maze and Egregor are linked in some way. In early November, Maze's operators said the strain was shutting down in a press release posted to its website, following a slowdown in activity. Soon after, [most of its affiliates migrated](#) to Egregor, leading some to believe that the Maze operators have simply rebranded as Egregor and instructed the affiliates to join. This is relatively common in ransomware, though it's also possible that the affiliates have decided for themselves that Egregor is their best option. It's even possible that the Maze affiliates became unhappy with the Maze operators, leading to the split. However, as [noted by Bleeping Computer](#), Maze and Egregor share much of the same code, the same ransom note, and have very similar victim payment sites. Cybersecurity firm Recorded Future [notes this too](#), as well as similarities between Egregor and a banking trojan called QakBot.



It's not just Egregor either. In another story, [Bleeping Computer claims](#) that SunCrypt representatives contacted them claiming to be part of the "Maze ransomware cartel" prior to Maze's shutdown announcement, though Maze has denied this. However, the claim of a connection is also supported by a privately circulated report from threat intelligence firm Intel471 claiming that representatives from SunCrypt described their strain as a "rewritten and rebranded version of a 'well-known' ransomware strain." [Intel471's](#) report also claims that SunCrypt only works with a small number of affiliates at a time, whom the SunCrypt operators interview and vet extensively. Therefore, we believe any overlap in affiliates between SunCrypt and other ransomware strains would be more likely to suggest a deeper connection between the two strains, rather than just coincidence.

Blockchain analysis suggests affiliate overlap and other possible connections between Maze, Egregor, SunCrypt, and Doppelpaymer

As we outline above, there's circumstantial evidence suggesting links between some of these four strains, as well as reports of affiliate migration. But what links do we see on the blockchain? Let's start with Maze and SunCrypt.

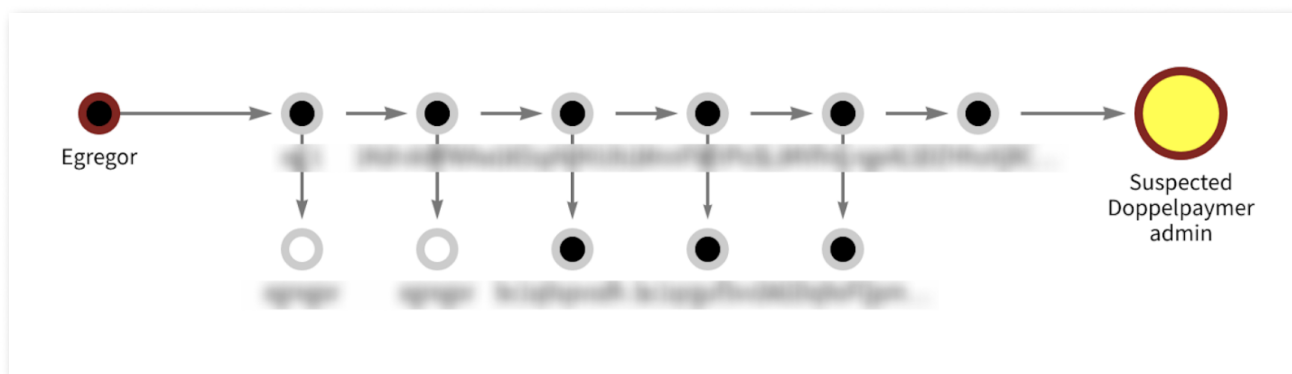




The [Chainalysis Reactor](#) graph above provides strong evidence suggesting that a Maze ransomware affiliate is also an affiliate for SunCrypt. Starting at the bottom of the graph, we see how Maze distributes funds taken in ransomware attacks. First, the majority of each successful ransom payment goes to the affiliate, as they're taking on the risk of actually carrying out the ransomware attack. The next biggest cut goes to a third party. While we can't know for sure what that third party's role is, we believe it's likely an ancillary service provider who helps Maze pull off attacks. Ransomware attackers often rely on third parties for tools like bulletproof hosting, penetration testing services, or access to vulnerabilities in victims' networks. These ancillary service providers can be found peddling their wares on cybercriminal darknet forums, but aren't necessarily involved in all ransomware attacks. Finally, the smallest cut of each ransom payment goes to another wallet that we believe belongs to the strain's administrators.

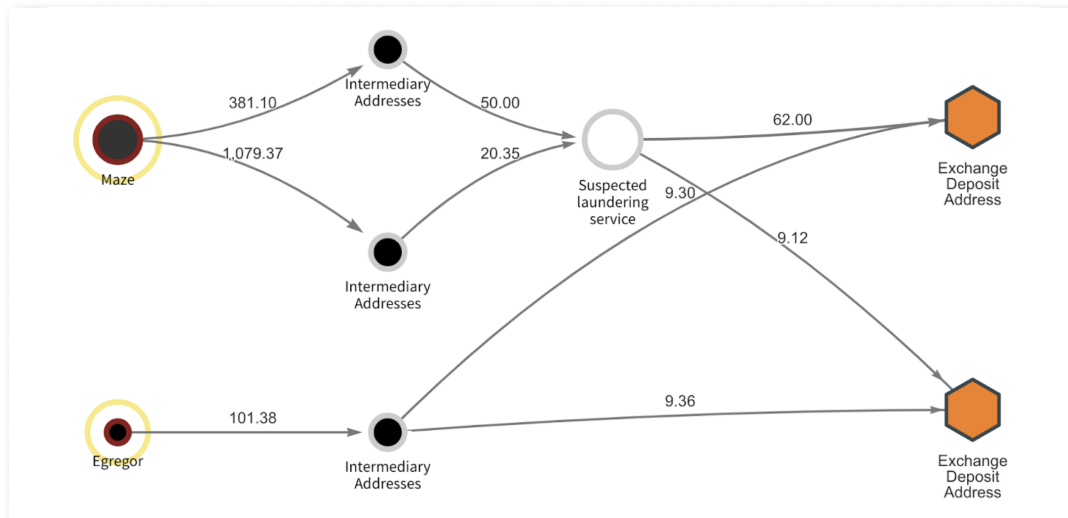
In this case, however, we see that the Maze affiliate also sent funds — roughly 9.55 Bitcoin worth over \$90,000 — via an intermediary wallet to an address labeled "Suspected SunCrypt admin," which we've identified as part of a wallet that has consolidated funds related to a few different SunCrypt attacks. This suggests that the Maze affiliate is also an affiliate for SunCrypt, or possibly involved with SunCrypt in another way.

Another Reactor graph shows links between the Egregor and Doppelpaymer ransomware strains.



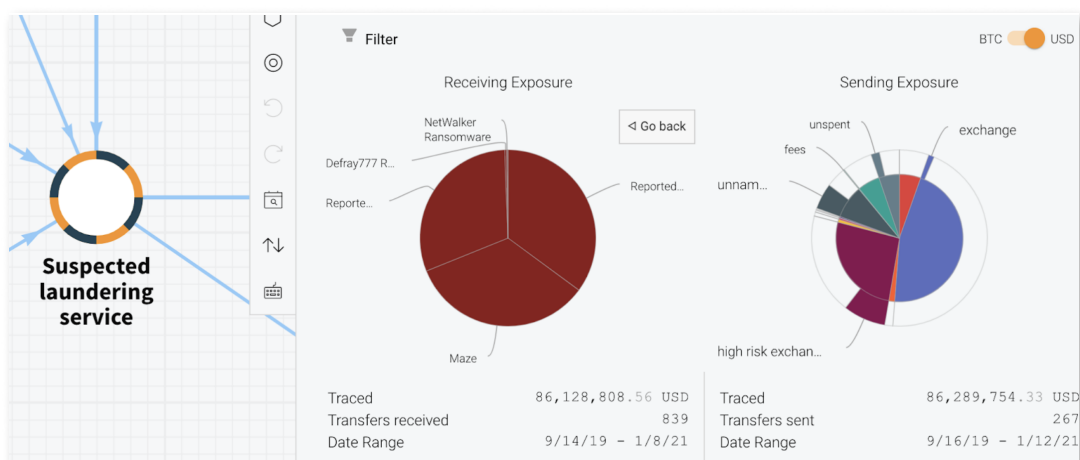
In this case, we see that an Egregor wallet sent roughly 78.9 BTC worth approximately \$850,000 to a suspected Doppelpaymer administrator wallet. Though we can't know for sure, we believe that this is another example of affiliate overlap. Our hypothesis is that the Egregor-labeled wallet is an affiliate for both strains sending funds to the Doppelpaymer administrators.

Finally, the Reactor graph below shows what we believe is an instance of Maze and Egregor administrators using the same money laundering infrastructure.



Both strains' victim payments' wallets have sent funds to two deposit addresses at a prominent cryptocurrency exchange via intermediary wallets. Based on their transaction patterns, we believe that both deposit addresses belong to over-the-counter (OTC) brokers who specialize in helping ransomware operators and [other cybercriminals](#) trade illicitly-gained cryptocurrency for cash. In the case of Maze, those funds first flow through another suspected money laundering service before reaching the OTC addresses — it's unclear whether Maze receives cash from that service or from the OTCs themselves, and it's also possible that the OTC broker and those running the laundering service are one and the same.

While this doesn't suggest that Maze and Egregor share the same administrators or affiliates, it's still an important potential lead for law enforcement. Cryptocurrency-related crime isn't worthwhile if there's no way to convert ill-gotten funds into cash. By going after bad actors like the money laundering service or corrupt OTC brokers on the graph above — the latter of whom, again, operate on a large, well-known exchange — law enforcement could significantly hamper the ability of Maze and Egregor to operate profitably without actually catching the strains' administrators or affiliates. It's not just those specific ransomware strains either.





The suspected laundering service has also received funds from the Doppelpaymer, WastedLocker, and Netwalker ransomware strains, taking in nearly \$2.9 million worth of cryptocurrency from the category as a whole. Likewise, it's received nearly \$650,000 worth of cryptocurrency from darknet markets such as Hydra and FEShop. The two OTC broker addresses on the graph have similar criminal exposure as well.

What does this mean for ransomware?

While we can't say for sure that Maze, Egregor, SunCrypt, or Doppelpaymer have the same administrators, we can say with relative certainty that some of them have affiliates in common. We also know that Maze and Egregor rely on the same OTC brokers to convert cryptocurrency into cash, though they interact with those brokers in different ways.

Regardless of the exact depth and nature of these connections, the evidence suggests that the ransomware world is smaller than one may initially think given the number of unique strains currently operating. This information can be a force multiplier for law enforcement. If they can identify and act against groups controlling multiple ransomware strains, or against OTCs enabling multiple ransomware strains to cash out their earnings, then they'll be able to halt or impact the operations of several strains with one takedown.

Mapping the ransomware ecosystem

As we show above, we can find connections between ransomware strains by examining common deposit addresses to which wallets associated with different strains send funds. We believe that most of the cases of deposit address overlap represent usage of common money laundering services by different ransomware strains, as we posited in the example of transactions connecting Maze and Egregor. Again, instances of overlap in money laundering services is important information for law enforcement, as it suggests they can disrupt the activity of multiple strains — in particular, their ability to liquidate and spend the cryptocurrency victims pay them with — by taking one money laundering operation offline.

Overlap also wouldn't be surprising, as we see a small number of money laundering services advertising on various hacking forums. "Many of these services use mules and other means to register lots of fake accounts at big exchanges that they control," said Dmitry Smilyanets, ransomware expert and Threat Intelligence Analyst at cybersecurity provider [Recorded Future](#). We see that reflected in the screenshots below.



Kudes Service is a store of verified accounts.

All are welcome! Our service provides ready-made verified accounts for any crypto-exchange or bookmaker's offices. We verify against European and American documents.

We work exclusively according to the client's requirements, we are ready to create an account for both our data and yours.

We have in stock a huge number of drops (M / F) of completely different ages. We can choose a drop according to your requirements.

We have accounts for the following

crypto exchanges in stock and on order: - Binance (com / us / je)

- BitFinex
- Bittrex
- Blockchain
- Cash App
- Coinbase
- Coinfalcon
- Coinmama
- Crypto Com
- Huobi
- Localbitcoins
- Monese
- Paxful
- Poloniex
- Revolut
- Uphold

and many others.

Contacts for communication:

Telegram: @Kudes

Jabber: kudes@exploit.im

Service rules:

- We do not work with domestic cryptocurrency exchanges under any circumstances.
- We do not advise on account processing and do not work with newbies.
- If your account is blocked (through our fault), we will gladly provide you with a replacement for free.

21.08.2020, 19:50

VFTFree ▼

Vendor of:
verification



Join Date: 18.08.2020

Deposit: 2000\$?

Business Level: 0 ?

SUBSCRIBE

WRITE PM

Account verification and sale

I welcome everyone!

We verify accounts for you at affordable prices!

crypto.com, paxful, localbitcoins, n26, wiresx, bitzlatto, skroll, binance US, etc.

There are ready-made accounts !!! I will sell Binance US accounts, complete with a photo of the document + a bank statement. Drop US! LVL 3!

Drops of the CIS and EU.

Telegram @VFTFree

Jabber teamverif@verified.pm

Last edited by VFTFree: 01.11.2020 at 18:53

Smilyanets also points out that many ransomware attackers are willing to wait to cash out their earnings. "They often feel safer waiting, and they believe in cryptocurrency and think it will keep growing, so they have no problem letting it sit for a few years."

However, money launderers aren't the only ones ransomware addresses send cryptocurrency to. Ransomware operators rely on several types of third-party providers to conduct attacks. These include:

- **Penetration testing services**, which ransomware operators use to probe potential victims' networks for weaknesses.
- **Exploit sellers**, who sell access to vulnerabilities in various types of software that ransomware operators and other cybercriminals can use to inject victims' networks with malware.

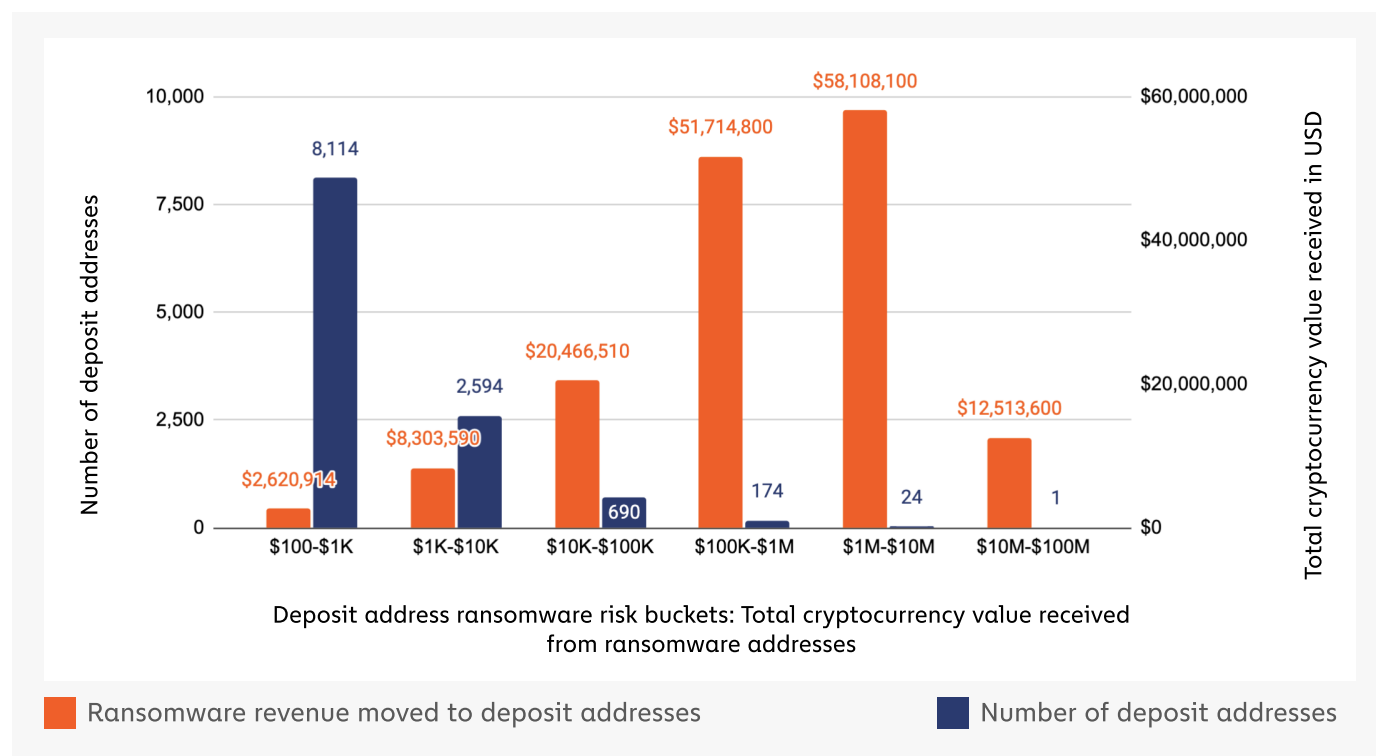
- **Bulletproof hosting providers**, who provide web hosting that customers can purchase anonymously and are generally lenient on the types of sites customers are allowed to host. Ransomware operators often need web hosting to set up command-and-control (C2) domains, which allow hackers' computers to send commands to victims' machines infected with malware.

Similar to money laundering services, law enforcement could theoretically disrupt several ransomware strains if agents were able to identify and act against service providers ransomware operators rely on to carry out attacks.

But just how concentrated are the deposit addresses receiving funds from ransomware addresses? Let's investigate.

As we mentioned at the beginning of the section, the majority of ransomware funds move to cryptocurrency exchanges. This activity is relatively concentrated to just a few services — a group of just five receives 82% of all ransomware funds. But what about when we look at the deposit address level?

Total illicit value received by deposit addresses by ransomware risk bucket vs. Number of deposit addresses per ransomware risk bucket | 2020



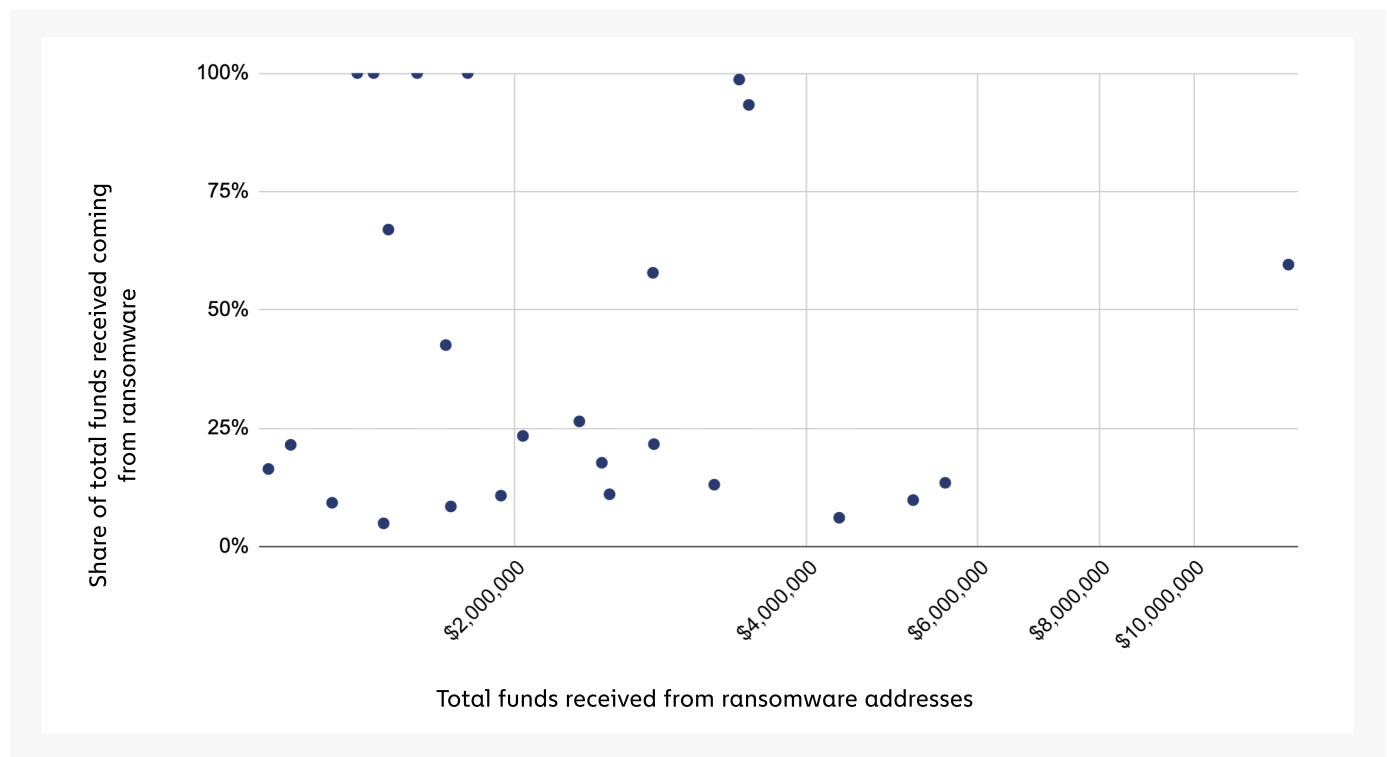
Accounts are bucketed by range of total value received from ransomware addresses. Each orange bar represents the total amount ransomware addresses sent to all addresses in the corresponding bucket, while each blue bar represents the number of individual deposit addresses in the bucket.



The data shows that ransomware money laundering is even more concentrated at the deposit address level. **Just 199 deposit addresses received 80% of all funds sent by ransomware addresses in 2020. An even smaller group of 25 addresses accounted for 46%.** Smilyanets and his colleague at Recorded Future, Roman Sannikov, reviewed these numbers and agreed the address sets taking in the most from ransomware strains were most likely money laundering services, while those taking in less were more likely to include third parties like exploit sellers and bullet-proof hosting providers. "Any address receiving \$10,000 or less especially would much more likely be a service provider than a money launderer," said Sannikov.

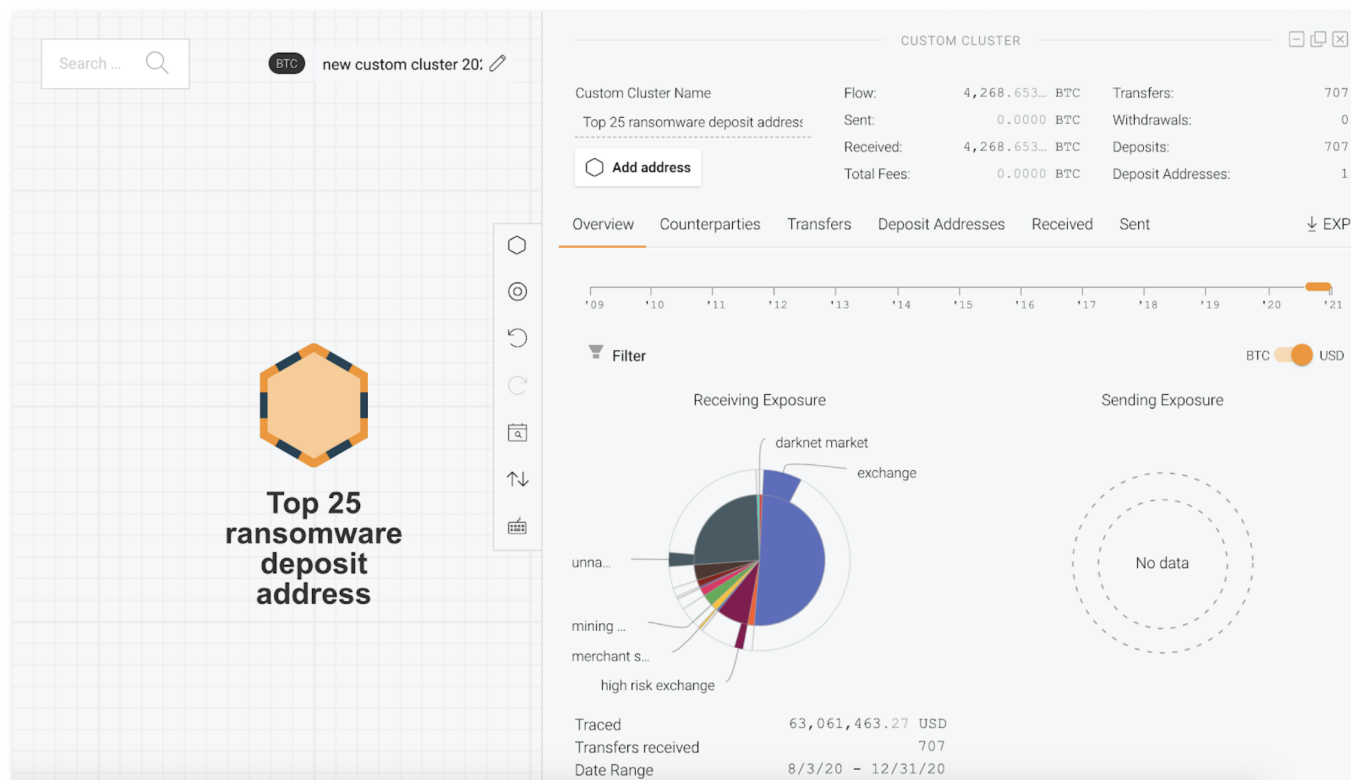
Let's look more closely at the addresses receiving the most from ransomware, and in particular the share of their total activity that's devoted to ransomware.

Top service deposit addresses for ransomware: Total funds received from ransomware addresses vs. Share of all funds received coming from ransomware addresses | 2020



Currencies included: BTC

On the scatter chart above, we sort the top 25 ransomware deposit addresses by the total amount they've received from ransomware addresses on the X axis, and the share of total funds they've received that ransomware makes up on the Y axis. We see that, save for a few outliers, ransomware makes up a relatively small percentage of all funds received by these deposit addresses. Below, we look more closely at the transaction history of one of those deposit addresses.



Please note that Chainalysis Reactor doesn't show sending activity for service deposit addresses, as services often move the funds received to their own internal addresses as needed. This means that tracing funds through service addresses can produce misleading results.

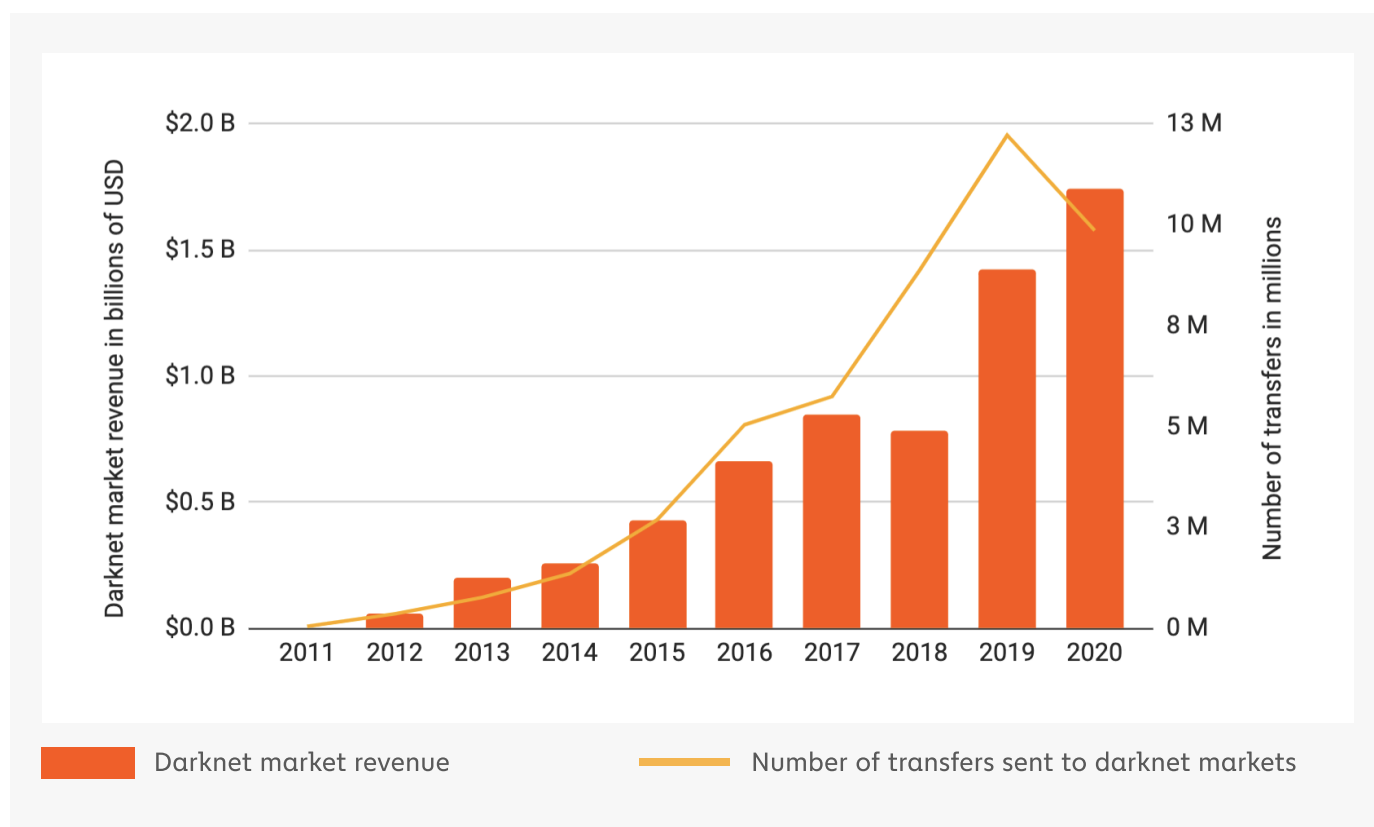
This deposit address belongs to a nested service hosted at a large, international cryptocurrency exchange and has been active since August 3, 2020. Between that date and the end of 2020, it received over \$63 million worth of Bitcoin in total. Most of it appears to be non-illicit activity – nearly half of those funds come from other mainstream exchanges, though a quarter comes from unknown services that may be identified as linked to criminal activity at a later date. However, while the share is low, the address has still received over \$1 million worth of Bitcoin from ransomware addresses, as well as \$2.4 million from multiple scams. Overall, criminal activity accounts for 10% of the address' total cryptocurrency received. Most of the other deposit addresses on our scatter chart with low shares of total funds coming from ransomware fit a similar profile.



Darknet Market

Darknet Market Activity Higher Despite Fewer Purchases and Dwindling Number of Markets

Darknet market revenue vs. Total transfers to darknet markets
| 2011 - 2020

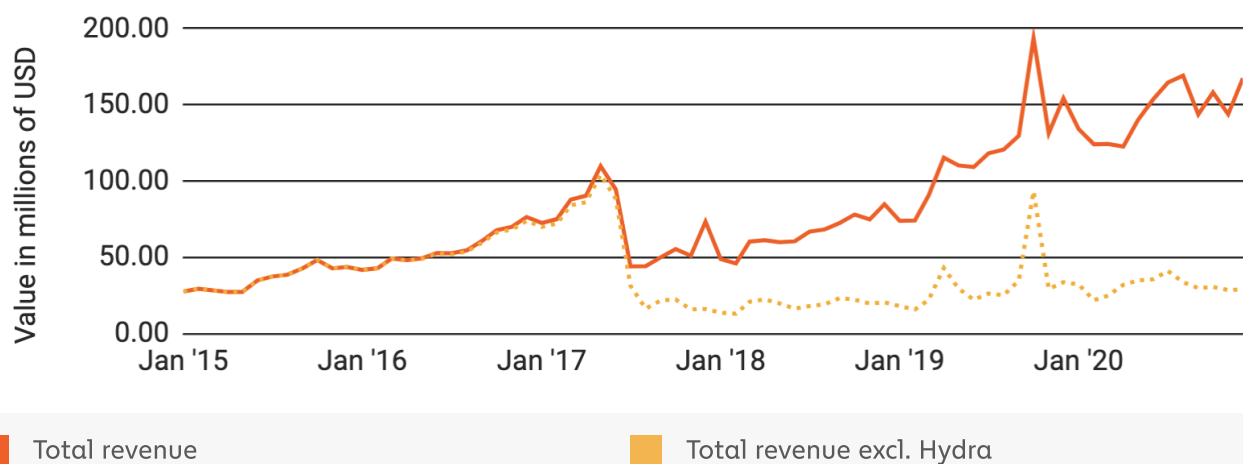


Currencies included: BCH, BTC, LTC, USDT

Darknet markets set a new revenue record in 2020, bringing in a total of \$1.7 billion worth of cryptocurrency. Interestingly, this record comes as individual purchases from darknet markets declined, falling from 12.2 million in 2019 to fewer than 10 million in 2020. However, if we look more closely, we see that nearly all of the growth in darknet market activity 2020 can be attributed to one specific market: Hydra.



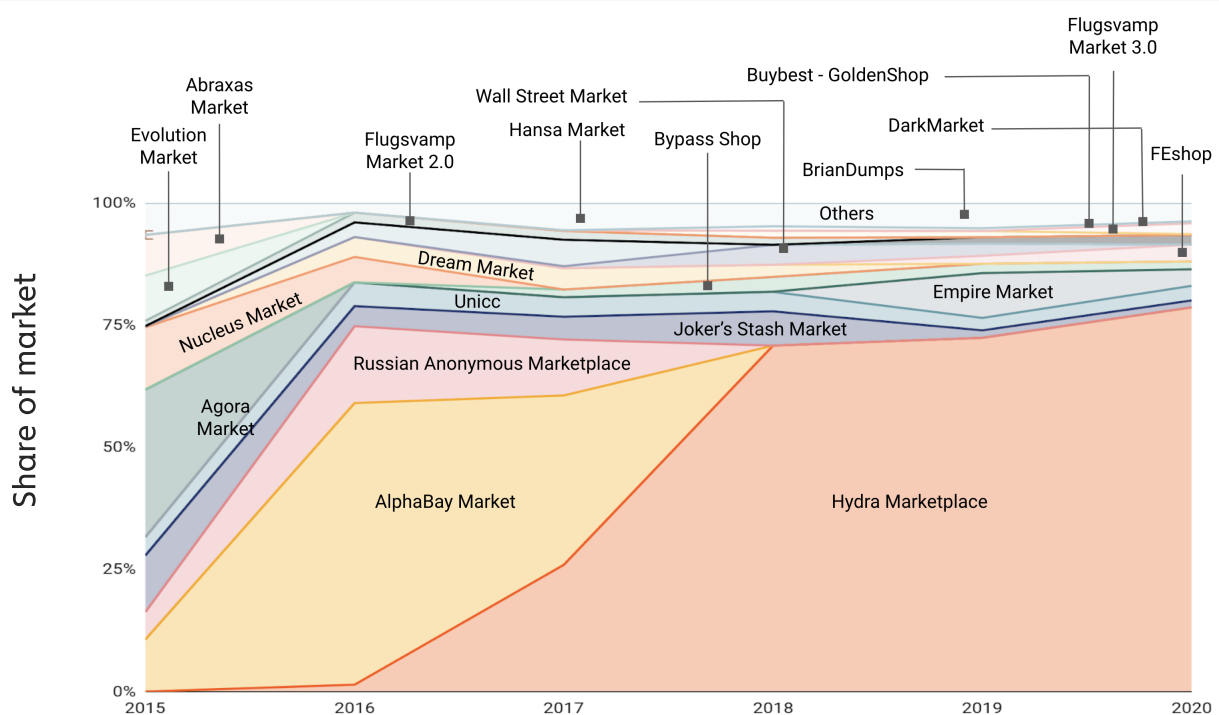
Monthly darknet market revenue | 2015 - 2020



Currencies included: BCH, BTC, LTC, USDT

If we exclude Hydra, we see that darknet market revenue stayed roughly flat from 2019 to 2020. Hydra is unique in that it only serves Russian-speaking countries and is by far the largest darknet market in the world, accounting for over 75% of darknet market revenue worldwide in 2020.

All darknet markets by share of total market size over time | 2015 - 2020

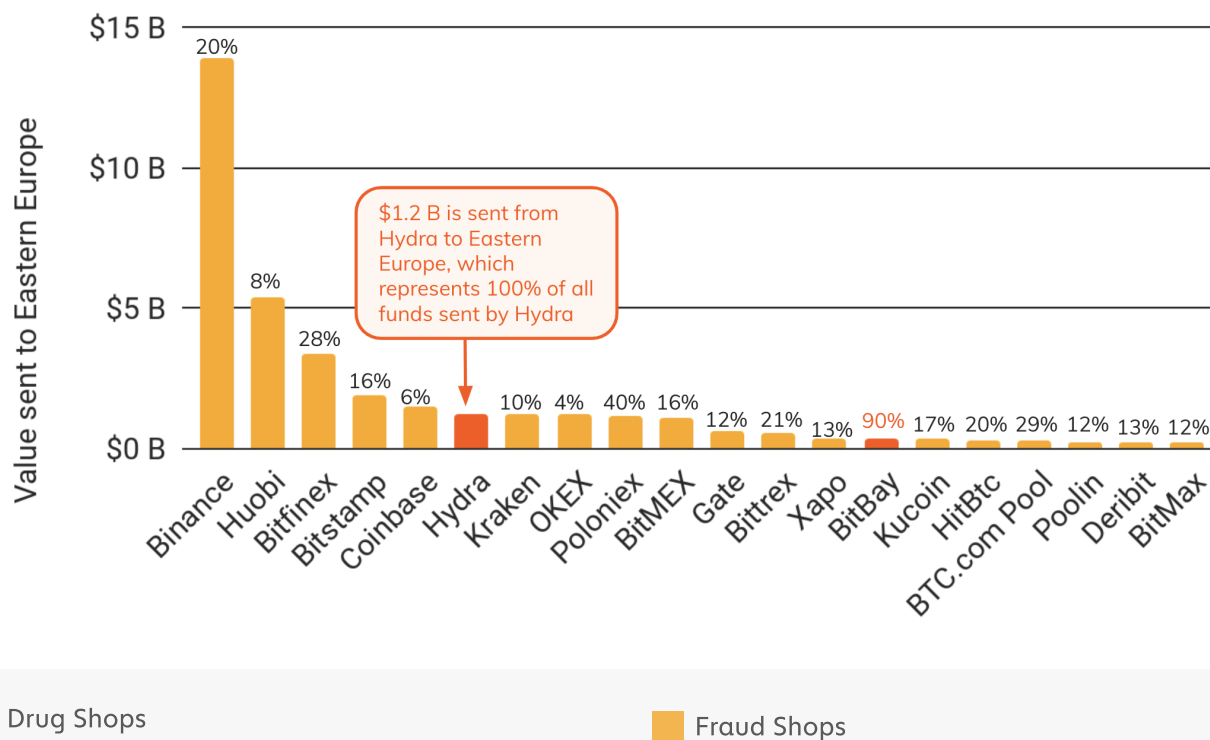


Currencies included: BCH, BTC, LTC, USDT



Hydra is a big driver of [Eastern Europe's unique crypto crime landscape](#). Eastern Europe has one of the highest rates of cryptocurrency transaction volume associated with criminal activity and, thanks to Hydra, is the only region with a criminal service as one of the top ten entities sending cryptocurrency value to the region.

Top 20 services by value sent to Eastern Europe | Jul '19 - Jun '20



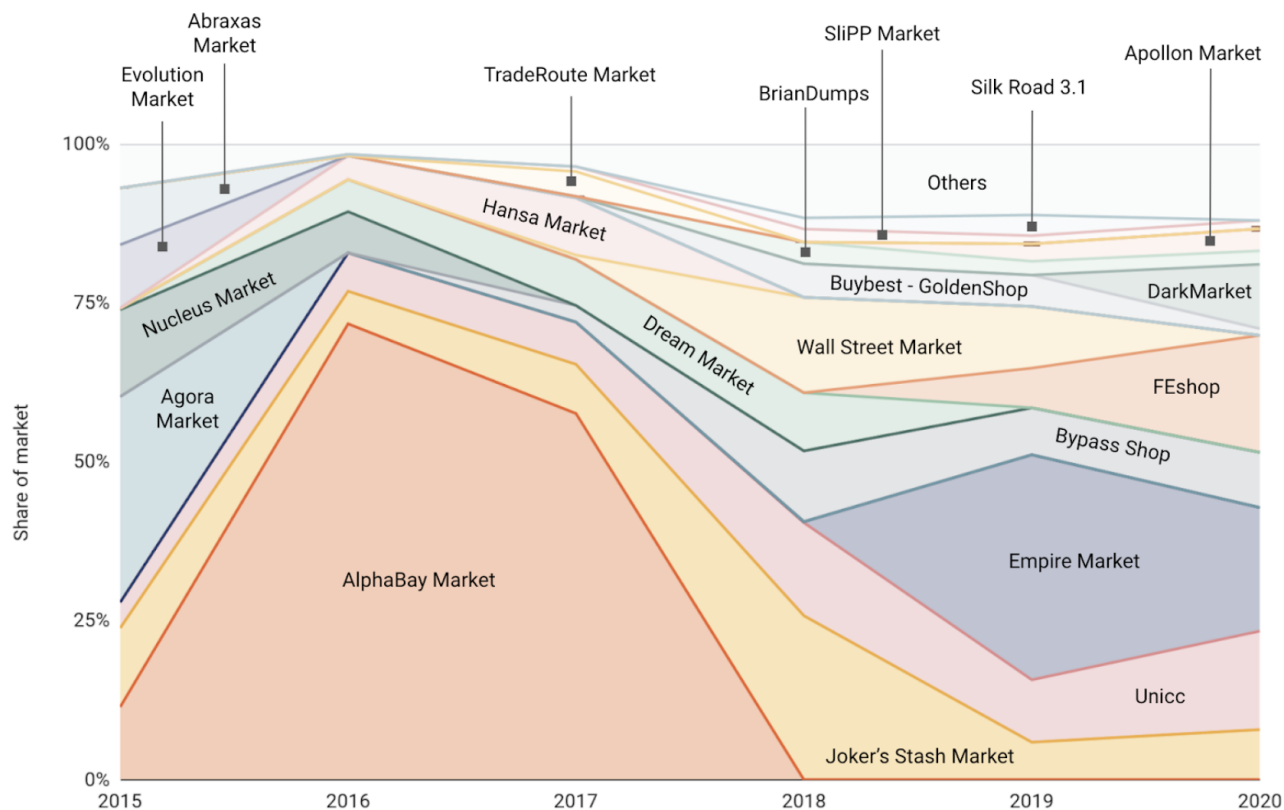
Currencies included: BAT, BCH, BNB, BTC, BUSD, CRO, CRPT, DAI, ETH, GNO, GUSD, HT, HUSD, ICN, LEO, LINK, LTC, MCO, MKR, MLN, OMG, PAX, PAXG, TGBP, TUSD, USDC, USDT, WETH, ZIL, ZRX

Hydra could eventually come to the English-speaking world as well. In December 2019, Hydra [announced plans](#) to raise \$146 million in an ICO for a new global DNM service called Eternos. While it appears Covid put this plan on hold, the announcement suggests that Hydra plans to expand. That could create a significant challenge for U.S. and European law enforcement, as Hydra has developed [uniquely sophisticated operations](#), such as an Uber-like system for assigning drug deliveries to anonymous couriers, who drop off their packages in out-of-the-way yet hidden public locations, commonly referred to as “drops,” which are then shared with the buyers. That way, no physical exchange is made, and unlike with traditional darknet markets, vendors don’t need to risk using the postal system.



Global darknet markets by share of total market size over time

| 2015 - 2020



Currencies included: BCH, BTC, LTC, USDT

If we exclude Hydra and other markets that serve customers in a particular region, we see that darknet market activity is much less concentrated outside the Russian-speaking world, with several different markets taking in significant revenue. Interestingly, many of the largest markets are fraud shops, which sell stolen credit card information and other data that can be used for fraud, including personally identifying information (PII), [SOCKS5](#), stolen accounts for different services, and hacking exploits rather than drugs.



Top 20 global darknet markets by revenue | 2020

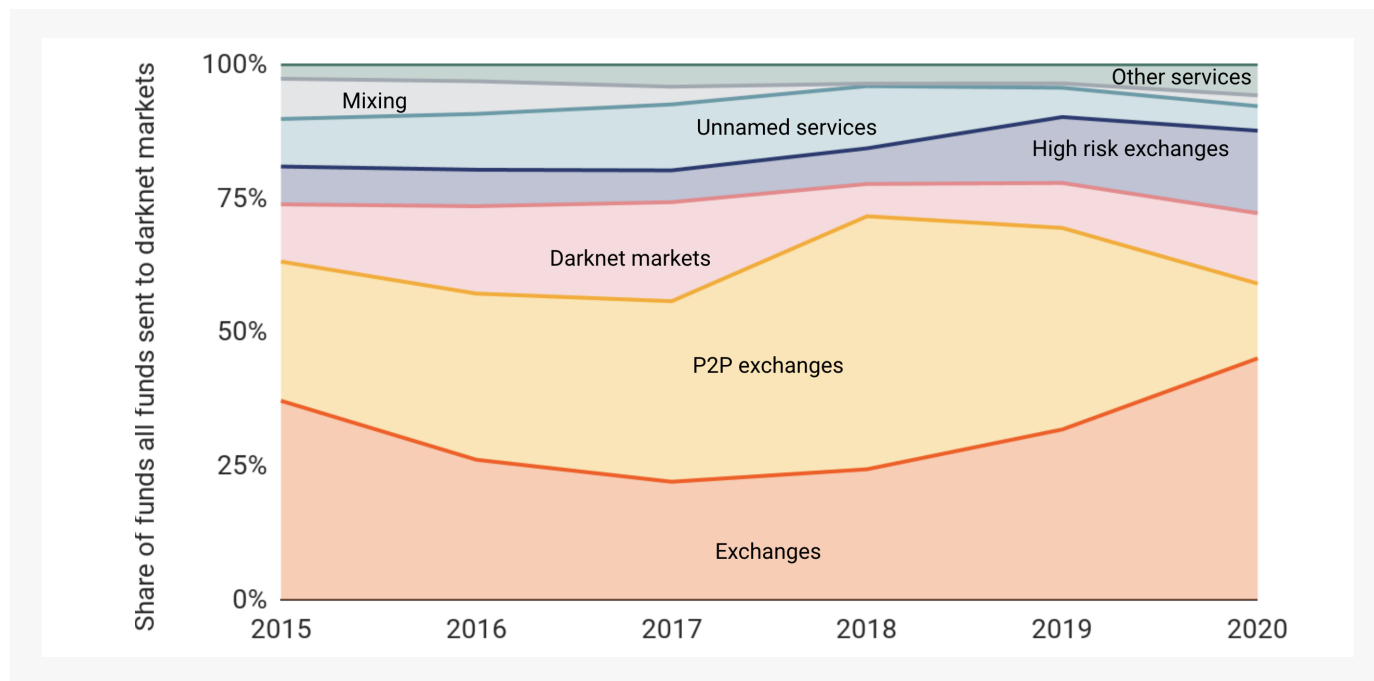


Currencies included: BCH, BTC, LTC, USDT

In fact, when we exclude Hydra, we see that card shops surpass drug shops in revenue amongst English language darknet markets.

What kinds of services are darknet market vendors and their customers using to facilitate these activities? We'll start with the customers. Below, we break down the services sending cryptocurrency to darknet markets by volume.

Origin of funds sent to darknet markets | 2015 - 2020



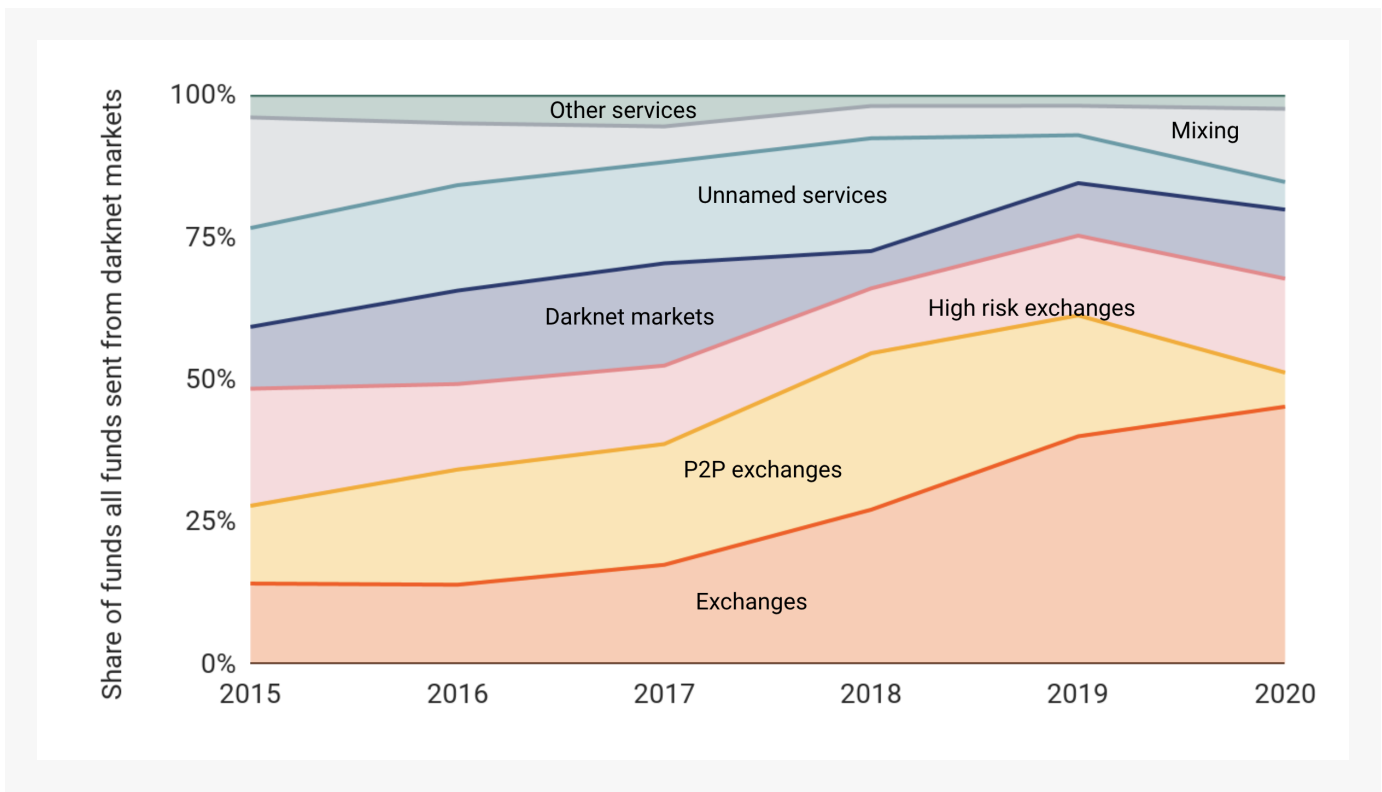
Currencies included: BCH, BTC, LTC, USDT



Standard exchanges, peer-to-peer (P2P) exchanges, high-risk exchanges, and other darknet markets account for nearly all of the cryptocurrency sent to darknet markets. Interestingly, 2020 has seen standard exchanges send a larger share of total darknet market revenue — about 45% in 2020 versus 31% in 2019 — while P2P exchanges' share has declined significantly. Given that standard exchanges tend to be more popular and easier to use, this could suggest that darknet markets attracted more first-time customers who are new to cryptocurrency in 2020, possibly due to declines in street sales during the Covid pandemic.

Below, we see the types of services receiving funds from darknet markets, which we use to approximate where darknet market vendors and administrators are cashing out their cryptocurrency earnings.

Destination of funds leaving darknet markets | 2015 - 2020



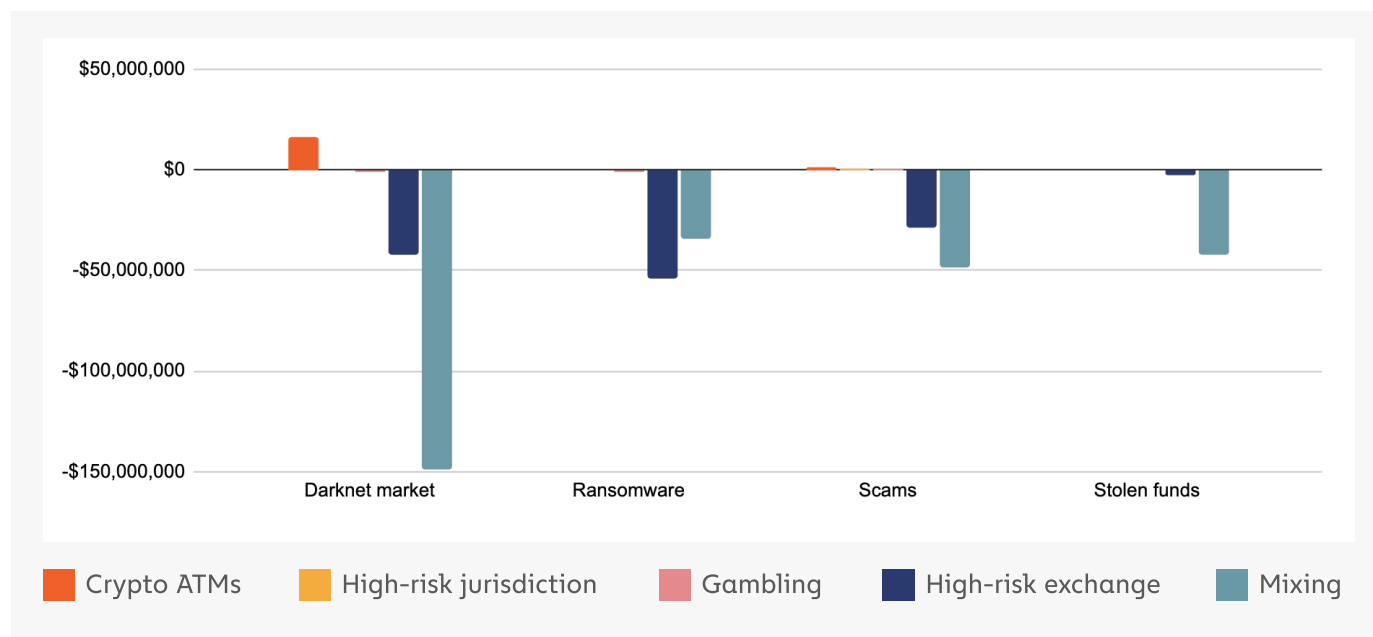
Currencies included: BCH, BTC, LTC

The numbers are somewhat similar to those on the receiving side, with standard exchanges taking in a larger share in 2020 compared to 2019, and P2P exchanges' share declining. However, we also see a significant uptick in the amount going to mixers as well, with their share more than doubling from 4.8% in 2019 to 13.7% in 2020. This may reflect increasing caution from darknet market vendors and administrators following law enforcement crackdowns.



Finally, if we combine these two analyses and examine darknet markets' net sending relationship with different cryptocurrency service types — meaning, the amount darknet market addresses receive from each service type minus what they send — and compare the results with other crime types, we see that darknet markets have an interesting relationship with cryptocurrency ATMs.

Criminal wallets' net value received by service type | 2020



Currencies included: BAT, BCH, BTC, ETH, LTC, MKR, OMG, PAX, TUSD, USDC, USDT

On the chart above, a bar with a positive value means addresses in that crime category received more than they sent from that particular service type, and a negative value means they sent more. It's no surprise that every crime category has a negative net sending relationship with mixing services. Mixers are typically used to launder criminal funds, so it makes sense that illicit addresses would be sending more to mixers than they get back. But we also see that as a category, darknet markets received over \$16.5 million on net from cryptocurrency ATMs. No other crime category-service pair had a similar relationship with ATMs. This could suggest that darknet market customers are funding their buying activity in fiat by depositing it at cryptocurrency ATMs, unlike those sending funds to addresses associated with other types of crime.

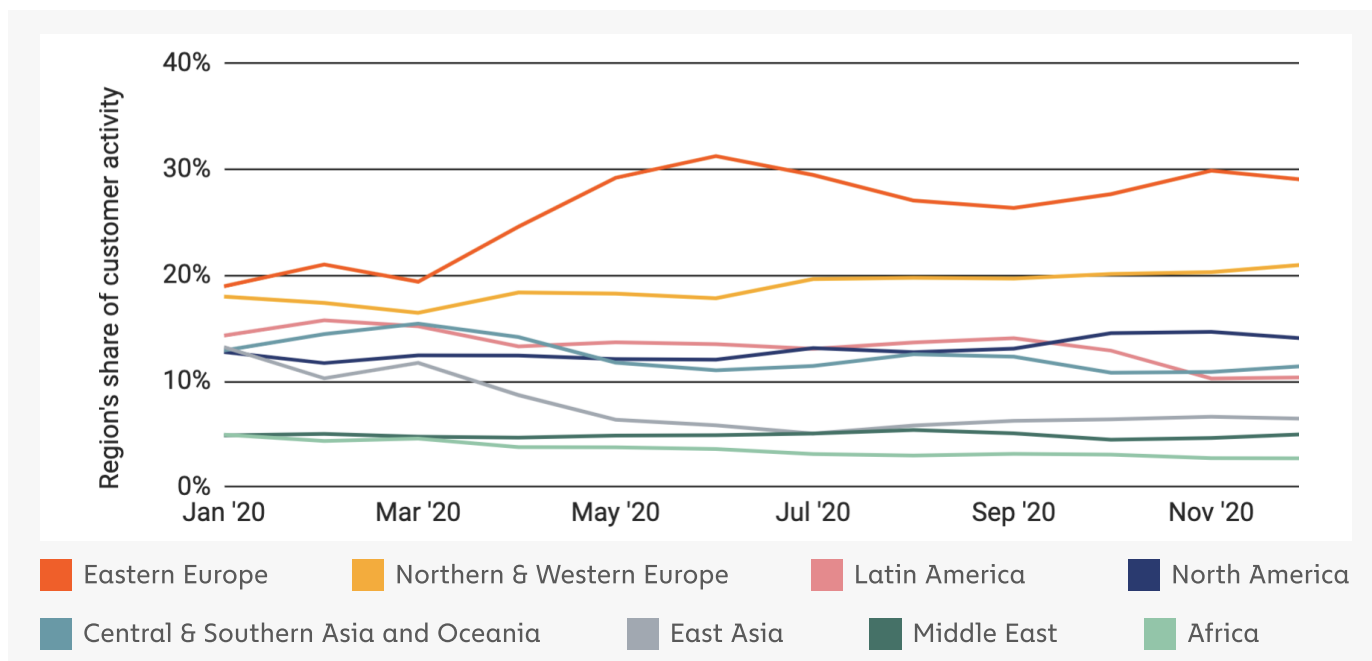
Geographic trends in darknet markets

Looking at transaction data across all darknet markets, we see that users in Eastern Europe, Northern & Western Europe, and North America are the biggest darknet market customers, based on the specific services that have sent the most cryptocurrency to darknet markets.



Value sent from drug-focused darknet market customers by region

|2020

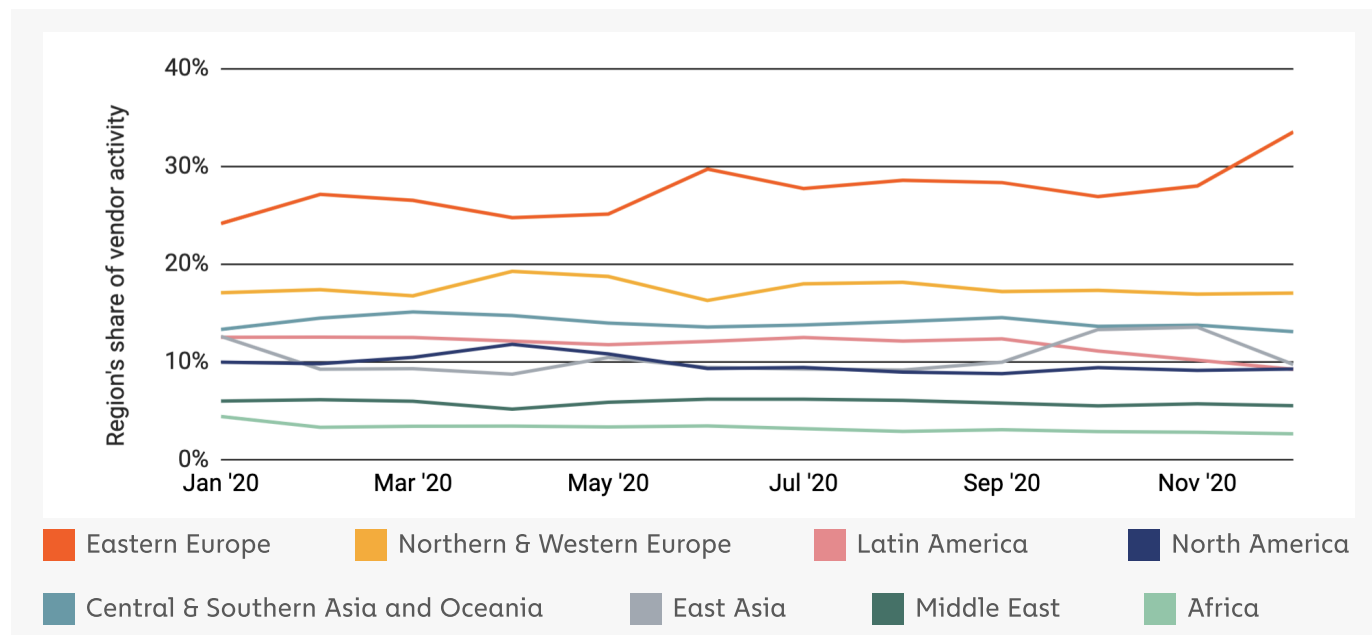


Currencies included: BCH, BTC, ETH, LTC, OMG, PAX, USDC, USD

Eastern Europe also receives by far the most value from darknet market vendor addresses, though much of this is due to massive volumes from Hydra, whose size makes it a major outlier. Northern & Western Europe receives substantial amounts as well, as does Central & Southern Asia and Oceania, East Asia, Latin America, and North America.

Value sent from drug-focused darknet market customers by region

|2020

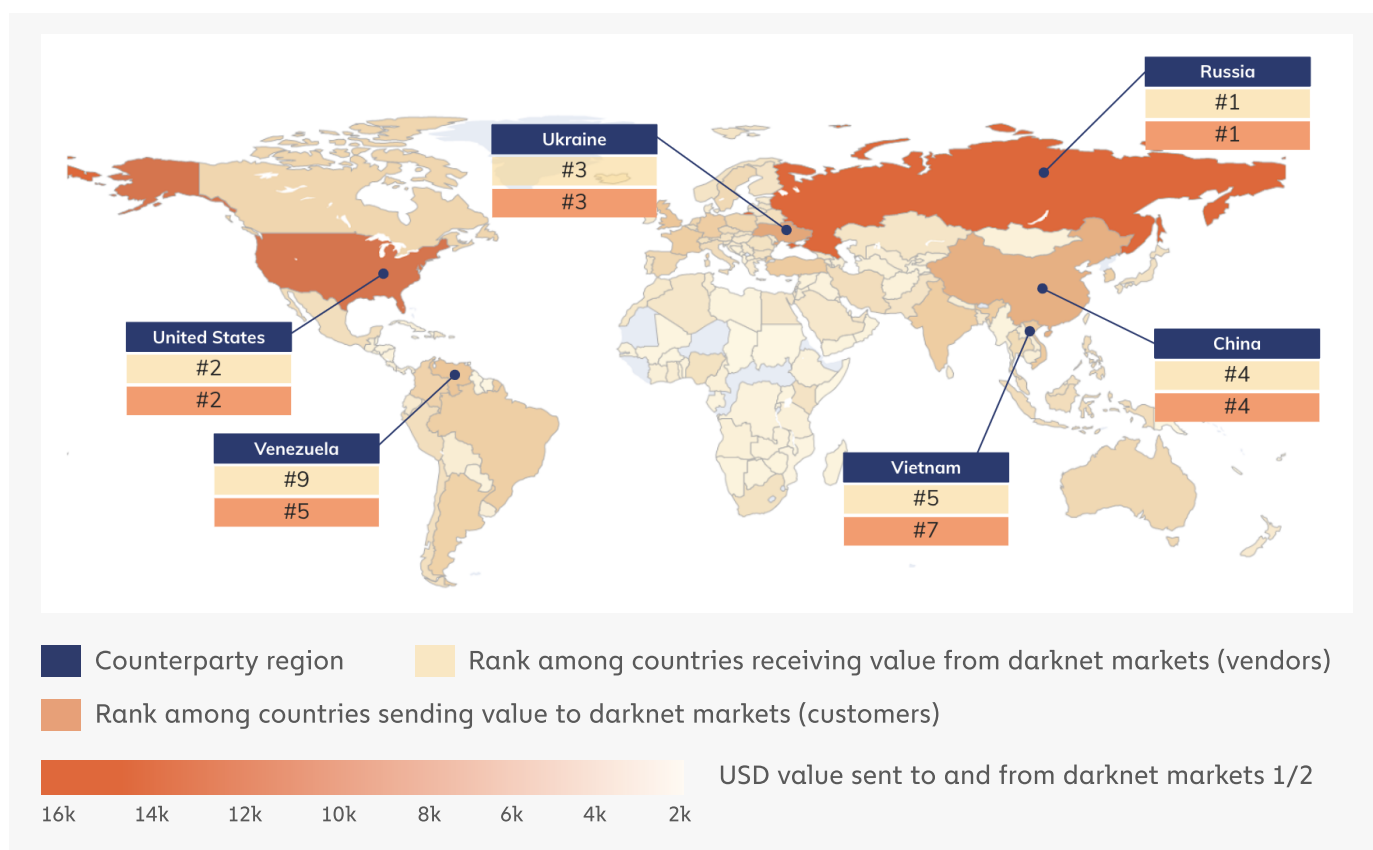


Currencies included: BTC, BCH, LTC



That pattern fits with what we know about the geography of the global drug trade. Broadly speaking, drugs are grown or manufactured in [Latin America and Asia](#) and consumed in North America and Northern & Western Europe. Darknet vendors and administrators typically launder funds through cryptocurrency services — often over-the-counter (OTC) brokers — in [China](#) or [Eastern Europe](#). We can see some of this activity in the blockchain data associated with darknet market transactions. On the map below, we show some of the most active individual countries' exposure to darknet markets in terms of value both sent and received.

Top countries by value sent to or received from drug-focused darknet markets | 2020



The geographic flows involving darknet markets roughly match what we would expect to see. The United States, Russia, Ukraine, and China dominate in terms of value both sent to and received from darknet markets. Venezuela and Vietnam also rank high on both sides, with their activity skewed slightly more toward darknet market buying, which could be related to the drug manufacturing activity prominent in both countries. We also suspect that a good deal of China and Russia's volume received by darknet markets represents funds flowing to money laundering services concentrated in those countries.

In the table below, we show the top ten countries by total cryptocurrency transaction volume flowing through darknet markets, with links to relevant news stories we believe exemplify each country's activity and role in the global drug trade.



Country	Value sent to darknet markets	Value received from darknet markets	Total value sent to or received from darknet markets	Rank of values (of 171 countries)			Examples and notes
				Value sent to darknet markets	Value received from darknet markets	Total value	
Russia	\$169 M	\$119 M	\$288 M	1	1	1	Thanks to Hydra Marketplace, Eastern Europe is the only region with a criminal service as one of the top ten entities sending cryptocurrency value to the region.
United States of America	\$115 M	\$64 M	\$179 M	2	2	2	A Costa Rican pharmacist and a co-conspirator were indicted in a US court for selling hundreds of thousands of opioid pills worth millions of dollars to US darknet market customers.
Ukraine	\$47 M	\$52 M	\$98 M	3	3	3	Ukraine tops the Chainalysis Global Crypto Adoption Index which measures grassroots adoption, including exposure to Hydra Marketplace which Ukraine shares with Russia and other countries in Eastern Europe.
China	\$45 M	\$43 M	\$87 M	4	4	4	Illicit proceeds are often laundered through OTC brokers based in China, a pattern that is also seen with fiat currency.
United Kingdom	\$33 M	\$22 M	\$56 M	6	6	5	170 arrested and \$6.5 million seized after law enforcement blew up ring importing MDMA from China and Canada to sell in US, UK and continental Europe.
Venezuela	\$35 M	\$20 M	\$55 M	5	9	6	Former President of Venezuela Nicolás Maduro Moros and top government officials charged with narco-terrorism, corruption, drug trafficking.
Vietnam	\$24 M	\$24 M	\$49 M	7	5	7	The most common material on Vietnamese darknet markets are narcotics, cryptocurrency exchange sites, and child abuse material.
Turkey	\$23 M	\$22 M	\$45 M	11	7	8	Drug trafficking has been a big problem in Turkey for a long time.
India	\$24 M	\$18 M	\$42 M	8	13	9	In a first, Indian drug vendor operating on Empire Market and Majestic Garden was arrested for shipping drugs to the US, UK, Romania, and Spain among other countries.
Germany	\$23 M	\$18 M	\$42 M	10	11	10	Last year, the Dutch police and Europol arrested three men in Germany for running Wall Street Market. Germany has the third highest daily average TOR users after the US and Russia as of 2020.

Currencies included: BCH, BTC, LTC, USDT



It will be interesting to observe in 2021 and beyond how these currency flows change if more of the global drug trade continues to move to cryptocurrency, particularly on the money laundering side.

Market closures: Covid is causing shipping issues, but natural competitive forces are causing darknet market consolidation

As we mentioned above, while darknet market revenue in 2020 surpassed that of 2019, the overall number of purchases, and likely customers as well, has fallen significantly, though the remaining purchases are for higher values. Similarly, the number of active markets has fallen, with several prominent ones shutting down and fewer new ones popping up to take their place.

Why is this happening? One might think the ongoing Covid crisis is the obvious answer. As we'll explore below, the pandemic has indeed strained postal systems around the world, leading to delivery failures and delays for many darknet market vendors. But the experts we spoke to don't think that Covid is to blame for this year's rash of market closures. Instead, it appears that ever-increasing competition combined with the efforts of law enforcement are causing the darknet market ecosystem to consolidate to a few big players — a pattern familiar to the technology industry and other markets, both legal and illegal. Below, we'll share our findings on darknet market activity in 2020, how it's changed throughout the pandemic, and provide possible reasons for why so many markets have closed.

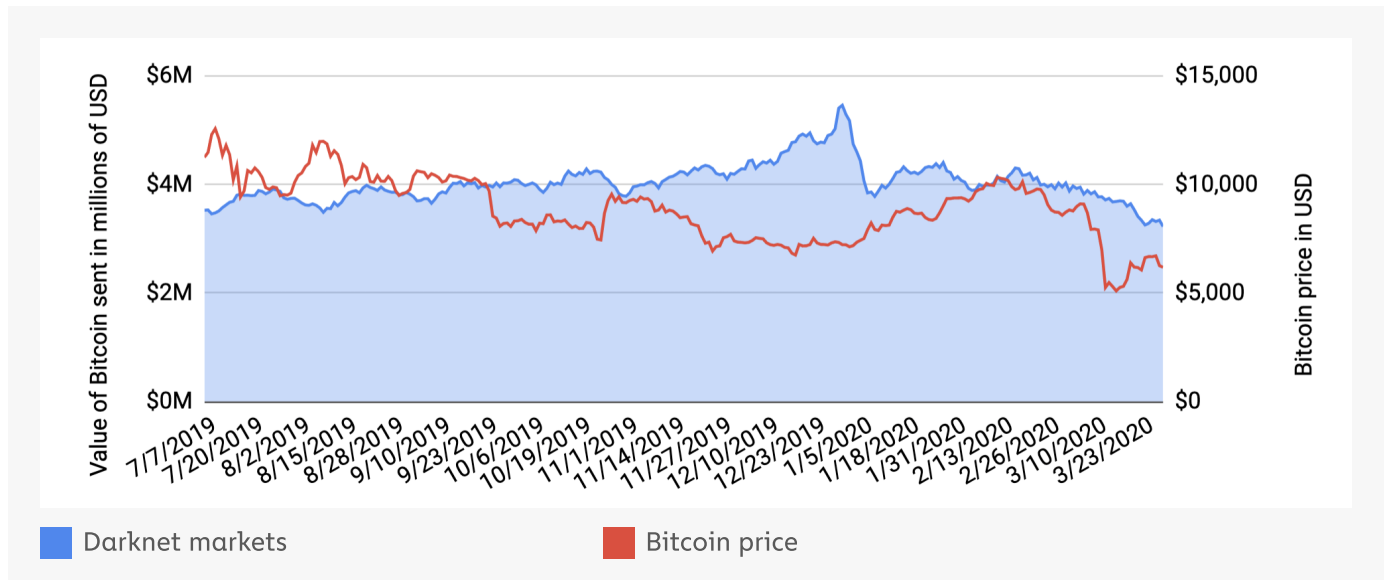
Darknet markets' initial reaction to the Covid pandemic and trends since March

Earlier this year, roughly three weeks after lockdowns began in the United States, [we examined the pandemic's effects on darknet market activity](#) and found that transaction volume had dropped following a sharp decline in the price of Bitcoin and other cryptocurrencies.



Value of Bitcoin sent to darknet markets, 7-day moving average

| Jul '19 to Mar'20



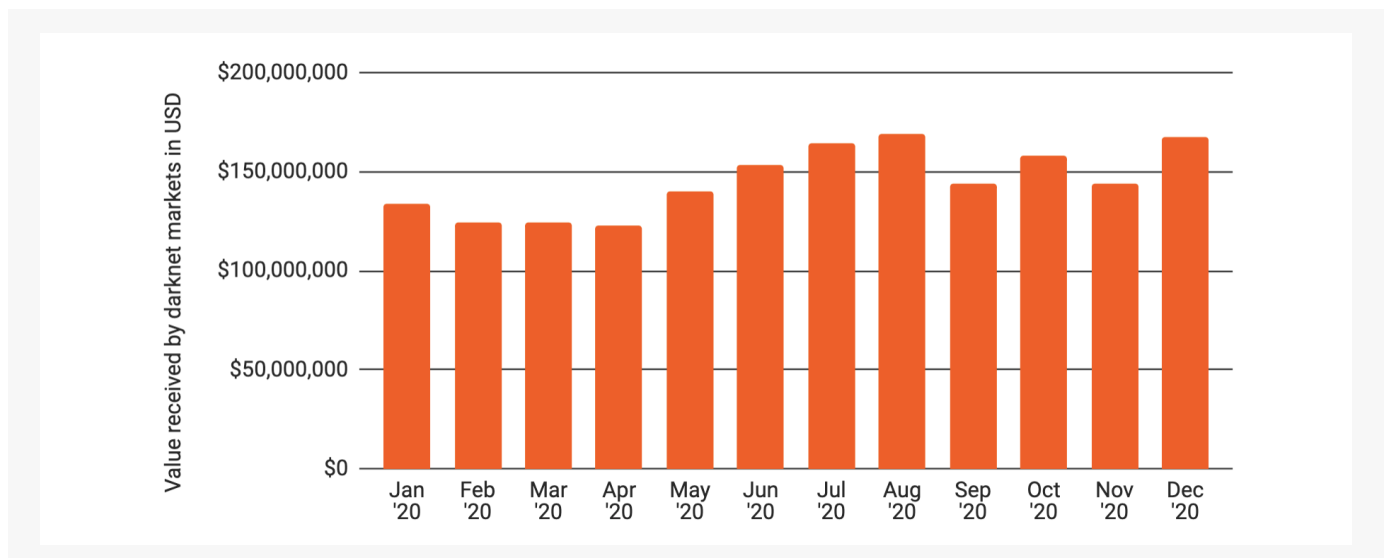
55

Currencies included: BCH, BTC, LTC, USDT

Notable in our findings was that up until this point, darknet market activity appeared to be impervious to Bitcoin market activity. Fluctuations in Bitcoin's price, which have always been common, rarely appeared to play a role in darknet market consumers' purchasing activity. However, when Bitcoin's price began to fall in mid-March following the first round of U.S. lockdowns, so too did darknet market activity.

But this change would prove to only be temporary. Starting around May, darknet market revenue returned to its previous state, no longer shifting in sync with Bitcoin's price. Since then, darknet markets' monthly revenue has steadily grown, save for small drops in September and November, which largely fall in line with seasonal trends.

Monthly darknet market revenue | 2020



Currencies included: BCH, BTC, LTC, USDT

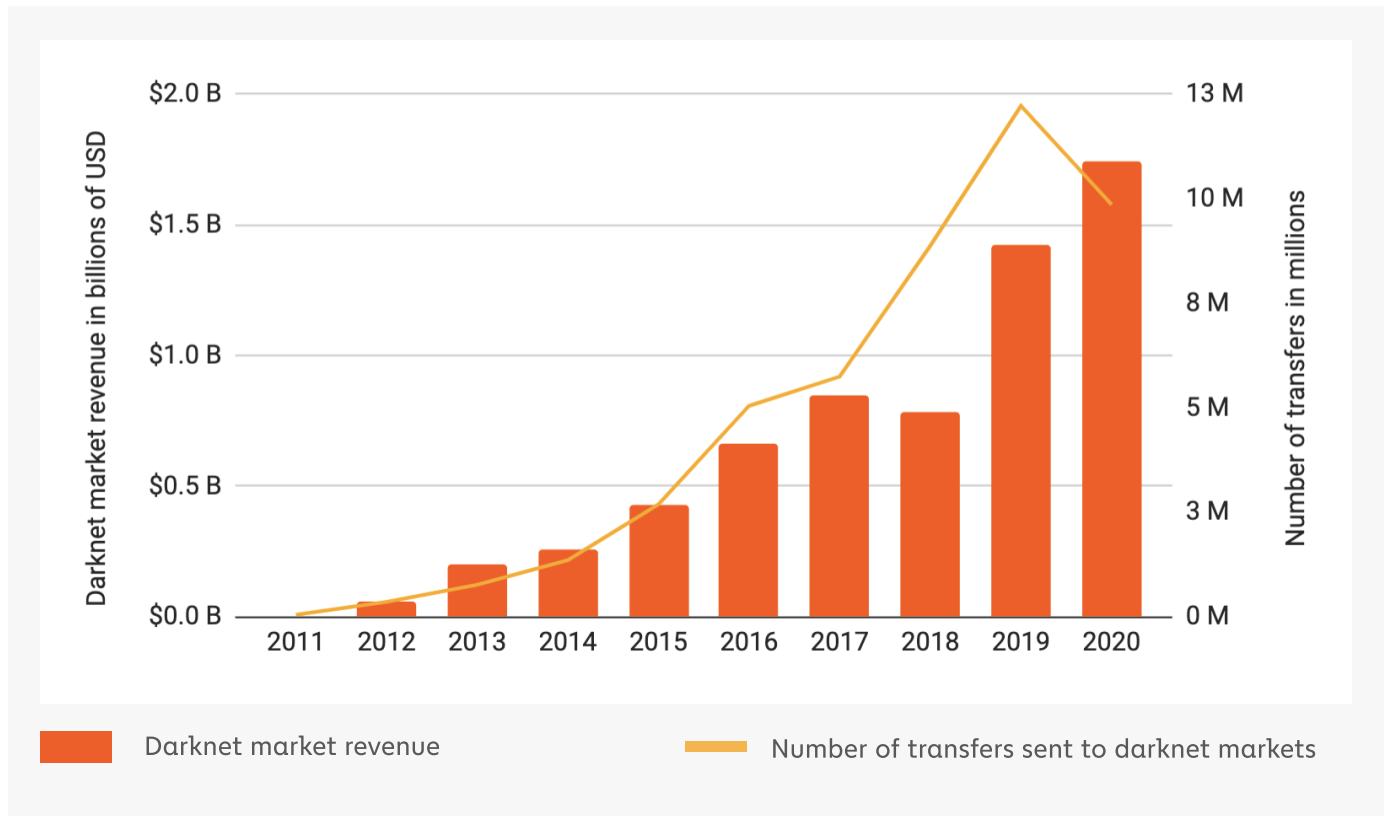
54



With these latest developments, overall darknet market revenue for 2020 surpassed that of 2019. But while total revenue may not change, other numbers indicate that tough times could be ahead for darknet markets.

Darknet market revenue vs. Total transfers to darknet markets

| 2011-2020



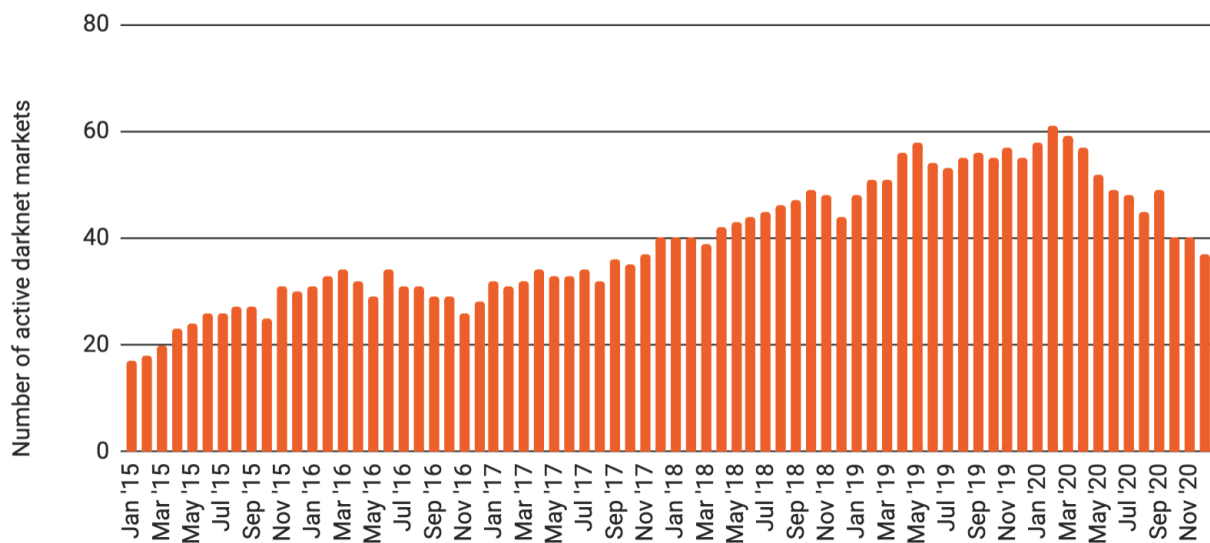
Currencies included: BCH, BTC, LTC, USDT

The graph above shows both total darknet market revenue by year, as well as the total number of transfers to darknet markets, which we can use to roughly approximate the number of individual customers and purchases. Interestingly, we see that while revenue surpassed its 2019 total, total transfers to darknet markets stand at just under 10 million — well below the 2019 total of over 12.0 million. The numbers show that customers in 2020 are making fewer purchases but for larger amounts per purchase compared to 2019. This could indicate that casual buyers or those buying drugs for personal use are shifting away from darknet markets, while those buying in larger amounts — either for personal use or to sell to others — are purchasing more. It could also mean that some casual buyers have begun placing larger orders to stock up amidst uncertainty.

We've also seen more darknet market closures in 2020, including prominent markets like Flugsvamp 2.0 and Empire. We see this reflected in the graph below, which shows the number of active markets in each month (active meaning the market has received at least \$100 worth of cryptocurrency in a given month) since January 2015.



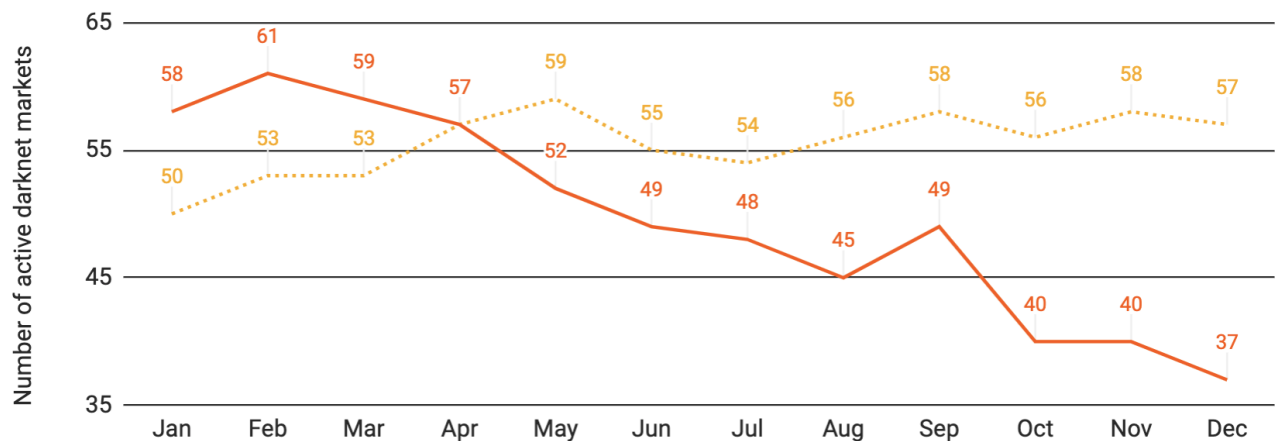
Number of active darknet markets | 2015-2020



Currencies included: BCH, BTC, LTC, USDT

While some markets claim their closures are only temporary, the 37 darknet markets active in December 2020 is the lowest total since November 2017. We saw no such decline in 2019. In fact, this year's decline in active markets follows a period of modest growth in the number of active markets from 2018 through February 2020.

Number of active darknet markets: 2019 vs. 2020



2020

2019

Currencies included: BCH, BTC, LTC, USDT




It's often difficult to tell why markets shut down when they do, as administrators commonly pull exit scams, in which the market ceases operations but publicly appears to still be active so that administrators can continue collecting money from purchases that will never be fulfilled. Other markets have fallen victim to denial-of-service (DoS) attacks from other markets, in some cases closing as an apparent result. We saw both phenomena in the case of Empire Market, a large and widely trusted darknet market whose operators [exit scammed](#) in 2020 two days after being hit by a DoS attack.

Is Covid causing darknet markets to close?

Covid has undoubtedly hindered darknet markets' sales and operations by causing supply chain disruptions, particularly shipping delays. Darknet market observers have seen this in the form of customer complaints on darknet market-focused forums like Dread and in notes from vendors setting expectations for buyers.

+Drugs

High Heat Bolivian Cocaine 1 Gram



Sold by: JefeJedi
Trust rating: High
Feedback score: 98
[Contact JefeJedi](#)
[View JefeJedi's profile](#)

Buy now

140 CAD

105 USD

You are protected by ESCROW

Product Description

Refund Policy

Seller's Feedback

What we have here is some Premium Top Shelf, High Heat Cocaine.

With Covid19 causing massive interruptions across the nation, i am still trying my best to keep prices Reasonable but competitive.

You will receive 1 Grams of what you see here discretely and quickly shipped to your address with tracking. Item as pictured more Below:

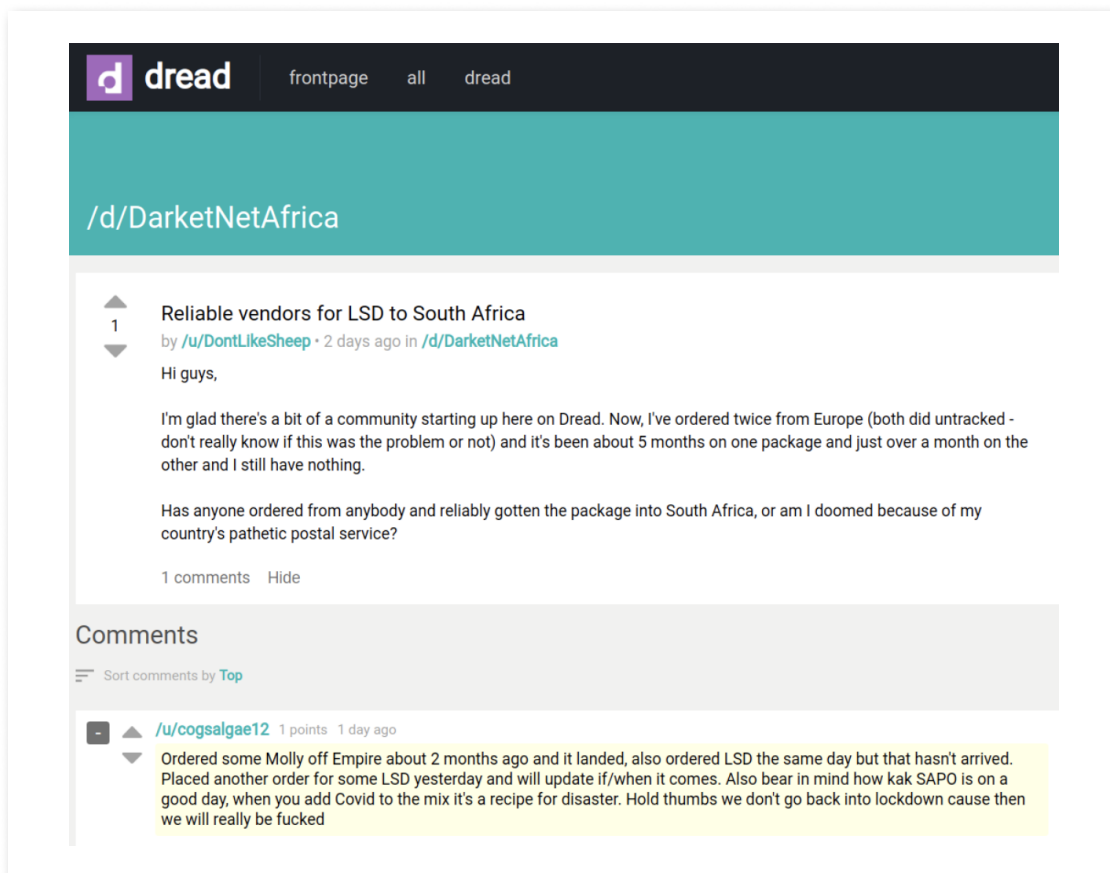
<https://ibb.co/TgK10vH>
<https://ibb.co/cxcvQYR>
<https://ibb.co/Kq0KsHC>
<https://ibb.co/8MDBqRw>
<https://ibb.co/xfJt791>
<https://ibb.co/cthP90d>
<https://ibb.co/lys3Zm2S>

Standard shipping Rate in Canada is \$30, this covers your Xpresspost™ envelope, the bubble envelope, the vacuum seal and your tracking number. this method covers all products under and up to 500g (five hundred grams) from East Cost to West Coast. For orders that exceed these parameters, different methods would be used.

Due to COVID19 interruptions, Canada post is not guaranteeing two business day delivery for the time being. Canada Post deliveries outside of Ontario could now take 2-5 business days, which isn't too bad at all. (SUPPORT CANADIAN BUSINESS!)

A darknet market vendor warns prospective buyers of shipping delays

58



Darknet market customers blame Covid for delayed orders

The evidence isn't just anecdotal either. Criminology researchers Andréanne Bergeron, David Décary-Hétu, and Luca Giommoni recently [published a study](#) analyzing hundreds of darknet market drug sales made before and after Covid lockdowns began in the U.S. and Europe to determine how much the virus impacted operations. They found that in the pre-Covid period of January 1 to March 21, 2020, between 60% and 100% of all orders on any given day were successful. After Covid lockdowns began, however, the study found that just 21% of all deliveries were successful and on time. Customers and vendors blaming Covid for longer delivery times therefore appear to be correct.

But are shipping delays and other Covid-related operational difficulties causing markets to shut down? We followed up with Lecturer Andréanne Bergeron and Professor David Décary-Hétu, two of the researchers behind the study, to ask their opinion. They reiterated their point that Covid has caused ongoing darknet market delivery delays by placing more strain on postal services. "The world hasn't gone back to normal yet, so it is unsurprising that the market hasn't corrected itself yet. Postal services aren't doing great," said Bergeron.



However, the researchers didn't think that any of the darknet market closures in 2020 were a direct result of Covid. "It's becoming more challenging than ever to run a darknet market — you have to enable security and guard against DoS attacks, and then on top of that there's competition. All of these factors limit the availability of drugs," said Décary-Hétu. He believes that these natural forces of competition, rather than the Covid crisis, were the real reason for increased closures, pointing to Chainalysis data to make his point.

"Excluding Hydra, if all darknet markets take in \$250 million per year and administrators make 5% commission, that's \$12.5 million total divided by all the markets, where a lot of employees have to be paid. It's simply not worth the risk of spending 100+ years in jail," said Décary-Hétu.

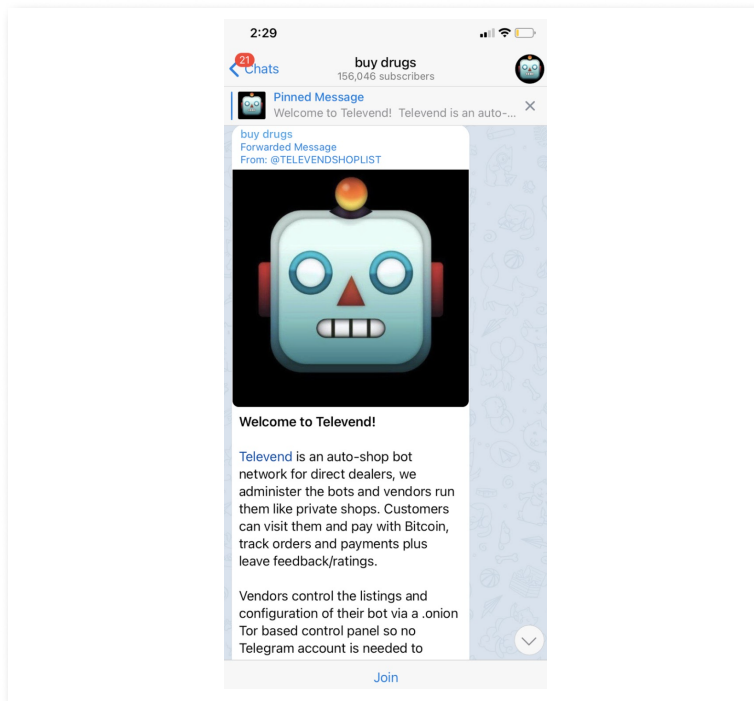
Will more darknet markets fail?

Darknet markets appear to be in a precarious position in 2020, with several closing down and the remainder relying on a shrinking pool of customers for revenue. Counterintuitively, and despite its impact on shipping times, Covid doesn't appear to be the primary cause of these issues. Instead, darknet market consolidation may be the result of competitive forces endemic to the category itself, with Covid at most simply speeding up a trend that already existed.

We see a similar dynamic play out in so-called [winner-takes-all markets](#) like technology, in which competition over time naturally whittles the market down to the biggest, most efficient players. There are, of course, key differences between darknet markets and technology companies — Apple, for instance, doesn't need to worry about being shut down by law enforcement. But still, as Professor Décary-Hétu points out, darknet markets are a tough business, and the dwindling number of markets suggests that not all of those standing today will survive.

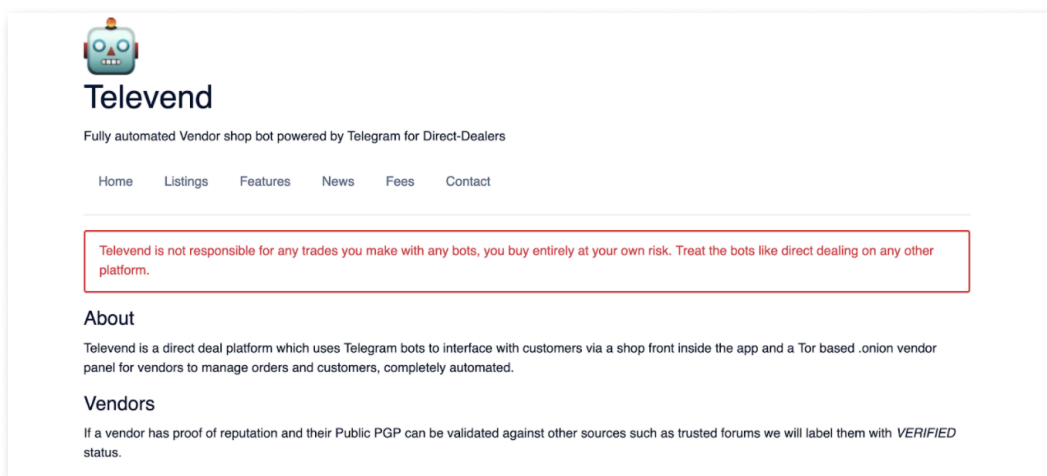
Decentralization is the next step for darknet markets

Despite 2020's difficulties, a new decentralized model embodied by platforms like Televend may solve many of these problems for darknet markets. Televend is a Telegram-based platform with over 150,000 users where darknet market vendors can sell drugs through automated chatbots, whose communications with buyers are highly encrypted.



A screenshot of Televend

Buyers simply access Televend's Telegram group, where they find a directory of drug vendors broken down by region and products on offer. From there, they simply place orders with their chosen vendor's chatbot, receive an automatically-generated Bitcoin address to which they send payment, and wait for their drugs to arrive in the mail.



A screenshot from Televend's darknet site



Fees/Top-Up

As our bots are direct payment only. We charge our fees by collecting them in advance. You top up your balance like a prepaid card and it gets used according to your sales turnover. We charge 1-4%. So if you top up €500, you can do €12,500-€50,000 in sales before your balance reaches 0 and you need to top up again. We track your sales via incoming payments to your bitcoin wallet linked to orders made through the bot.

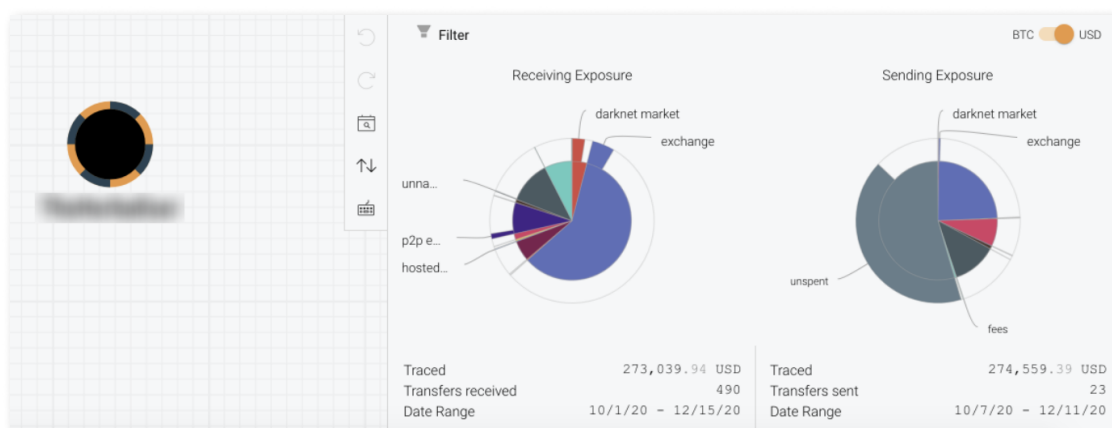
FEE STRUCTURE

Monthly sales revenue/fee %
0-50k = 4%
50k-75k = 3%
75k-100k = 2%
100k+ = 1%

Televend's fee structure explained

Televend receives commissions on each sale, but never actually touches the funds, so there's no central entity for law enforcement to track through blockchain analysis – the transactions blend in much more easily.

We studied the Bitcoin transaction history of one prominent Televend vendor, which you can see a summary of in the [Chainalysis Reactor](#) screenshot below.



Since Televend became active in October 2020, this vendor's wallet has received over \$270,000 worth of Bitcoin across nearly 500 transactions. Customers appear to have paid mostly through cryptocurrency exchanges, which is also where the vendor has sent most of the funds. However, while we don't show it above, this wallet has been active since June 2019 – Televend allows vendors to receive their earnings to any address of their choosing – and received an additional \$1.4 million worth of Bitcoin before Televend opened. It therefore appears likely that this vendor was active on traditional darknet markets before migrating to Televend. This vendor is one of over 150 active on Televend, though it's unclear if the others are bringing in as much revenue.

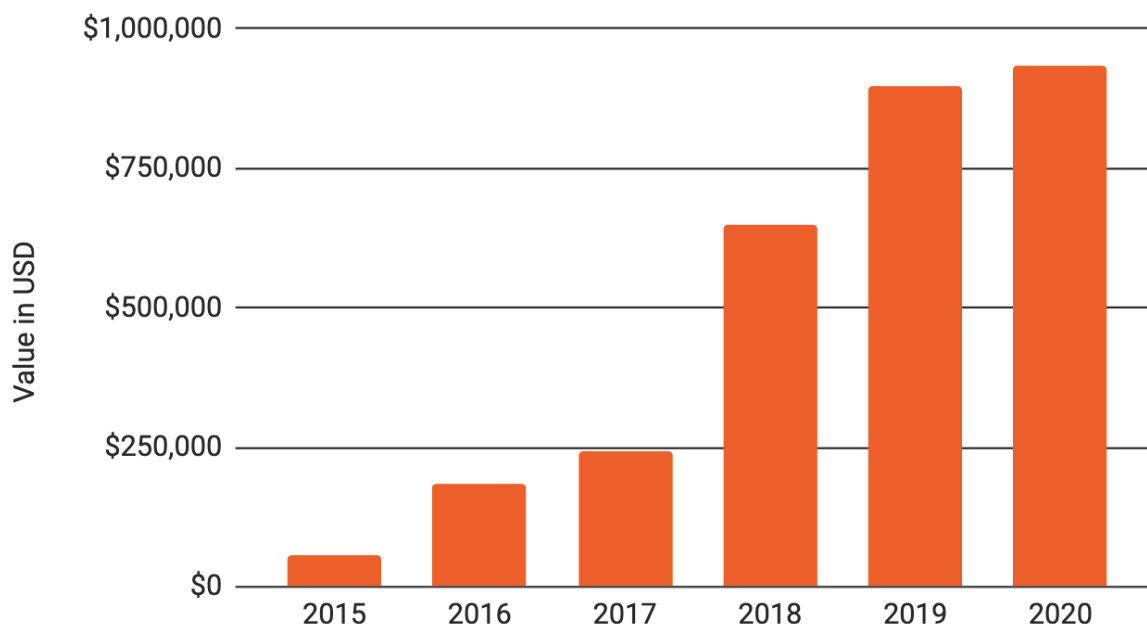
We expect platforms like Televend to grow and take in a larger share of total darknet market revenue in 2021, as their decentralized nature makes them more resilient to attacks from both law enforcement and rival markets. While future decentralized markets may run on platforms other than Telegram, Televend shows that the encrypted messaging platform can offer customers an easy buying experience.



Child sexual abuse material and darknet markets

Darknet markets selling drugs and stolen data take in the vast majority of funds going to this service category. But while their revenue remains minuscule compared to markets specializing in child sexual abuse material (CSAM), it is especially troubling.

Yearly revenue to child abuse material sites | 2015-2020



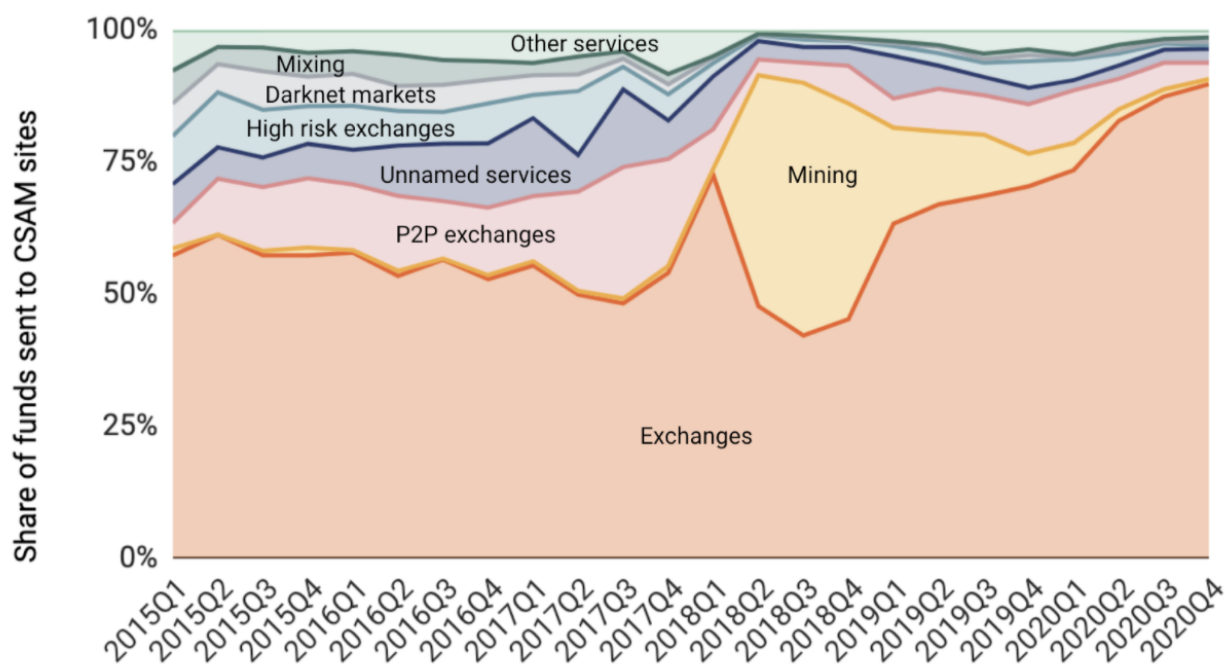
Currencies included: BCH, BTC, ETH, LTC, USDT, ZRX

As we see above, CSAM markets' revenue has increased each year since 2015. For clarification, these figures come from cryptocurrency addresses Chainalysis has attributed as belonging to CSAM markets in the course of our investigations alongside law enforcement, as well as from addresses flagged by [Internet Watch Foundation](#) (IWF), a UK-based non-profit dedicated to stopping the online proliferation of CSAM.

As is the case with most forms of cryptocurrency-based crime, payments to CSAM providers mostly come from exchanges. Similarly, CSAM addresses send most of the funds they receive to exchanges, which is presumably where they convert their cryptocurrency into cash.

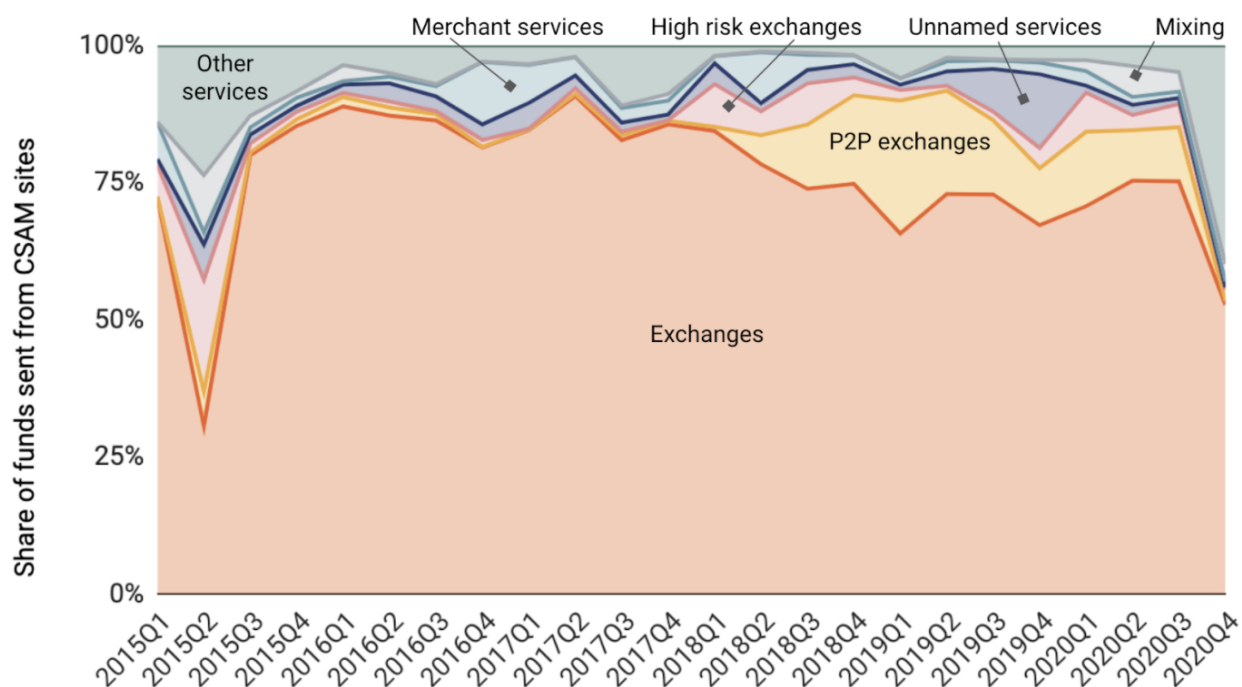


Origin of funds sent to child abuse material sites | 2015-2020



Currencies included: BCH, BTC, ETH, LTC, USDT

Destination of funds sent from child abuse material sites | 2015 - 2020



Currencies included: BCH, BTC, ETH, LTC, USDT



This isn't necessarily surprising, as it fits the wider patterns of cryptocurrency-based crime. Still, it's shocking that CSAM buyers and providers would use regulated, compliant exchanges, all of which collect KYC information (we count exchanges that don't in our "high-risk exchange" category), for such serious and rightly stigmatized criminal activity.

Case study: Dark Scandals

In 2019, Chainalysis helped strike a blow against CSAM on the darknet by assisting authorities in taking down [Welcome To Video](#), the largest ever Bitcoin-powered CSAM marketplace identified to date. In March 2020, we assisted in the takedown of another darknet market for CSAM: Dark Scandals.

Videos that are welcome:

Rules:

- Videos with real rape, blackmail, forced, or other rare material (blackmail would be better with chatlog))
- Bully videos with some nudity
- Real groped girls (not acted videos) (extreme kind)
- Real busted girl doing some nasty stuff (like busted sex with animal or something extreme)
- Real underground sold slave girl videos
- * This video has to be good quality (Not blurred out)
- * This video can not be found on other accesable sites
- * Your video is not already in the pack.
- * Only videos with face in it will be accepted
- We prefer own made material (If you have some material where you are also on it, and you want yourself out of the video, send the original, we will edit it how you want it and put it in the packs)
- * Please do NOT send videos with dead stuff, fake, amateur, masturbation or acted movies!
- (If the video is new to us, and also whats this site is about, you will receive the Darkscandal Packs)

If you want to give a financial contribution (for the Darkscandal packs) you can send the money to:

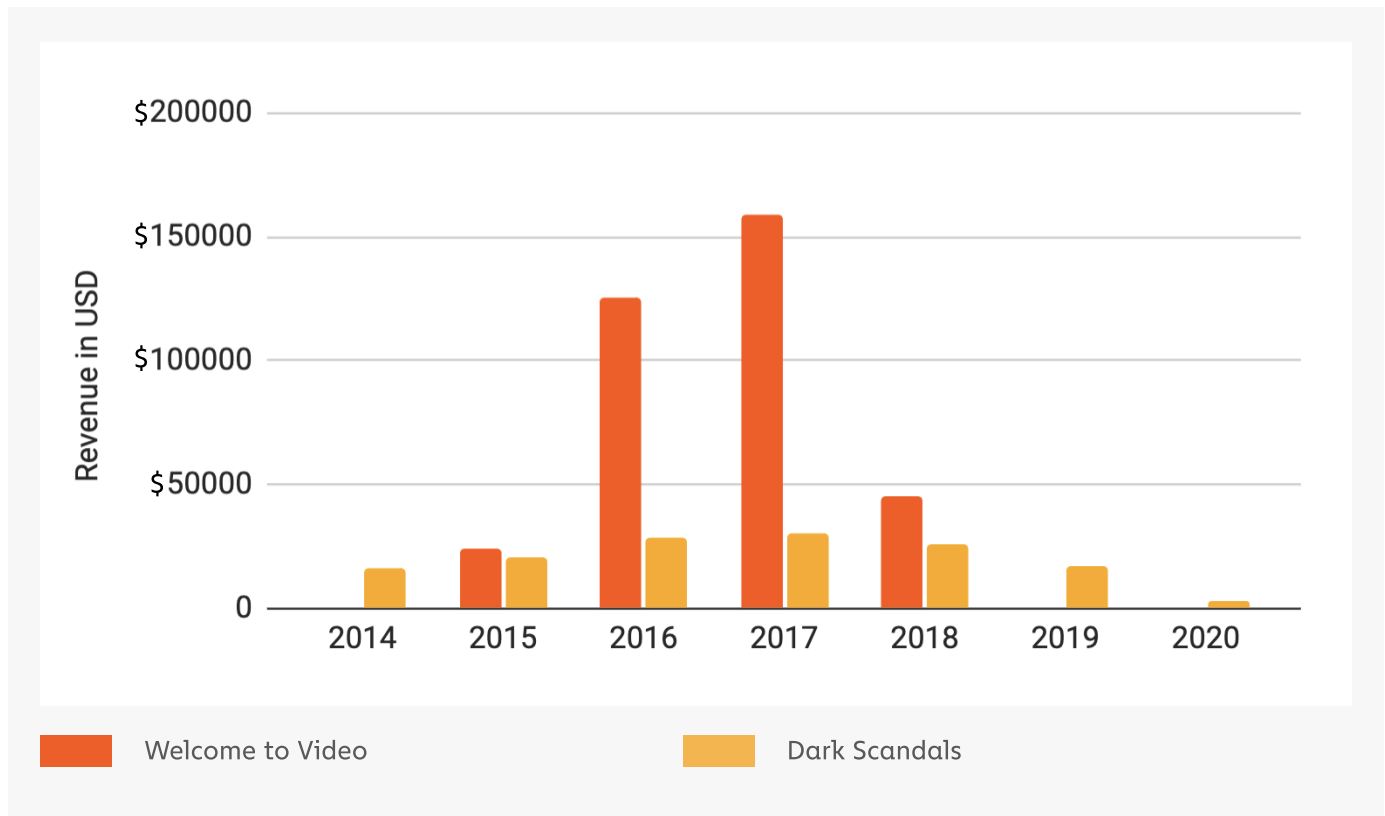
Using Bitcoins: send at least 0,04xxxx bitcoins to : 1Fiptr7bQdh6754yWzfmuytEe6ekihZ8V6
xxxx stands for a random number so we know the donation is from you (example 0.041247 Btc)([example here](#))
(After the payment send a email with your bitcoin number to my email:
(can be used by any clearnet or darkweb emailservice)
darkscandals @ bitmessage.ch
(after we verify your payment, we will email the Darkscandal Packs)

Instructions from Dark Scandals on the types of content users should upload

While Welcome To Video hosted more content than Dark Scandals and collected more revenue overall, the latter operated for longer and took in more money per transaction.



Yearly revenue to Welcome to Video and Dark Scandals | 2014-2020



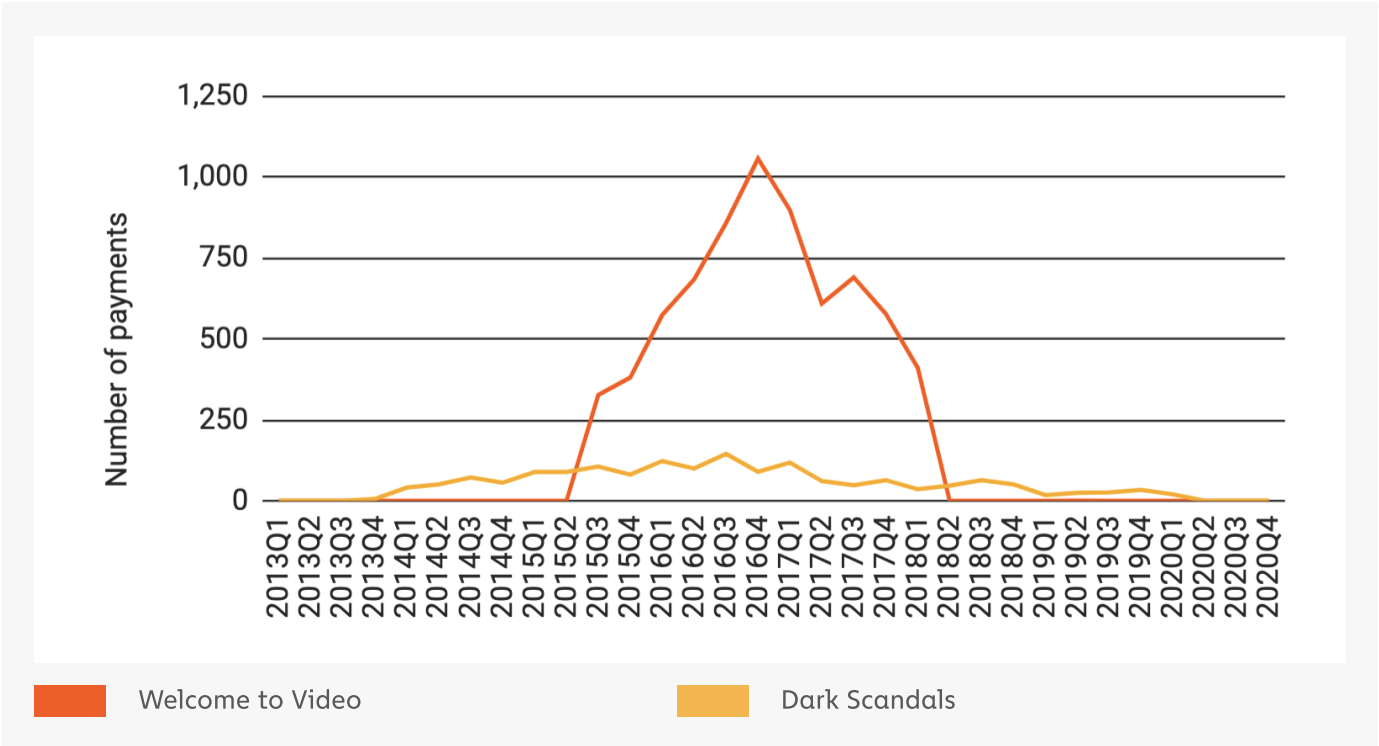
Currencies included: BCH, BTC, LTC, USDT

Overall, Dark Scandals took in just under \$143,000 worth of cryptocurrency revenue during its time active from 2014 to March of 2020. We spoke to Special Agent Chris Janczewski of the IRS Criminal Investigations unit that led the Dark Scandals and Welcome to Video investigations, and he told us a bit about how Dark Scandals worked. "Dark Scandals differed from Welcome to Video in that it was all or nothing. Customers could pay once and get access to nearly all of its material, whereas Welcome To Video functioned on a points system where users could upload their own videos or pay money, and use their points to acquire a bit of content at a time. It was common to see people pay into Welcome To Video multiple times, versus just once for Dark Scandals," he said. "The websites themselves varied also. The Welcome to Video site automatically distributed the content, while the Dark Scandals site was more of an advertisement, and the administrator had to manually distribute the content via email and file hosting sites."

We see this dynamic reflected in a comparison of the two platforms' cryptocurrency transaction history.

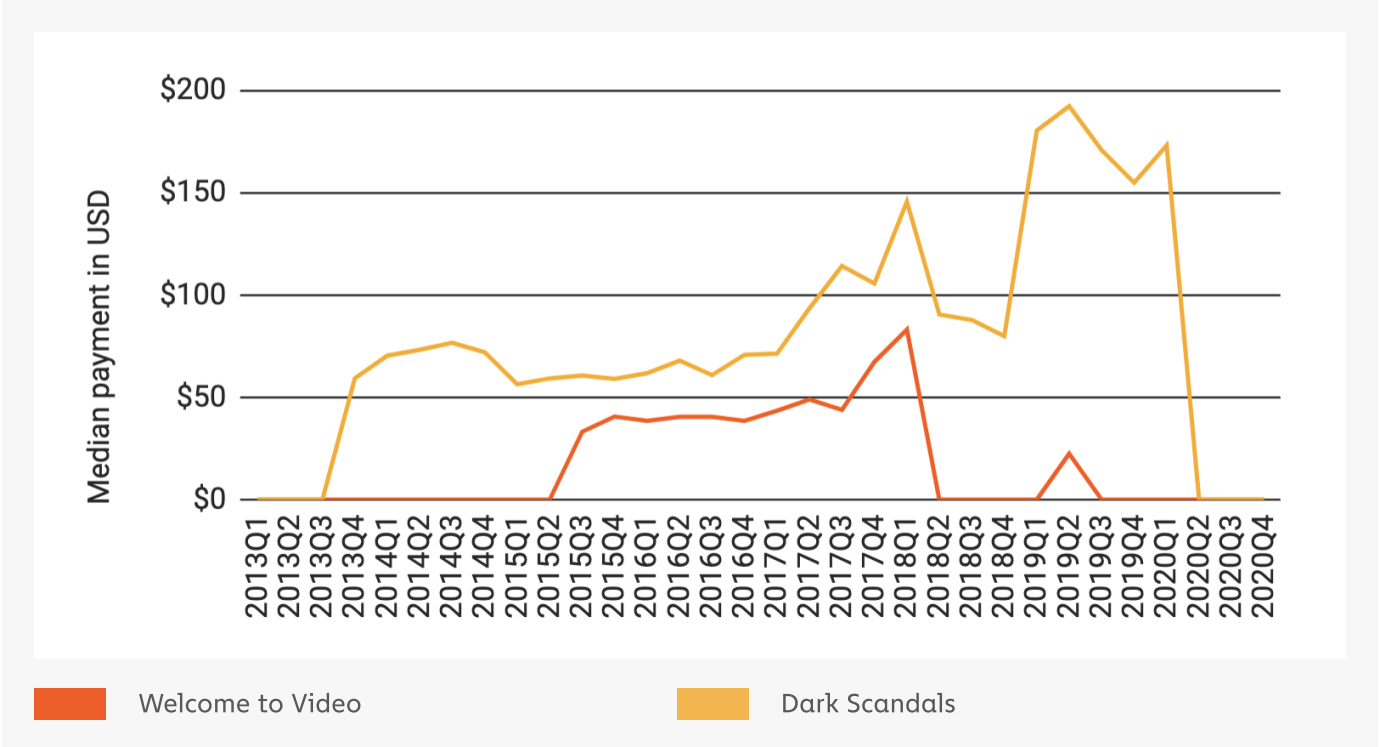


Quarterly number of payments sent to Welcome to Video and Dark Scandals | 2014-2020



Currencies included: BCH, ETH

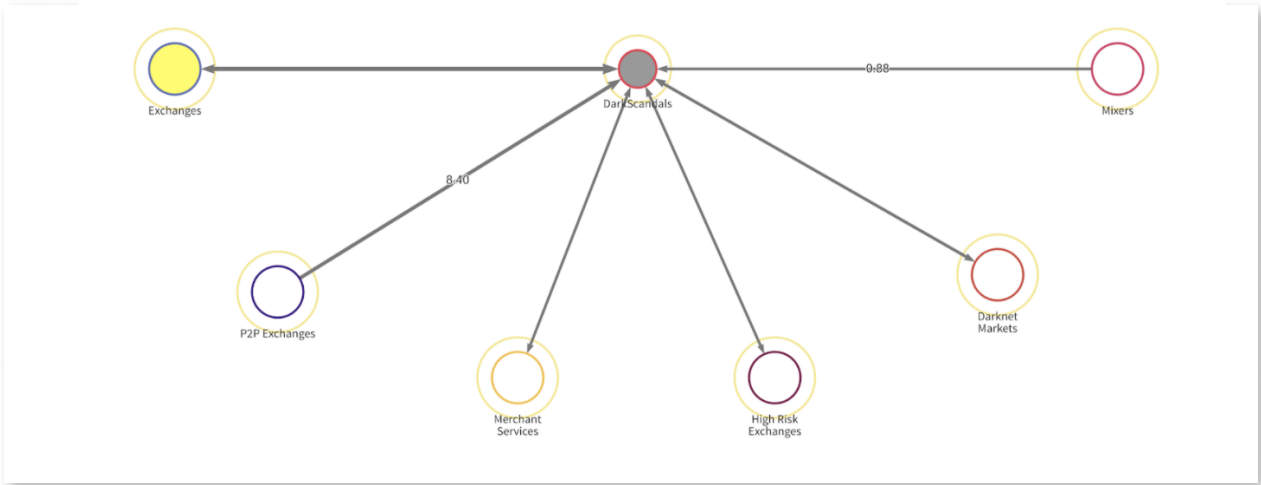
Quarterly median payment sent to Welcome to Video and Dark Scandals | 2014-2020



Currencies included: BCH, ETH

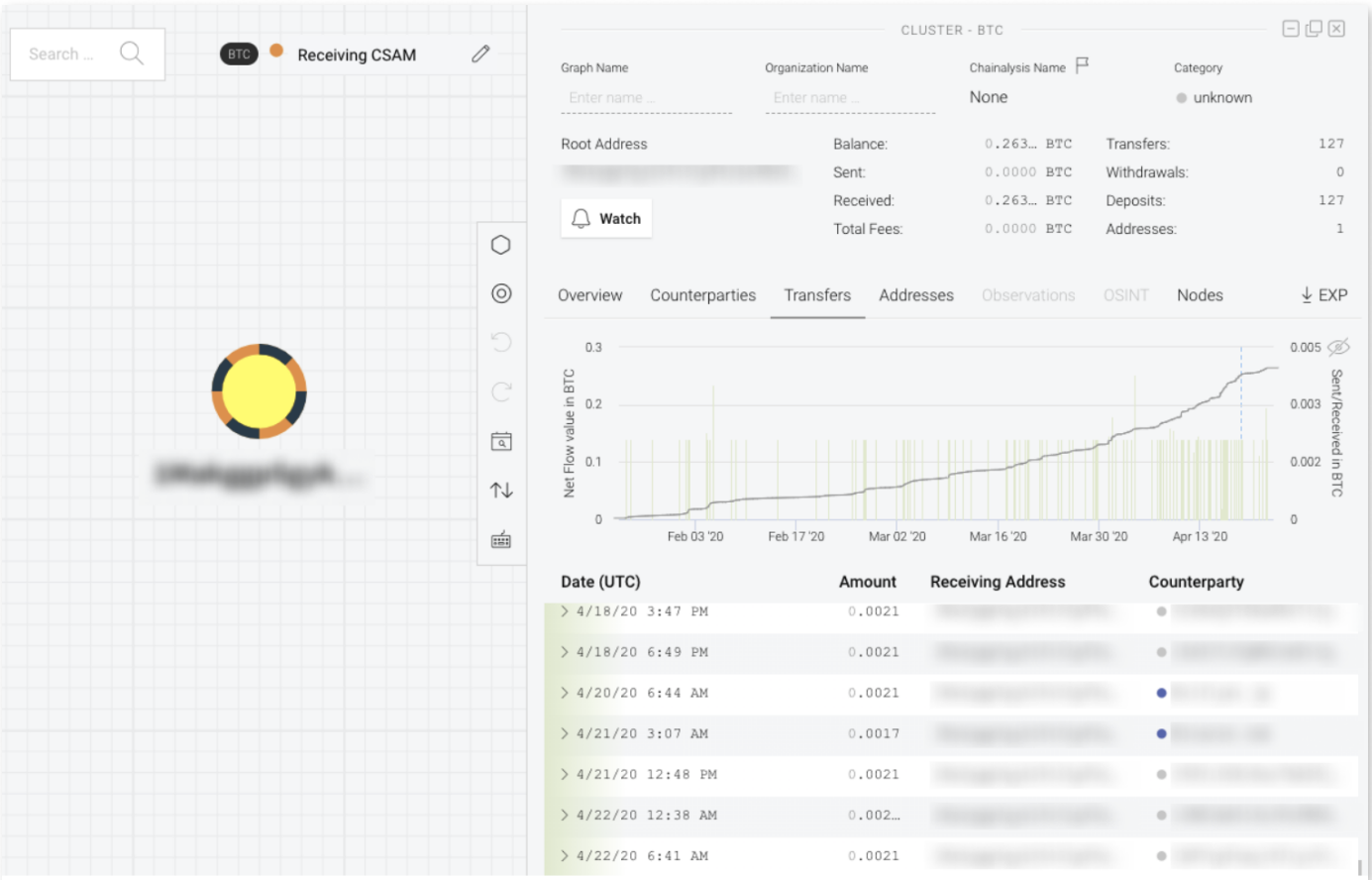


Dark Scandals received funds from a relatively small group of customers, who sent payments from a variety of different service types, with the majority coming from exchanges.



This Reactor graph aggregates the addresses that sent funds to Dark Scandals by service type

Law enforcement initially discovered Dark Scandals by analyzing the transaction history of an individual under investigation for purchasing CSAM from Welcome to Video and examining other addresses to which they had sent funds.





Note the uniformity of payments received by Dark Scandals. Nearly every one is equivalent to roughly \$15 worth of Bitcoin

Law enforcement agents made undercover payments to Dark Scandals in order to obtain and verify its customer-facing cryptocurrency addresses. Many of those addresses were hosted at compliant exchanges, so agents were able to subpoena them for the account holders' identity. Similar tactics, paired with other cyber-investigative techniques, allowed them to identify Michael Rahim Mohammed, a Dutch national, as the platform's alleged operator.

Since Mohammed's arrest though, Special Agent Janczewski notes that sites imitating Dark Scandals have popped up, at least some of which are scams. "There were no videos on the darknet version of Dark Scandals itself," Janczewski said. "The website advertised what addresses clients should make a payment to. Then the administrator replied to the client's email with a download link for a file hosting site so that the client could receive the content. It's been easier for scammers to spoof Dark Scandals versus Welcome to Video and trick people into paying." Chainalysis continues to track payments to Dark Scandals imitators and others alleged to monetize CSAM.

Overall, the takedown of Dark Scandals has Janczewski optimistic about law enforcement's ability to fight cryptocurrency-based CSAM markets. "Traditional CSAM investigators are working with cryptocurrency experts to get better at tracking transactions. Tools and educational efforts from blockchain analysis companies and government agencies have been invaluable," he said. "As the CSAM ecosystem adapts, so too does law enforcement."

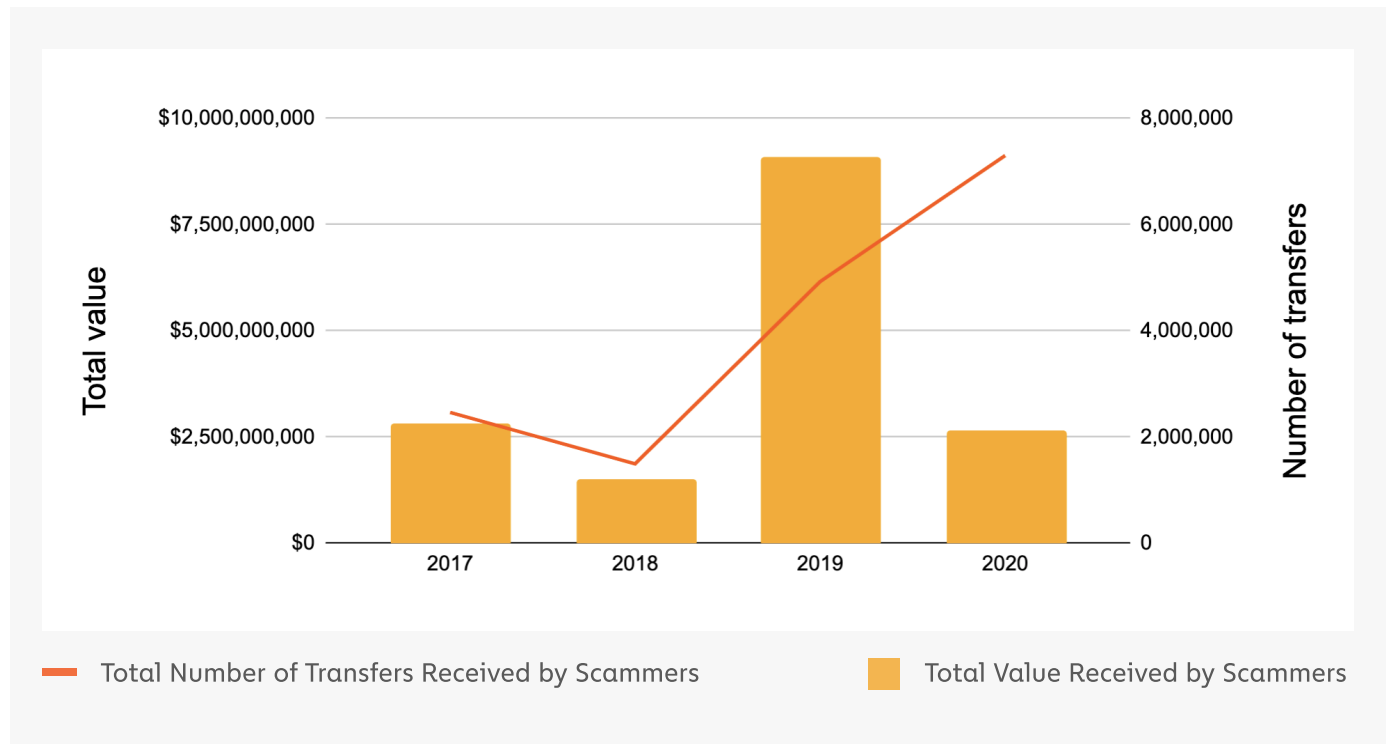


Scams



Cryptocurrency Scam Revenue Fell 75% in 2020 Despite Increase In Victims

Total cryptocurrency value received by scammers vs. Total Number of transfers to scammers | 2017 - 2020



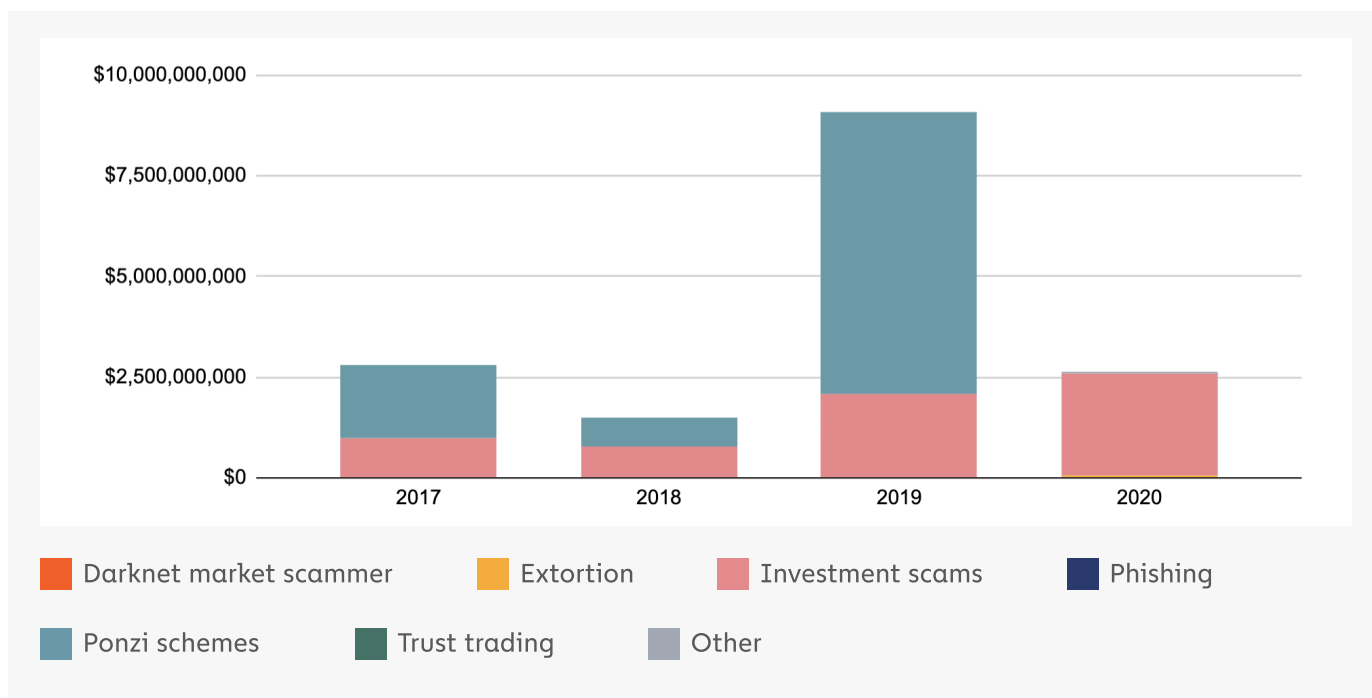
Currencies included: BCH, BNB, BTC, ETH, HT, LTC, MKR, OMG, PAX, TUSD, USDC, USDT

While scams remain the highest-grossing form of cryptocurrency-based crime, total scam revenue fell drastically in 2020, from roughly \$9 billion to just under \$2.7 billion. Interestingly though, the number of individual payments to scam addresses rose from just over 5 million to 7.3 million, suggesting that the number of individual scam victims rose by more than 48%.

Why did scam revenue decline even as the number of victims grew? The reason is that there were no large-scale Ponzi schemes like those we saw in 2019. Below, we break down yearly scam revenue by type of scam.



Total cryptocurrency value received by scam category | 2017 - 2020



Currencies included: BCH, BNB, BTC, ETH, HT, LTC, MKR, OMG, PAX, TUSD, USDC, USDT

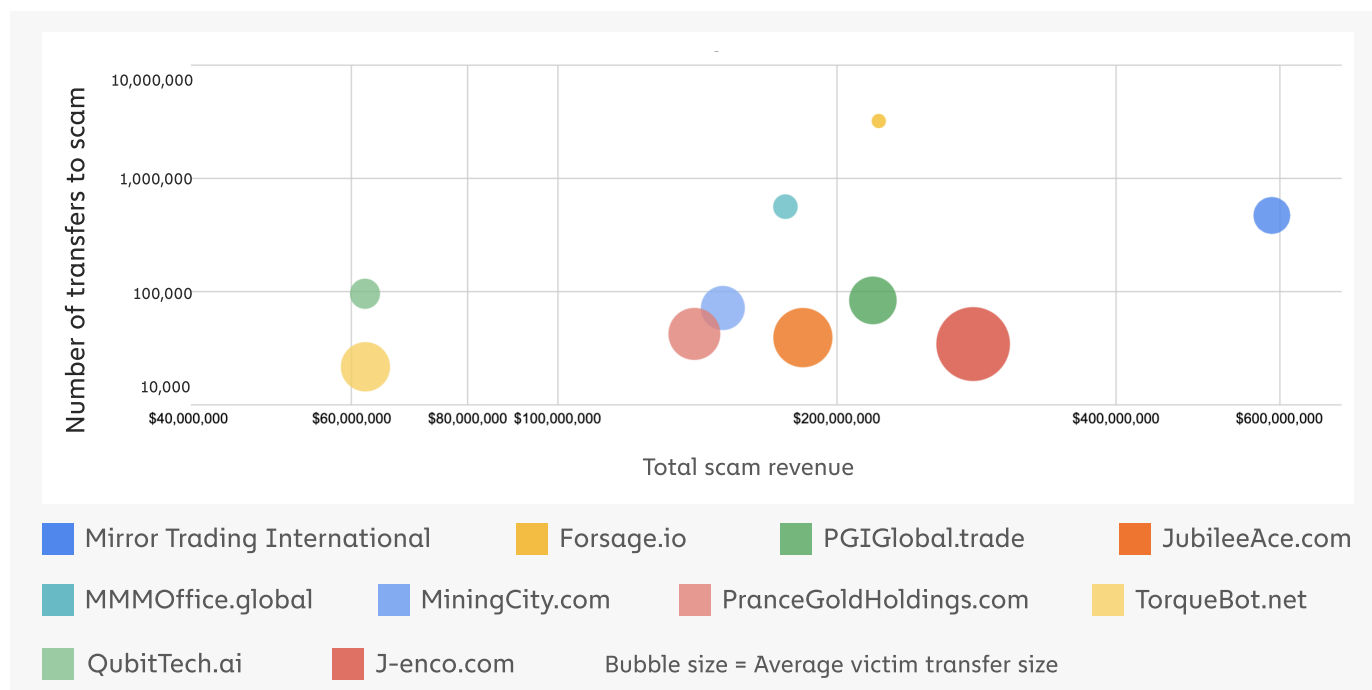
Ponzi schemes took in nearly \$7 billion worth of cryptocurrency in 2019, which is more than double what all scam categories made in 2020. Even more shocking is the fact that just six individual Ponzi schemes accounted for that \$7 billion. Most notable of the six was the infamous [PlusToken scam](#), a Ponzi scheme that reaped at least \$3 billion worth of cryptocurrency from millions of victims, mostly in Asia. Since we covered PlusToken in last year's Crypto Crime Report, Chinese authorities [have arrested](#) 109 individuals associated with the scam and prosecuted six of the most prominent.

Luckily, we're not aware of any other Ponzi schemes comparable to PlusToken that took place in 2020. This suggests that cryptocurrency users and the general public have grown more suspicious of such scams, or that potential Ponzi scheme operators have been scared off by the punishments doled out to the PlusToken operators.

Instead, nearly all scam revenue in 2020 went to smaller-scale investment scams. Investment scams have been a more consistent mainstay of cryptocurrency-based crime, as there are many more happening at any given time compared to Ponzi schemes. Unlike Ponzi schemes, these more generic investment scams don't tend to pay out fake proceeds to early investors and take in less cryptocurrency from each individual victim. We see this reflected in the graph below, which shows 2020's biggest scams — all of which are generic investment scams — broken down by total revenue, total victims (approximated by the number of individual payments), and average amount received per victim.

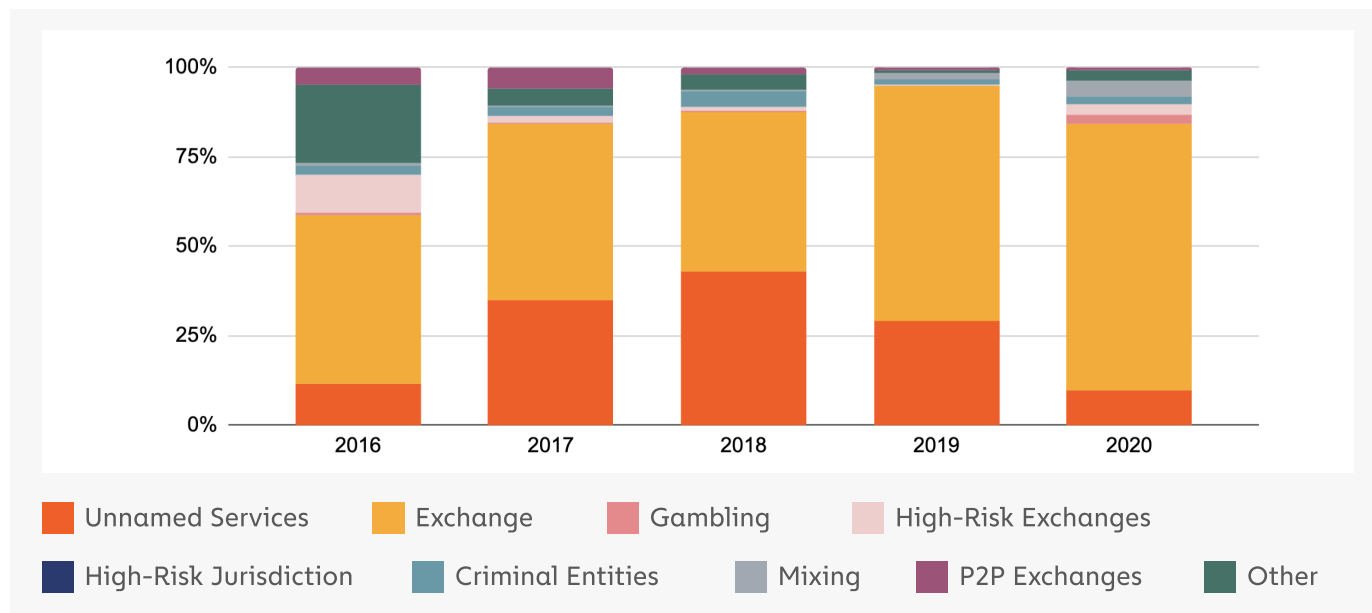


2020 Top 10 cryptocurrency investment scams



Mirror Trading International was by far the year's biggest scam, taking in \$589 million worth of cryptocurrency across more than 471,000 deposits, suggesting a number of victims in the hundreds of thousands. We'll dive more into Mirror's business model and operations later in the section. Other notable scams included J-enco and Forsage.

Destination of funds sent from scam addresses | 2016 - 2020





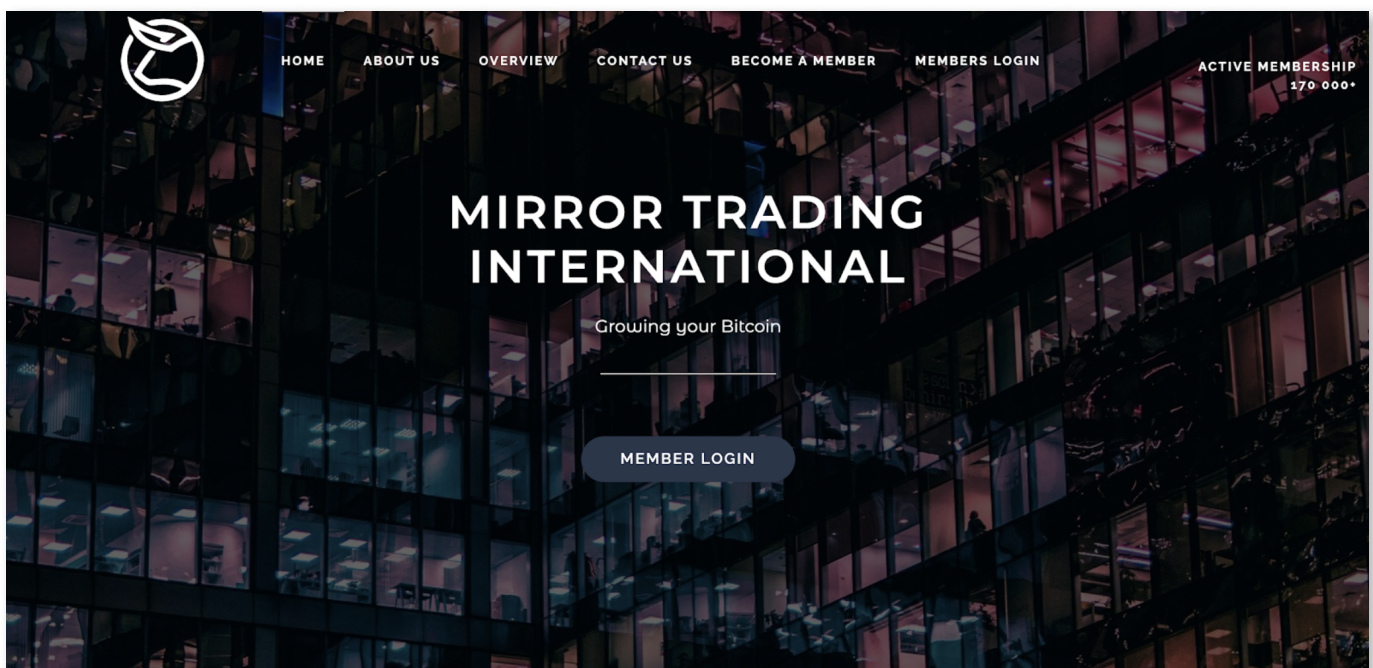
As was the case in previous years, scammers moved cryptocurrency received from victims primarily to exchanges in order to convert it into cash.

However, we also saw an increase in the share of scam proceeds sent to mixers and high-risk exchanges, meaning those with weak or non-existent compliance programs. This may be a sign that some scammers are becoming warier of compliant exchanges, which are more likely to flag illicit activity using a transaction monitoring solution and cooperate with law enforcement investigations.

Below, we'll analyze two prominent 2020 scams.

Investigating 2020's biggest investment scam: Mirror Trading International

Mirror Trading International (MTI) presents itself as a passive income source. According to its website, users simply deposit a minimum of \$100 worth of Bitcoin, and MTI promises to grow it using an AI-powered foreign exchange trading software. The site indicates that customers can achieve consistent daily returns of 0.5%, which would translate to yearly gains of 500%. Algorithmic trading is a common premise for many cryptocurrency investment scams.





WHY MIRROR TRADING INTERNATIONAL?

Using Bitcoin as its base currency, the company uses advanced digital software and artificial intelligence (AI) to trade on the international Forex markets. Members join a trading pool with a minimum of US\$100 worth of Bitcoin.

Daily profits generated from the trading are divided in a sustainable manner and are added to member accounts according to their share in the total trading pool.

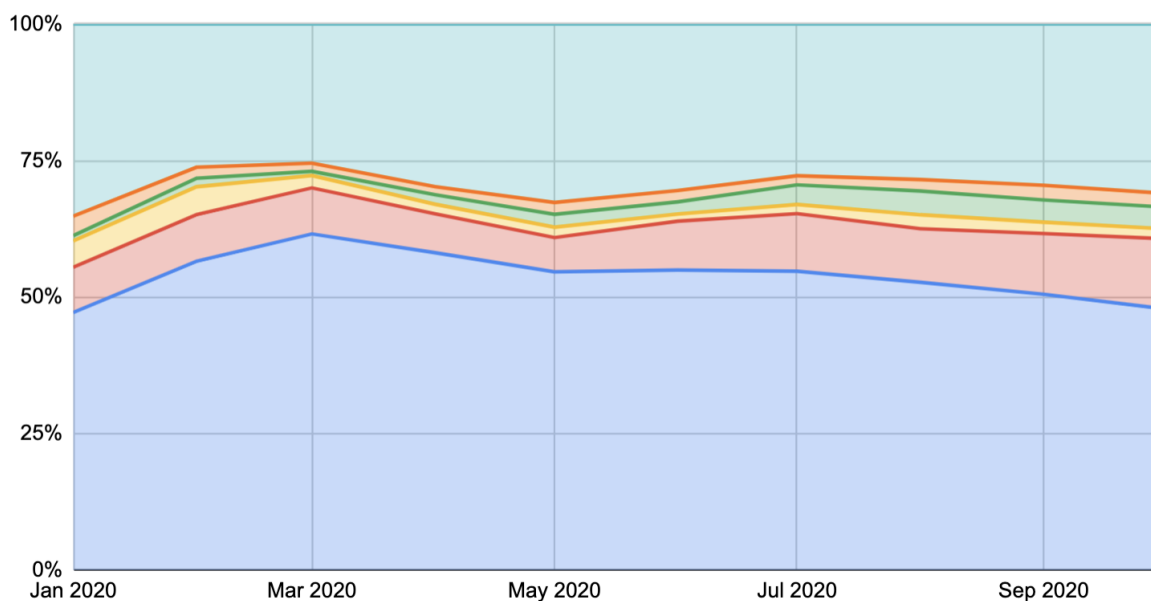
This allows your Bitcoin to grow daily quietly accumulating in your account. No trading experience is required as the system is automated and does everything for you.

All you need to do is sit back and relax. Your daily trading statements allow you to track your profit.



MTI is based in South Africa, and claims to have offices in Stellenbosch and Johannesburg. Its web traffic falls in line with that, as more than half comes from South Africa.

Mirror Trading International Web Traffic Data



Mexico Canada United Kingdom United States
South Africa All others

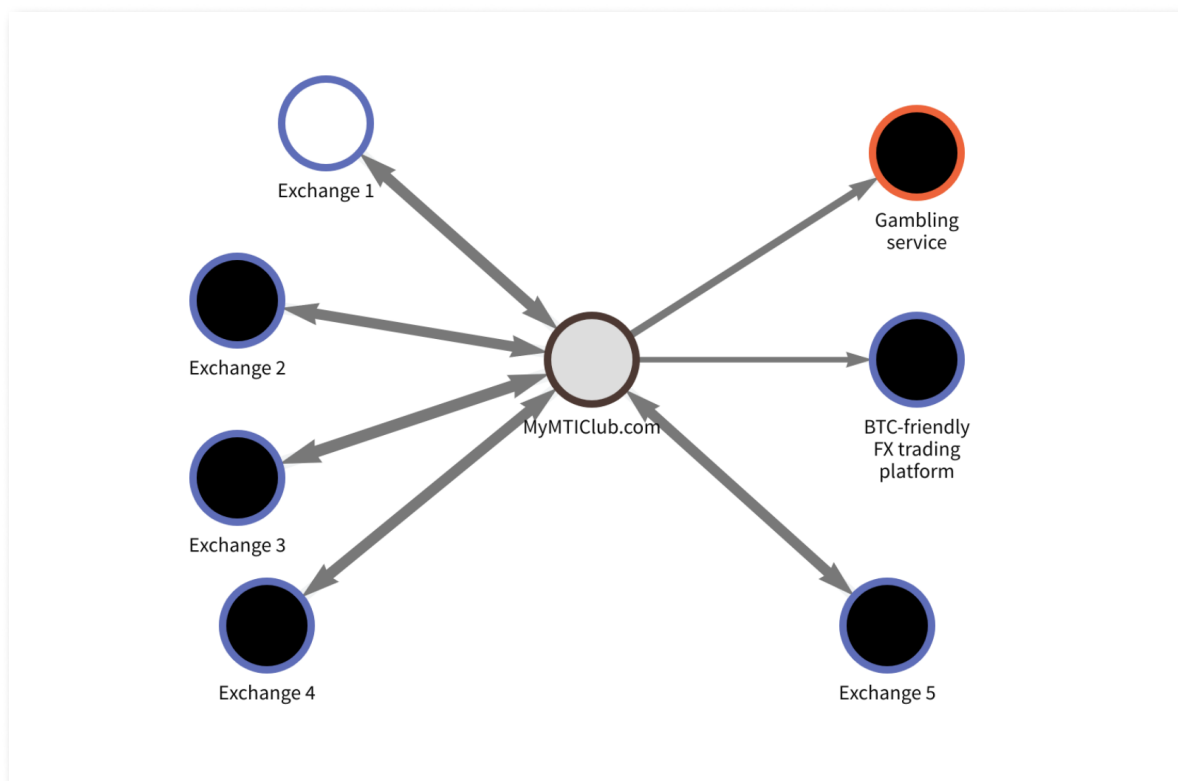
Currency included: BCH, BTC, ETH, LTC, OMG, PAX, TUSD, USDC, USDT



The U.S., U.K., Canada, and Mexico also make up significant portions of MTI's web traffic. We assume from this that most MTI victims hail from these countries in similar proportions as well. MTI has been actively receiving Bitcoin from "customers" since June 2018 and even has 150 employees listed on its [LinkedIn company page](#).

However, despite these airs of legitimacy, Google searches reveal that people have been rightly speculating that the company is a scam for most of its existence. In August 2020, CoinDesk [published an article](#) encouraging all MTI users to withdraw their funds as soon as possible, citing the decision of Texas state regulators to formally label the company a scam, as well as a pending investigation by South Africa's Financial Services Conduct Authority (FSCA). On December 18, 2020, the FSCA [filed charges](#) against MTI after its investigation found that the company falsified trade statements, didn't declare losses and committed other acts of fraud to deceive the market. The investigation also found that MTI had over 16,000 Bitcoin of claimed customer investment funds unaccounted for. MTI claimed to have transferred those funds to a new FX trading platform after its old platform banned MTI due to its scamming reputation, but the new platform says these funds were never deposited. Since those charges were filed, MTI customers have complained that they can no longer access or withdraw funds they've deposited to the platform, and MTI CEO Johan Steynberg has [fled South Africa](#).

Using Chainalysis Reactor, we can analyze MTI's cryptocurrency transaction history to learn more about the scam.

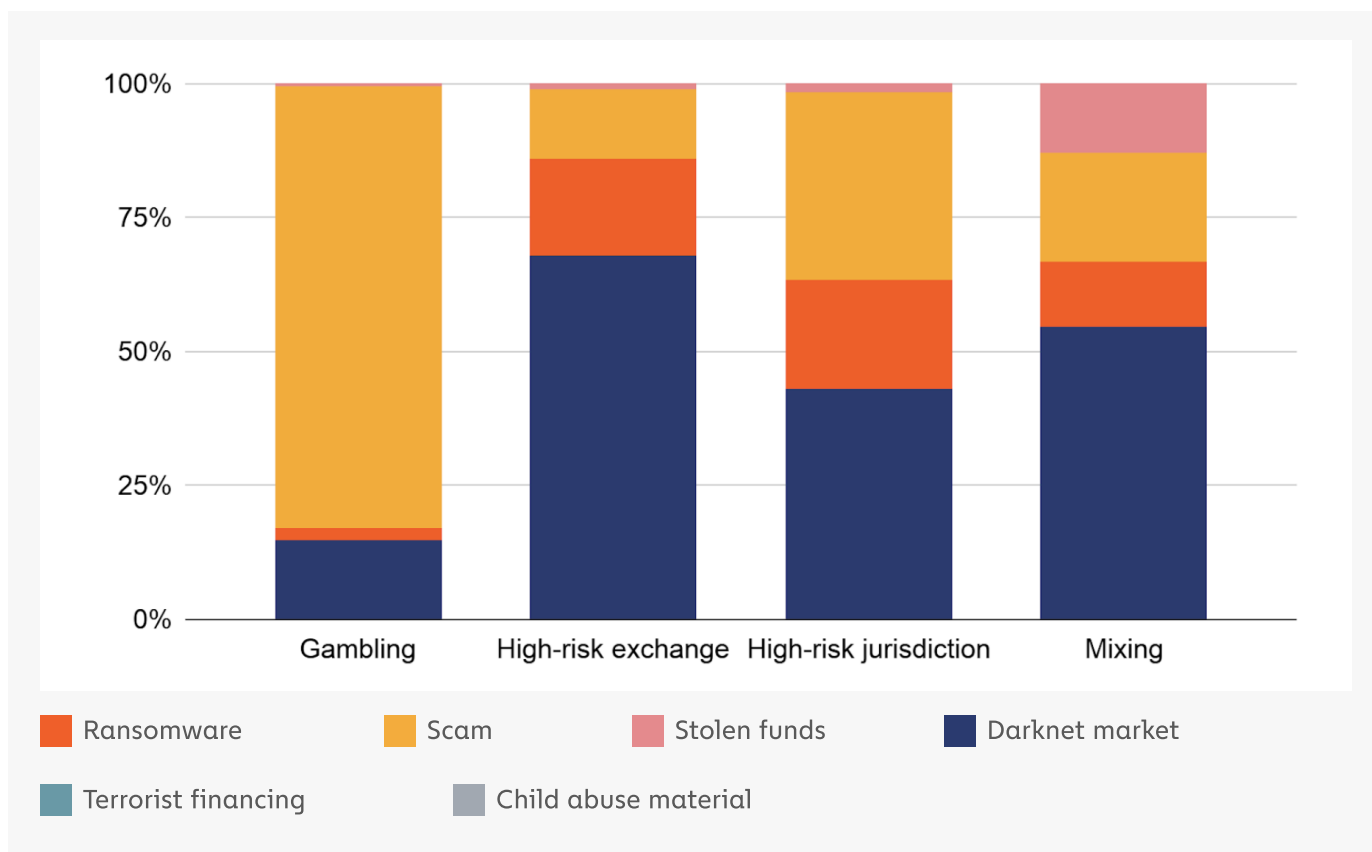




MTI Club has received \$588 million worth of Bitcoin across more than 470,000 transactions, primarily from exchanges, but also from self-hosted wallets. MTI has also sent and received significant funds to and from a popular, Bitcoin-friendly FX trading platform, as we show in the Reactor graph above.

Perhaps most interesting is MTI Club's apparent usage of a popular cryptocurrency gambling service as a money laundering and cash out mechanism. The platform is the biggest risky destination of MTI funds by volume, having received \$39 million worth of cryptocurrency from the scam in 2020. Cryptocurrency observer and venture capitalist Dovey Wan [has remarked](#) that this is becoming a common money laundering technique for many cybercriminals who use cryptocurrency, as gambling platforms can be used similarly to mixers to obscure the origins and flows of illicitly-obtained funds. Our data suggests that this is especially true for scammers.

Risky services receiving illicit funds by crime type | 2020



Currencies included: BCH, BTC, ETH, LTC, OMG, PAX, USDC, USDT

As the above chart shows, scammers are disproportionately likely to send funds to gambling platforms rather than other services frequently used for money laundering.

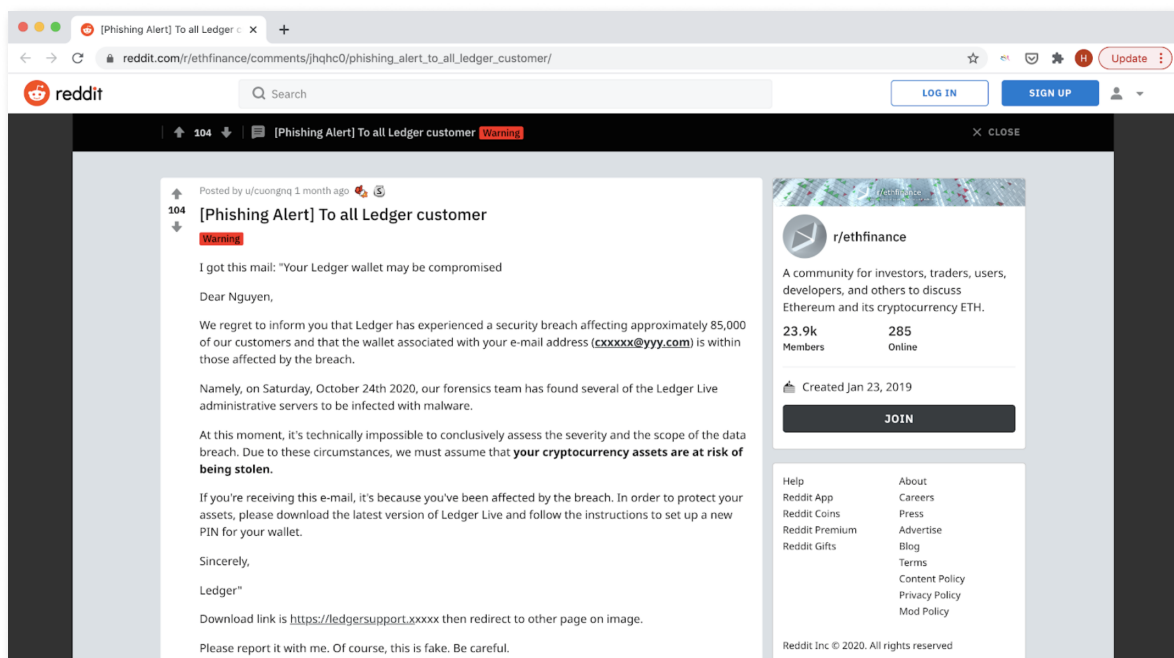


Mirror Trading International is another example of why the industry must spread the word that algorithmic trading platforms promising unrealistically high returns are nearly always scams. When cryptocurrency exchanges and other services learn of these scams and receive their cryptocurrency addresses, they should discourage users from sending funds to those addresses or at least warn them that financial losses are highly likely. In addition, exchanges, gambling platforms, and other services that these scams use to launder funds should consider blocking incoming transactions from businesses that relevant government bodies label as scams or potential scams, as removing the ability to convert funds to cash makes it more difficult for scams to operate.

The Ledger phishing scam is a wake up call for exchanges

While phishing scams made up a very small share of overall scam revenue in 2020, one phishing scam in particular has received a great deal of attention due to its high visibility and the number of potential victims: The Ledger phishing scam.

Ledger is a popular provider of [hardware cryptocurrency wallets](#), which are physical devices on which cryptocurrency can be stored, similar to a conventional cryptocurrency wallet. In July 2020, the company published a [blog post](#) revealing that many users' email addresses had been compromised in a data breach. A few months later in October, Ledger customers reported receiving emails from closely spoofed versions of the Ledger website domain. The email claimed that Ledger's servers had been hacked with malware and that customers' funds were in danger of being stolen unless they clicked a link in the email to download the latest version of Ledger's software. Clicking the link leads users to a web page that mimics the Ledger website.



A [reddit post](#) describing the phishing emails.



The email and website however, are part of a sophisticated phishing scam. Instead of a software update, Ledger users who click the download link on the fake web page actually download malware that drains their Ledger wallet. Overall, [CoinTelegraph reported](#) that Ledger users lost 1.1 million XRP (roughly \$645,000) within the first week of the phishing campaign. We should also note that since the leaked Ledger database has been sold on the dark web, it's possible that more than one criminal group has launched phishing attacks against Ledger users. This is also backed up by the fact that since October, Ledger users have received multiple waves of phishing messages, including some delivered by SMS and using different social engineering techniques.

Our analysis of a selection of the suspected scammers' addresses reveals that their wallets have been active since 2018, suggesting that the cybercriminals may have been conducting phishing scams for at least two years preceding the publication of the Ledger scam in 2020. In addition, we found that the assets stolen from Ledger customers span many cryptocurrencies, a large share of which have been moved to exchanges and other services. The stolen assets we've identified amount to upwards of €3 million.

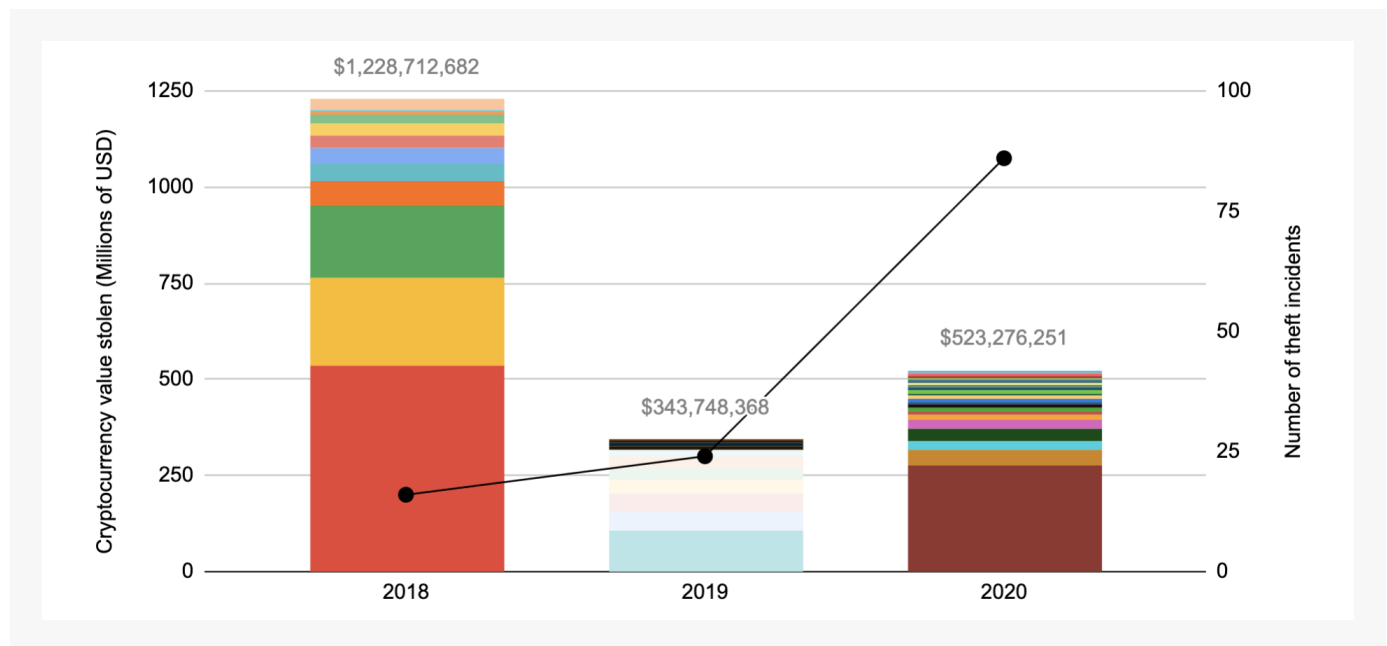
The Ledger phishing scam shows how important it is for exchanges and other cryptocurrency services to educate customers on phishing techniques, especially if they know customers' emails or other personal information has been compromised, thereby making customers more vulnerable to phishing attacks.



Stolen Funds

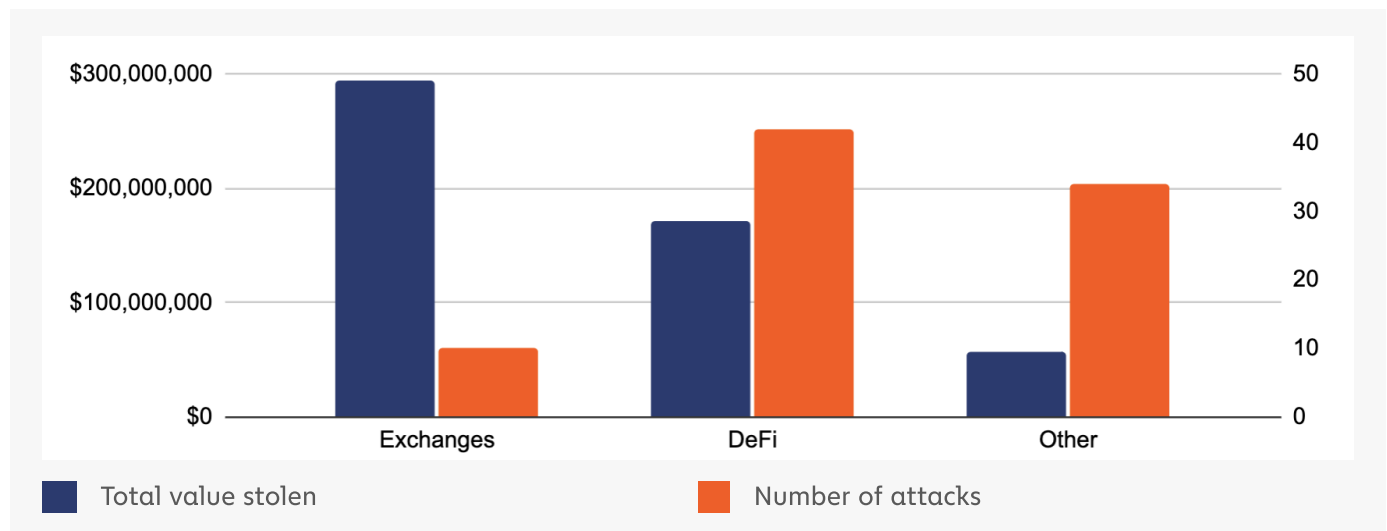
More Cryptocurrency Stolen in 2020 As DeFi Platforms Appear Uniquely Vulnerable to Attack

Number of cryptocurrency theft incidents vs. Total value stolen by year | 2018 - 2020



Different colors denote different instances of cryptocurrency theft. Please note that this graph relies in part on public reporting, so we cannot list all currencies included.

Total value stolen and number of attacks by victim type | 2020



Note: The "other" category here refers to cryptocurrency thefts from individuals or from cryptocurrency businesses other than exchanges.

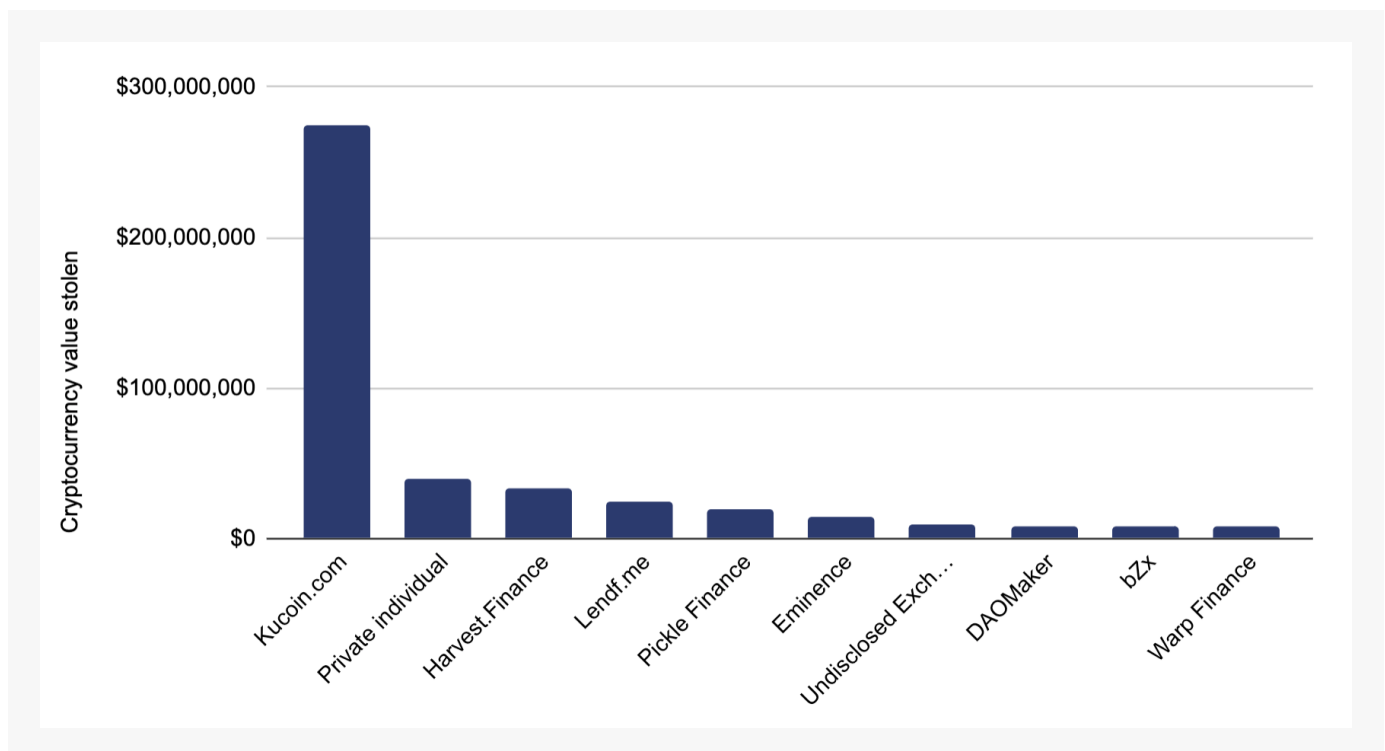


Year	Number of attacks	Received USD
2018	16	\$1.23B
2019	24	\$343.7M
2020	86	\$523.3M

In 2020, over \$520 million worth of cryptocurrency was stolen from services and individuals through hacks and non-technical attacks like social engineering or phishing efforts. That represents an uptick from 2019 following a huge decline from the amount stolen in 2018, most of which could be attributed to the [\\$534 million Coincheck hack](#). **More than half of the amount stolen in 2020 was from the [hack of the exchange KuCoin](#), which we can now publicly attribute to Lazarus Group, a notorious North Korea-aligned cybercriminal syndicate responsible for hacking numerous cryptocurrency exchanges over the last few years.** The hackers managed to take \$275 million worth of cryptocurrency from KuCoin, making it the biggest cryptocurrency theft of the year and third-largest of all time, though KuCoin claims to have recovered most of the funds. Later in this section, we'll look more at this hack and share details on how Lazarus Group's money laundering strategy changed in 2020.

The chart and table below provide details on the ten largest cryptocurrency thefts of 2020.

Top 10 cryptocurrency theft attacks | 2020





The Top 10 Cryptocurrency Thefts of 2020

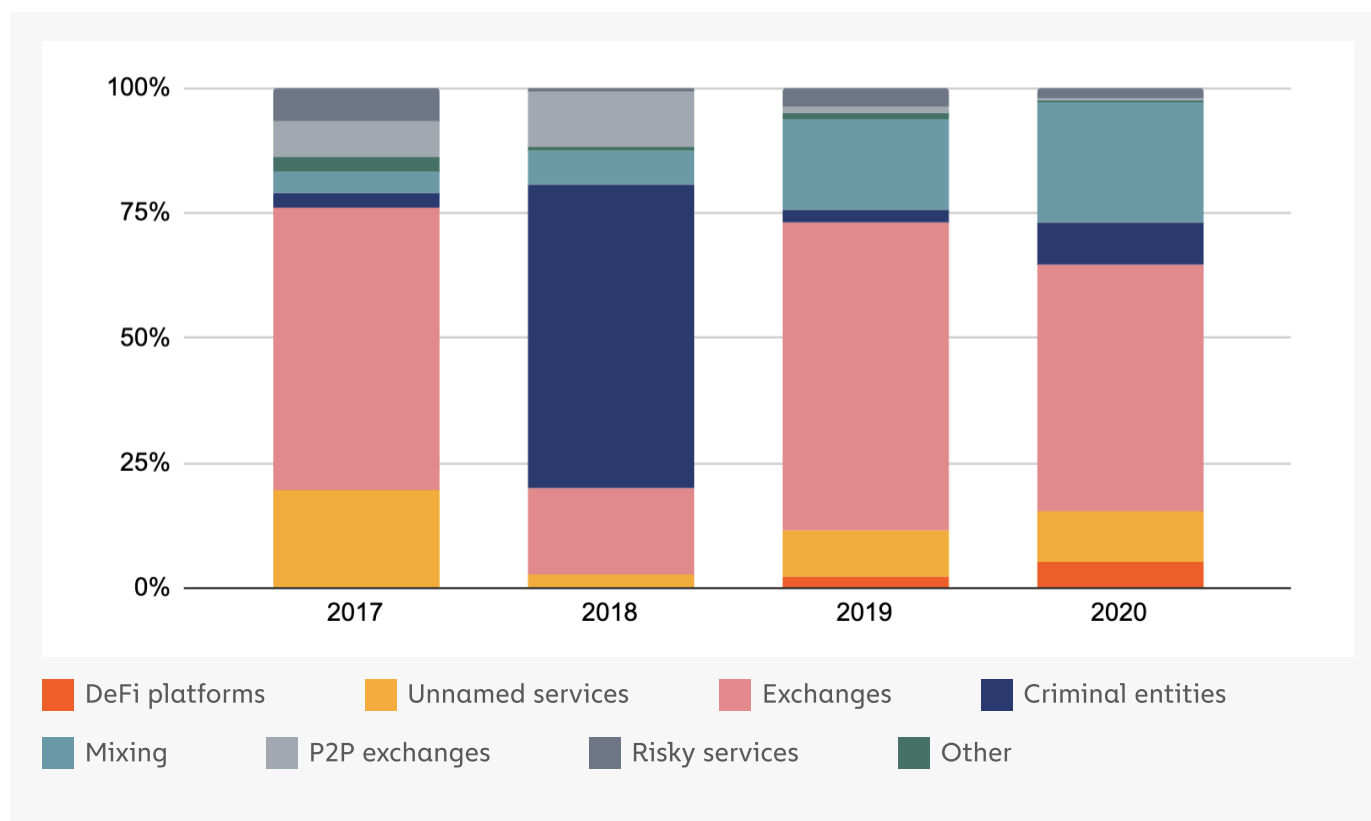
Victim	Victim type	Amount stolen (USD)	Description
KuCoin	Exchange	\$275 million	Third-largest cryptocurrency theft ever. Lazarus Group hackers accessed private keys of KuCoin hot wallets and stole numerous types of cryptocurrency. Hackers then used DeFi platforms like Uniswap and Kyber to swap stolen funds for different types of cryptocurrency.
Josh Jones	Personal Attack	\$40 million	Funds stolen from the private wallets of Josh Jones, CEO of Bitcoin Builder.
Harvest Finance	DeFi platform	\$34 million	Cybercriminals launched a flash loan attack , using borrowed funds to manipulate cryptocurrency prices and artificially increase their share of Harvest's yields.
Lendf.me	DeFi platform	\$25 million	Cybercriminals exploited a code vulnerability in Lendf.me, a DeFi lending platform, to pull off a reentrancy attack .
Pickle Finance	DeFi platform	\$20 million	Cybercriminals launched a flash loan attack .
Eminence	DeFi platform	\$15 million	Cybercriminals launched a flash loan attack .
Undisclosed exchange	Exchange	\$9 million	Due to ongoing investigations, we can't reveal the victim or nature of this exchange hack.
MakerDAO	DeFi platform	\$8.3 million	Cybercriminals exploited vulnerability in MakerDAO's price oracle during flash crash .
bZx	DeFi platform	\$8 million	Cybercriminals exploited code error to manipulate their balances and create new tokens at will.
Warp Finance	DeFi platform	\$8 million	Cybercriminals launched a flash loan attack .



One trend that jumps out is the amount that's been stolen from DeFi platforms. DeFi platforms' usage has skyrocketed in 2020 but has also given cybercriminals a new, uniquely vulnerable service to attack. Despite representing just 6% of all cryptocurrency activity, DeFi platforms lost roughly 33% of all cryptocurrency stolen in 2020 and were victims in nearly half of all individual attacks. Later in the section, we'll examine what makes DeFi platforms so susceptible to attacks.

DeFi platforms also figure prominently when we look at the services cybercriminals have used to launder stolen cryptocurrency and convert it into cash.

Destination of stolen cryptocurrency by year | 2017 - 2020



Currencies included: BAT, BCH, BTC, ETH, LTC, MKR, OMG, PAX, TUSD, USDC, USDT

Stolen funds primarily move to exchanges, as is the case with proceeds from other forms of cryptocurrency-related crime. But DeFi platforms' share of all stolen funds received more than doubled in 2020. Their decentralized nature is likely what makes DeFi platforms attractive as a money laundering mechanism — since these platforms never directly take custody of funds deposited to them, many don't collect know your customer (KYC) information or report on transaction activity as demanded by the Bank Secrecy Act (BSA) and other financial regulations.



What makes DeFi platforms vulnerable to attack?

DeFi's extraordinary growth has been one of cryptocurrency's biggest stories of 2020. DeFi stands for decentralized finance, the decentralization arising from the fact that DeFi platforms can, at least in theory, run autonomously without the support of a central company, group, or person. DeFi platforms are built on top of smart contract-enriched blockchains — primarily the Ethereum network — and can fulfill specific financial functions determined by the underlying code, executing specific transactions like trades and loans automatically when certain conditions are met. Without the need for centralized infrastructure or human governance, DeFi platforms can enable users to execute financial transactions at lower fees than other fintech applications or financial institutions. Overall, DeFi platforms received \$86.5 billion worth of cryptocurrency in 2020, which represents a 67x increase over the 2019 total.

However, cybercriminals stole more than \$170 million from DeFi platforms in 2020, which is disproportionately high in comparison to the share of total cryptocurrency activity DeFi accounts for. The primary reason for this is that DeFi platforms are uniquely vulnerable to **price manipulation attacks**. Price manipulation was the key to nearly every notable attack on DeFi platforms in 2020. Transactions happen almost instantly in DeFi with very few mechanisms in place to prevent shady transactions, so bad actors can reap huge gains by manipulating a cryptocurrency's price on one or more DeFi platforms. DeFi platforms rely on tools called [price oracles](#) to get asset pricing data from an external source — usually from another exchange, other service, or data provider like CoinMarketCap — to ensure its assets are priced in accordance with the rest of the market. However, most DeFi platforms use centralized price oracles, which rely on just one node to feed data to the rest of the platform and often draw on a single source of pricing data, leaving them vulnerable to attack.

Price manipulation might seem like an unlikely attack method for cybercriminals, as upping the price of any one crypto asset requires upfront capital to pump up its value, right? Not so in DeFi, thanks to **flash loans**.

Flash loans allow DeFi users to instantly receive loans without putting up collateral, use the loaned funds to make trades elsewhere, and repay the loan in one instant transaction. If they don't pay back the loan, the entire transaction is instantly rolled back, meaning the lender receives the original capital back as if the loan never happened, something only possible with smart contracts. In effect, this means little to no risk for either side: If the trade the borrower wants to make with the loaned funds doesn't work out and they can't pay back the loan, neither they nor the lender loses anything. This also means lenders can charge very low interest on flash loans. Traders often use flash loans to get the funds necessary to exploit arbitrage opportunities, using borrowed funds to take advantage of pricing disparities across platforms and come away with a small profit after paying back the loan.



However, in 2020, cybercriminals weaponized flash loans by using the borrowed funds to purchase a crypto asset, pump up its price, and sell it for a large profit, thereby enabling them to easily pay off the original loan and pocket the remaining funds. We saw an example of this in February's [two hacks of bZx](#), a DeFi protocol that allows users to build apps for decentralized lending, margin trading, and other financial activities. In the [first hack](#), the cybercriminals borrowed a large amount of Ether from bZx in a flash loan, used it to buy and pump up the price of wrapped Bitcoin on Uniswap — at one point, the wrapped Bitcoin price on Uniswap reached 109.8 ETH, compared to 38 for the market in general. The attacker then exchanged their wrapped Bitcoin for a healthy profit of Ether, some of which was used to pay off the original flash loan. All in all, the attacker netted \$350,000 worth of Ether. The second attack, a copycat of the first, netted \$633,000. The identity of the hackers is unknown, and it's unclear whether or not the same individual or group is responsible for both hacks.

These attacks on bZx worked because the platform's code contained no failsafes to account for large price jumps on other DeFi platforms, which may have caught the cybercriminals pumping wrapped Bitcoin's price on Uniswap. [bZx's GitHub repository](#) shows the issue has now been fixed. But this underlines another reason DeFi platforms are vulnerable to attack: their use of open-source code. DeFi platforms move users' funds based solely on their underlying code without human intervention, so users need to be able to audit that code in order to trust the platform, making open source a necessity. However, that means cybercriminals can also analyze the code for vulnerabilities and plot the perfect attack, as it appears they did in the case of the bZx flash loan attacks. In fact, bZx was hacked again later in the year to the tune of [\\$8.1 million](#), all because a single misplaced line of code allowed users to manipulate their own balances under certain circumstances, creating new tokens for themselves at will.

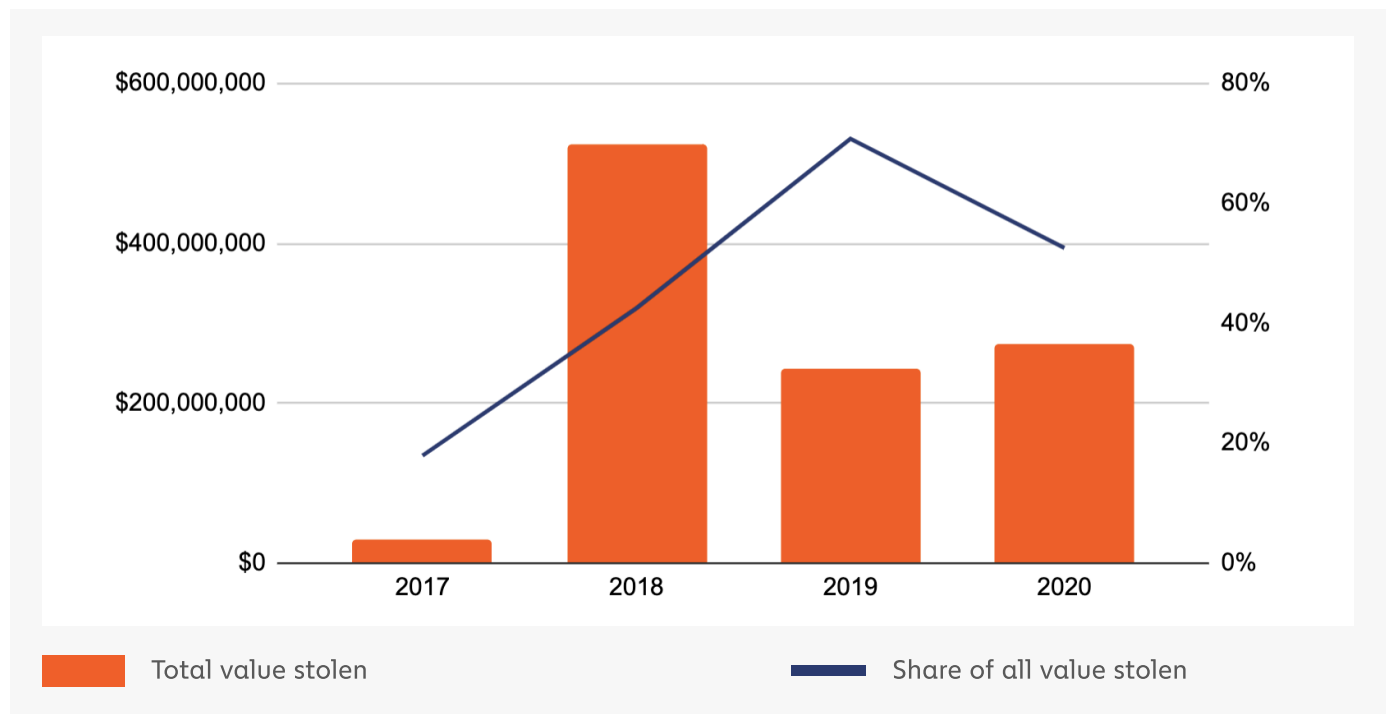
These attacks go to show how important it is for DeFi platforms to implement the latest and greatest security measures. One provider to watch here is [Chainlink](#), a company that helps DeFi platforms protect against price manipulation attacks with **decentralized price oracles**. Decentralized price oracles aggregate pricing data from more sources and deliver it to the DeFi platform on-chain through a network of independent nodes, thereby making it harder for price manipulators to target a single weak spot. However, even with such advancements, regulators and law enforcement should look for ways to ensure the extremely promising DeFi space remains safe for investors.



Lazarus Group pulled off 2020's biggest exchange hack and appears to be exploring new money laundering options

Lazarus Group is a cybercriminal syndicate working on behalf of the North Korean government. Lazarus has been responsible for numerous cryptocurrency exchange attacks, such as the [2019 UpBit hack](#), which netted them more than \$49 million worth of cryptocurrency. Overall, the group is believed to have stolen more than \$1.75 billion worth of cryptocurrency in the time it's been active. Experts believe proceeds from Lazarus Group hacks go toward North Korea's [nuclear weapons program](#), so combatting their activity is of utmost importance for international safety and stability. That's why in 2020, the U.S. government took actions such as [sanctioning two Chinese nationals](#) who helped Lazarus Group launder funds stolen in multiple cryptocurrency hacks, and [filing forfeiture complaints](#) against 280 cryptocurrency addresses associated with Lazarus Group hacks.

Total cryptocurrency value stolen by Lazarus Group vs. Lazarus Group's share of all stolen cryptocurrency | 2017 - 2020

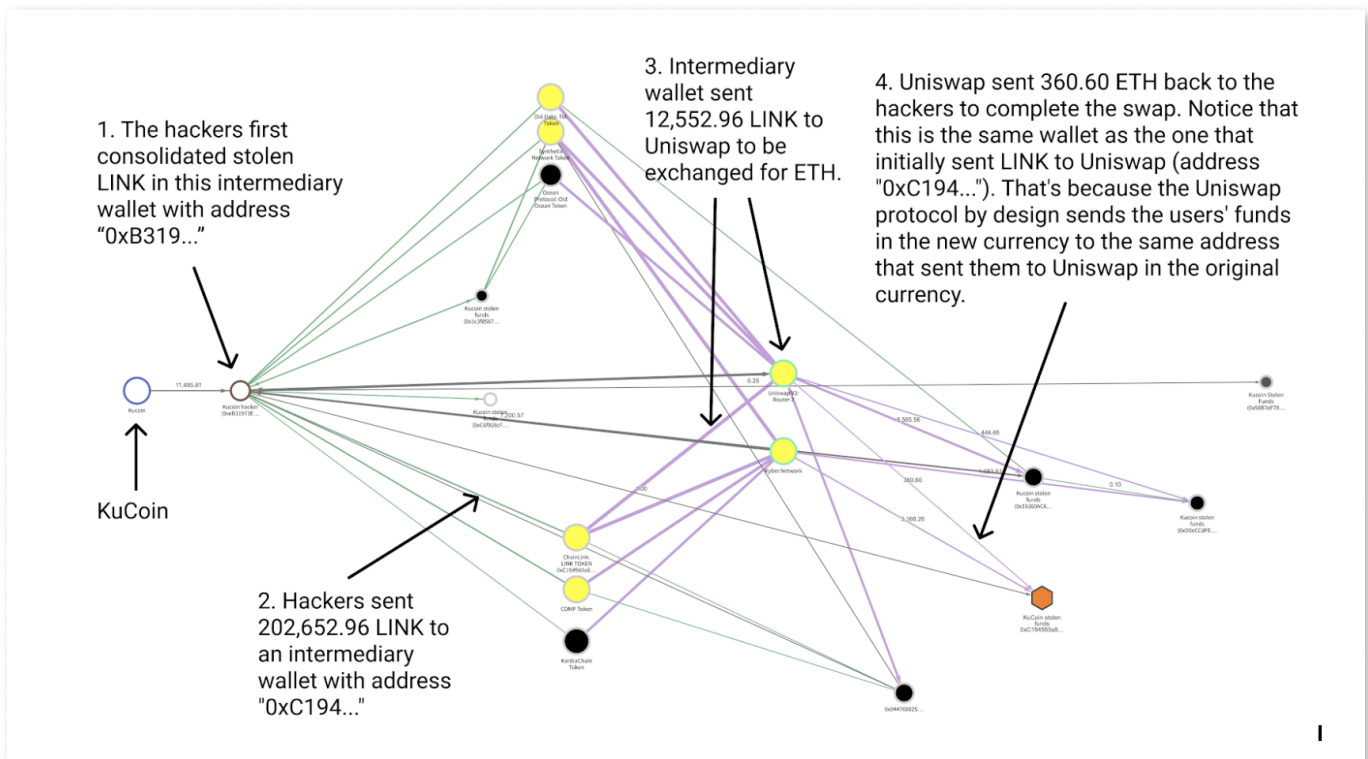


Currencies included: BAT, BCH, BNB, BTC, ETH, LTC, MKR, OMG, PAX, TUSD, USDC, USDT

However, Lazarus Group still managed to pull off the biggest cryptocurrency theft of the year, stealing roughly \$275 million worth of cryptocurrency from the cryptocurrency exchange KuCoin. The \$275 million represents over half of all cryptocurrency stolen in 2020. [According to KuCoin's CEO](#), the hack occurred after cybercriminals gained access to the private keys to the exchange's hot wallets. Soon after, he claimed that the exchange [had recovered](#) \$204 million worth of the stolen funds.

We were able to attribute this hack to Lazarus Group due in part to the KuCoin hackers' use of a specific money laundering strategy Lazarus has frequently used in the past. The strategy involves sending stolen funds to mixers in structured payments of the same size — usually an amount just below a round number in Bitcoin — that can be higher or lower depending on the size of the total amount to be laundered. Lazarus typically waits for each payment's output to be confirmed by the mixer before sending a new one, allowing them to minimize losses in the event the mixer fails. Once the funds are mixed, Lazarus Group then typically sends funds to OTC brokers on one of a few exchanges. The KuCoin hackers utilized this strategy for portions of the funds stolen. This, along with other pieces of evidence we're unable to share at this time, helped us identify Lazarus Group as the culprits. Additionally, two deposit addresses to which Lazarus Group sent stolen cryptocurrency this year also received funds stolen in the Harvest Finance hack, leading to speculation that Lazarus Group may have carried out that attack as well. However, this is still unconfirmed.

One new aspect of the KuCoin hack was how Lazarus Group [used DeFi platforms](#) to launder a portion of the stolen funds. DeFi platforms allow users to swap one type of cryptocurrency for another without a centralized platform ever taking custody of the users' funds. The lack of custody means that many DeFi platforms believe they don't have to take KYC information from customers, making it easier for cybercriminals to move funds with greater anonymity. The Reactor graph below gives an example of how exactly Lazarus Group used DeFi platforms to launder a portion of the funds stolen from KuCoin.

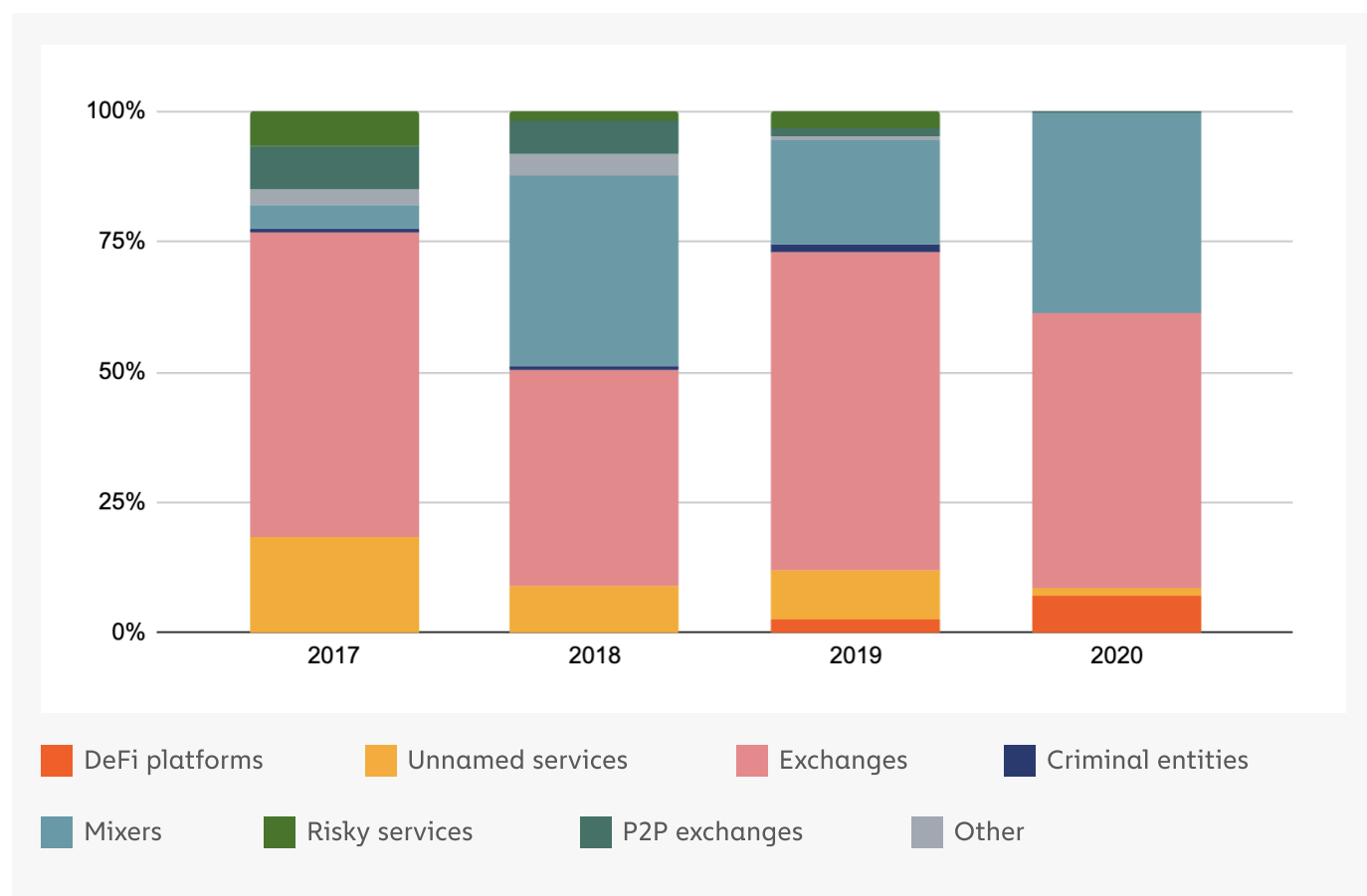




The cybercriminals first moved stolen LINK from their initial wallet to an intermediary, and from there, sent it to Uniswap to be traded for ETH. As a DeFi platform, Uniswap allows users to swap between ETH and several types of ERC-20 tokens without Uniswap ever taking custody of the funds, meaning that users don't have to provide KYC information. Users simply send funds to Uniswap from one address, and receive the equivalent amount back (minus minimal fees) at the same address in the token of their choice. So, in this case, the Kucoin hackers sent 12,552.96 LINK to Uniswap from the address "0xC194..." and received 360.60 ETH back to the same address. If investigators didn't already know that the hackers controlled the wallet that sent and received these funds, it would have been difficult to trace the funds' movements and spot the swap. As we can see on the graph, the hackers carried out many similar DeFi transactions using other types of tokens stolen in the hack.

The use of DeFi platforms represents a shift in Lazarus Group's money laundering strategy. The graph below shows the breakdown of the types of services the group has sent stolen funds to over the last few years.

Destination of cryptocurrency stolen by Lazarus Group | 2017 - 2020



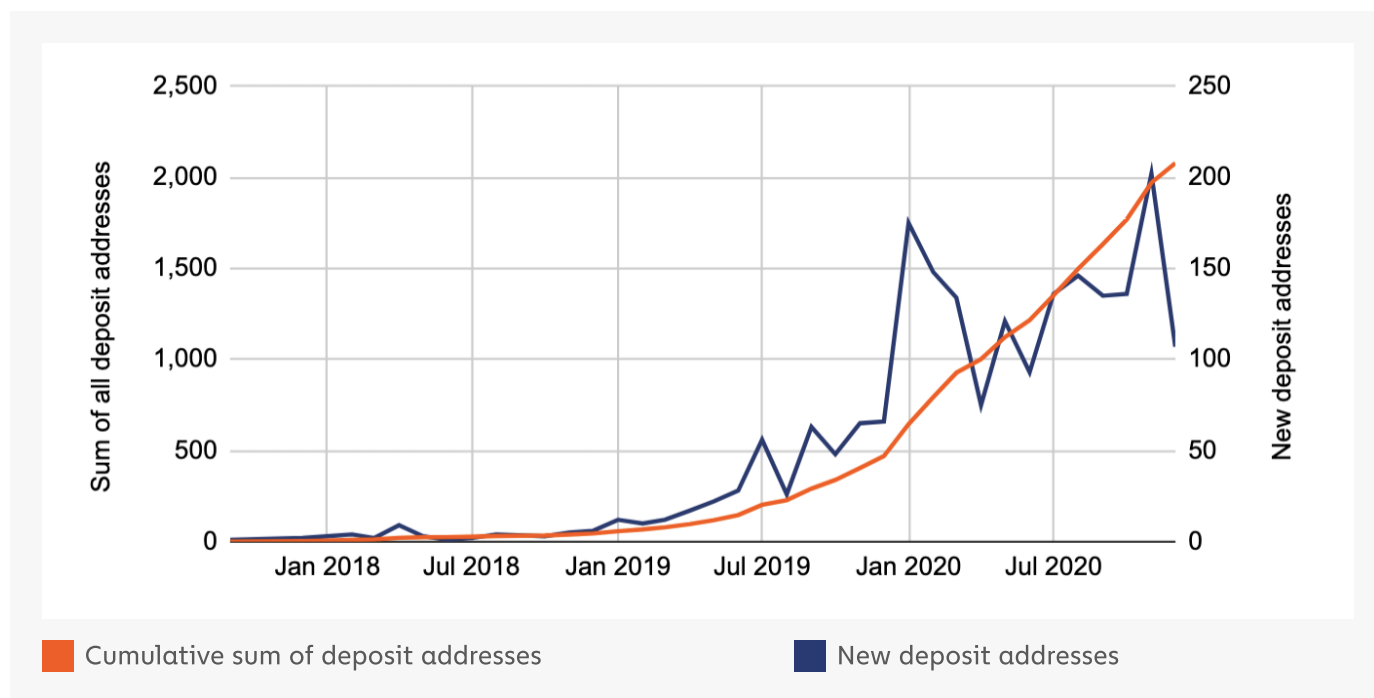
Currencies included: BCH, BTC, ETH, LTC, MKR, OMG, PAX, TUSD, USDT



Lazarus Group's use of DeFi platforms nearly doubled in 2020. The other trend that jumps out is the group's declining use of mainstream exchanges. While exchanges received the majority of funds stolen by Lazarus Group in 2019, much of that volume went to mixers in 2020. This may be a result of increased security efforts by exchanges following the DOJ's civil complaint against in August, which [highlighted](#) how Lazarus Group hackers frequently moved stolen funds through exchanges and OTC brokers using addresses nested at exchanges.

However, even if Lazarus Group isn't sending as high a percentage of funds to services, they're using more and more unique deposit addresses at services to launder funds. This trend accelerated in September 2019 and has continued since. Lazarus Group typically favors deposit addresses at a group of 20 different exchanges. In the chart below, we show the growth of deposit addresses at those exchanges that have received funds from Lazarus Group since 2018.

New deposit addresses vs. Cumulative sum of all deposit addresses used by Lazarus Group | Sep '17 to Dec '20



Currencies included: BCH, BTC, LTC, USDT

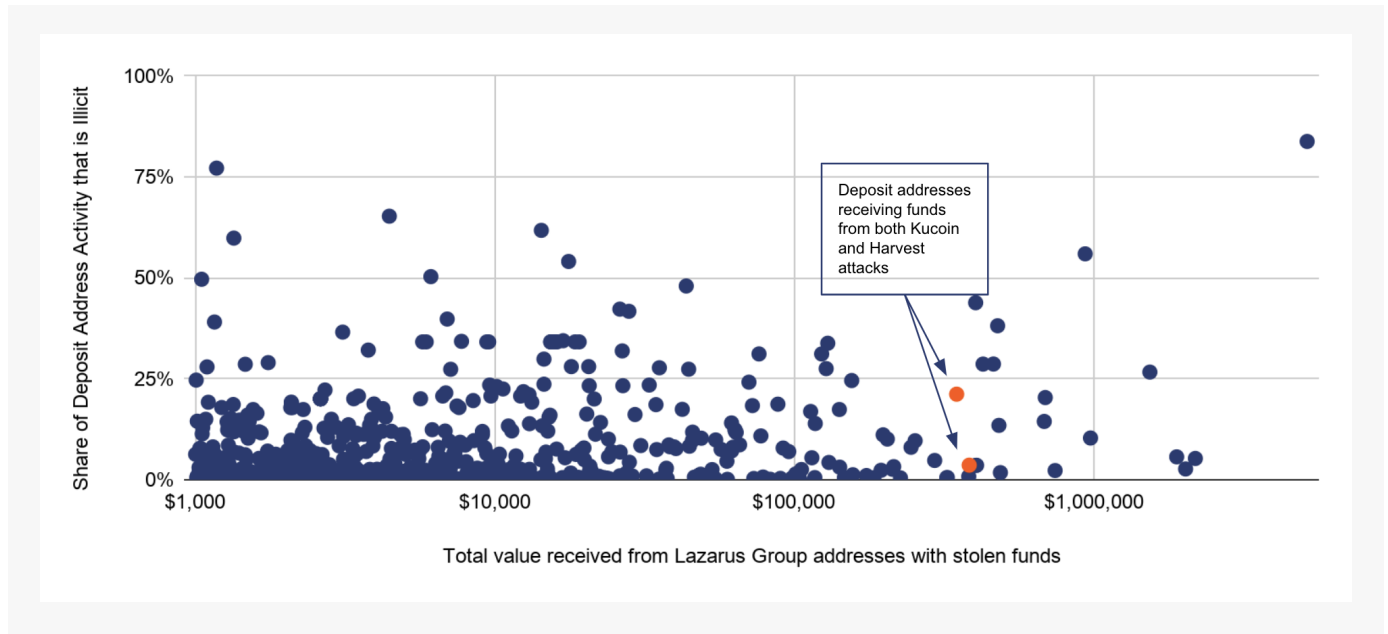
Note: Only includes deposit addresses at Lazarus Group's top 20 preferred exchanges

In December 2019, Lazarus Group had 470 separate cryptocurrency addresses at its top 20 exchanges that had received at least \$1,000 worth of stolen cryptocurrency. By the end of December 2020, that number had risen to 2,078. This suggests that Lazarus Group is spreading its funds around more to mitigate the risk of any one address being identified and frozen. It also fits a pattern of adaptability on the part of Lazarus Group — each year, their money laundering strategy changes as services improve their security efforts.




We can't say for sure how many of these addresses are directly controlled by Lazarus and how many are controlled by OTC brokers and other nested service providers moving funds on behalf of Lazarus. However, we try to approximate it below by analyzing the activity of all service deposit addresses that have received more than \$1,000 worth of cryptocurrency from Lazarus Group addresses in 2020, looking at the total value they've received from those addresses versus the share of all funds they've received that come from criminal sources.

Deposit Addresses Receiving Illicit Funds with Lazarus Group Connections



Currencies included: BTC

The majority of the funds go to deposit addresses that have received large sums from Lazarus Group and other criminal addresses, but whose overall activity is mostly non-illicit, and may therefore appear safe at first glance. Those addresses likely belong to nested services mostly processing legitimate transactions, rather than to wallets only moving illicit funds. That trend underlines the importance of exchanges digging into the details on the transactions carried out by nested services on their platforms — even large nested services for whom risky transactions make up a low share of total activity can be moving hundreds of thousands on behalf of rogue state actors like Lazarus Group, making them much more dangerous than they first appear.



Terrorism and Extremism Financing



Countries Around the World Collaborate to Fight Growing Cryptocurrency Usage in Terrorism Financing

In 2020, government agencies around the world uncovered, investigated, and prosecuted more terrorism financing schemes involving cryptocurrency than ever before. The most notable example came in August, when the United States Department of Justice (DOJ) announced the [largest ever seizure](#) of cryptocurrency from a terrorist group. Following an investigation into several different cryptocurrency donation campaigns, U.S. government agencies recovered more than \$1 million worth of Bitcoin from wallets controlled by terrorist groups and their financial facilitators.

Below, we'll summarize the cryptocurrency-based terrorism financing campaigns law enforcement agencies investigated and prosecuted in 2020.

Disruptions of terrorism financing networks involving cryptocurrency announced in 2020





Case 1: al-Qaeda and ISIS

Investigating country: France

Destination of funds: Syria

Date of activity: 2019 - 2020

Summary: French authorities [arrested](#) 29 individuals in a cryptocurrency-based terrorism financing scheme. Dozens of people in France bought cryptocurrency coupons worth \$11-\$165. The coupons were credited to accounts opened abroad by jihadis who then converted them into cryptocurrency. Hundreds of thousands of euros are thought to have been supplied via the network, benefitting members of al-Qaeda still hiding out in northwest Syria, as well as jihadis of the Islamic State group.

Case 2: ISIS

Country investigating: U.K.

Destination of funds: Syria

Date of activity: 2016 - 2020

Summary: Hisham Chaudhary of Leichester, England is [alleged](#) to have gathered and transferred Bitcoin to jihadist groups, allowing captured ISIS militants to escape Kurd-controlled prison camps in northern Syria.

Case 3: The al-Qassam Brigades (Hamas' military wing)

Country investigating: U.S.

Destination of funds: Multiple

Date of activity: 2019 - 2020

Summary: Starting in 2019, the al-Qassam Brigades posted calls on its social media pages for [Bitcoin donations](#) to fund terror campaigns, before moving solicitation to its official websites and incorporating more sophisticated cryptocurrency wallet infrastructure.

Case 4: al-Qaeda and affiliated terrorist groups in Central Asia and elsewhere

Country investigating: U.S.

Destination of funds: Syria

Date of activity: 2019 - 2020

Summary: Terrorist organizations in several countries — primarily [Syria](#), but also [Central Asian countries](#) such as Uzbekistan — solicited cryptocurrency donations from around the world on Telegram and other social media platforms, often posing as charity groups to bypass platform policies. These groups laundered and distributed funds using a Syria-based cryptocurrency exchange called BitcoinTransfer.



Case 5: Islamic State Khorasan Province

Country investigating: India

Destination of funds: India and Syria

Date of activity: 2019 - 2020

Summary: Kashmiri couple Jahanzaib Sami and Hina Bashir Beigh were [arrested](#) in Delhi on March 8 for allegedly planning to carry out attacks in India. The couple was accused of soliciting cryptocurrency donations to a Bitcoin address they received from a Syria-based ISIS operative. Sami discussed the possibility of using cryptocurrency donations to source weapons and explosives.

Let's dive into a few of these cases, starting with the most prominent: the now-disrupted terrorism financing campaigns launched by al-Qassam Brigades and al-Qaeda in Syria.

Taking down two large-scale terrorism financing campaigns

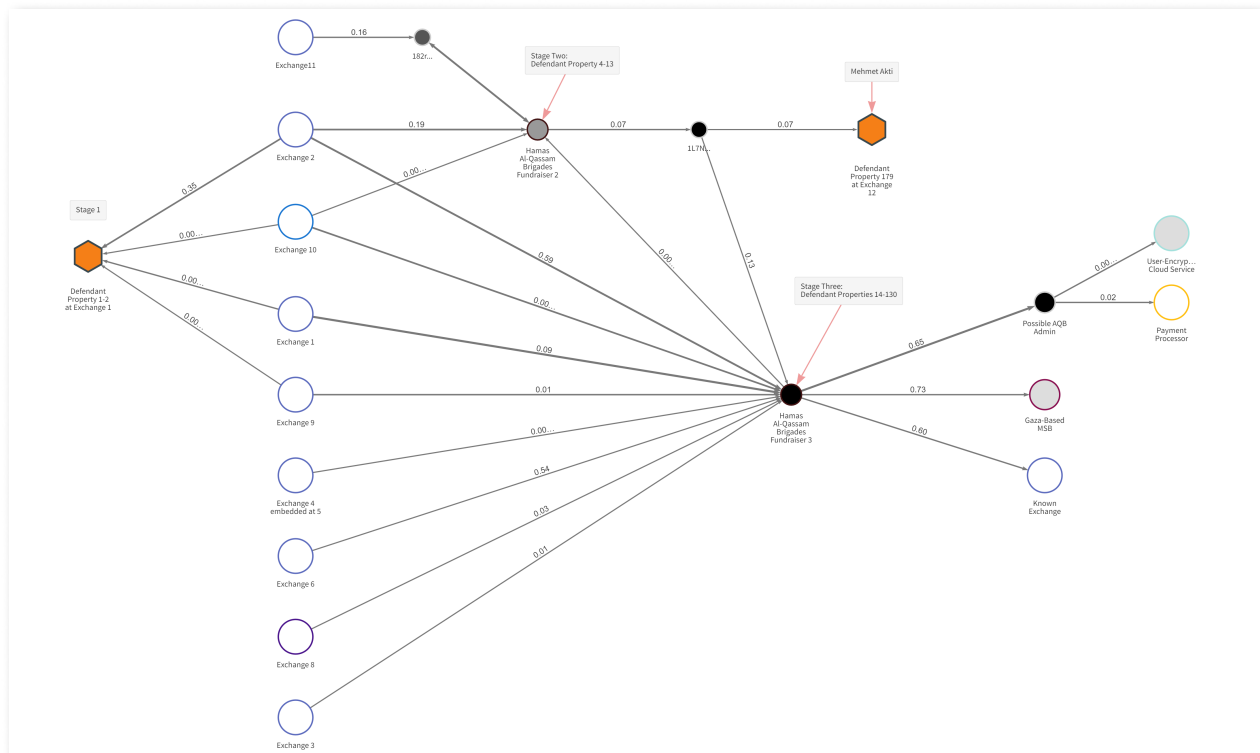
In August 2020, the Department of Justice announced the takedown of two of the most significant cryptocurrency-based terrorism financing campaigns seen to date. The first campaign (number 3 on our map) was conducted by Hamas' military wing, the al-Qassam Brigades (AQB), and took in tens of thousands of dollars' worth of Bitcoin between 2019 and 2020. The second campaign (number 4 on our map) was conducted by al-Qaeda and several associated groups in Syria, who used an Idlib, Syria-based cryptocurrency exchange called BitcoinTransfer to launder donations and distribute them between the groups involved. We'll recap both below.

Revisiting the al-Qassam Brigades' terrorism financing campaign

We covered AQB's terrorism financing campaign in last year's Crypto Crime Report, while the campaign was still ongoing. [Our analysis](#) focused on the campaign's growing sophistication throughout the year. Prospective donors were initially invited to send Bitcoin to a static address posted on social media, but within months, AQB built out a wallet infrastructure that generated a new, unique address for each individual donor, making the funds more difficult to trace. Jessi Brooks, an Assistant U.S. Attorney who prosecuted the AQB case, told us about the transformation. "It's a perfect example of how terrorists are learning more and more about cryptocurrency and figuring out how to use the technology for their own benefit," Brooks said. "During the investigation, we could literally see the financiers getting better at soliciting cryptocurrency donations in real time. I'm sure other terrorist groups will only build on AQB's techniques in the next campaigns."



Since then, however, U.S. agents seized AQB's primary web page promoting the campaign, and the organization hasn't received any new donations since October 2020. The Reactor graph below shows the three wallets AQB used throughout its campaign, which unfolded in three distinct stages of increasing technological sophistication. On the left, we see donations come in from several addresses, mostly hosted at large, mainstream exchanges, and on the right, we see where AQB moved cryptocurrency donations in an effort to launder and convert them to cash.



AQB used a mainstream cryptocurrency exchange, cryptocurrency merchant services provider, and two unlicensed money services businesses (MSBs) to convert cryptocurrency donations into cash. One of the unlicensed MSBs ran its cryptocurrency operation as a nested service, meaning it conducted all transactions using addresses at a mainstream exchange. Agents reached out to the exchange hosting those addresses and learned that they belonged to a Turkish national named Mehmet Akti, who owns and operates the unlicensed MSB. Most of the more than \$1 million worth of cryptocurrency seized in this investigation came from Akti's businesses. According to the DOJ complaint, the main address he used to run his MSB received over \$80 million worth of cryptocurrency and U.S. dollar wire transfers between October 2017 and March 2019, though the majority of this was likely unrelated to terrorism financing.

Unlicensed MSBs, many of which function on the [hawala model](#), have always been important for terrorism financing. According to Brooks, that isn't changing, as many of these MSBs have incorporated cryptocurrency services as another means of sending funds around the world. "Terrorist groups taking cryptocurrency donations have a huge reliance on unlicensed MSBs because they need to turn their crypto into cash, but can't go to services that follow the



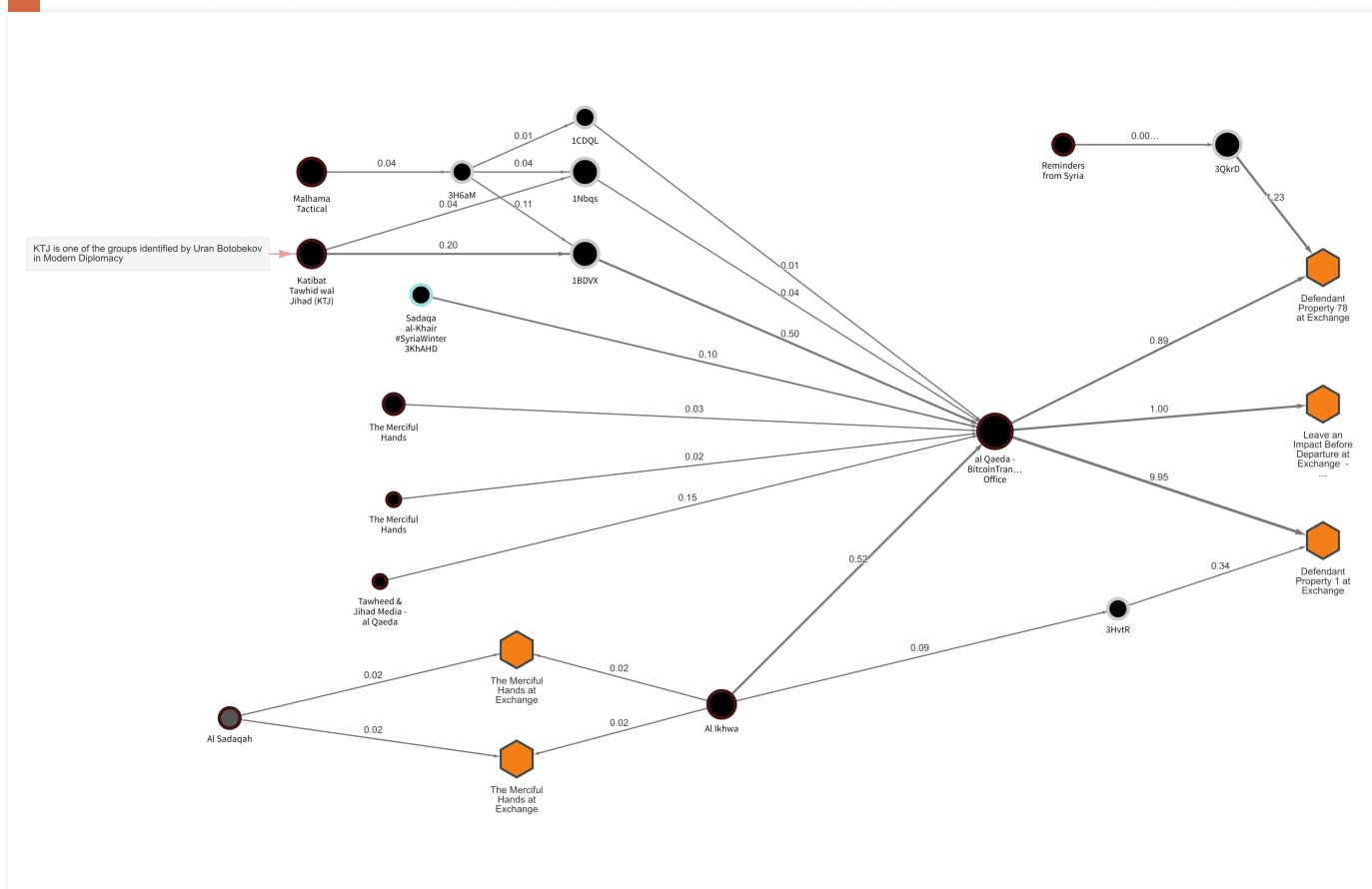
regulations," she said. "These businesses aren't solely working with terrorists. Terrorists aren't moving enough money to build a business around. What's scary is that many of them just don't care — they don't bother with KYC, and they get big while allowing terrorist groups to abuse them, but still transact with legitimate cryptocurrency businesses and with U.S. users."

How al-Qaeda used a cryptocurrency exchange as the hub of several linked donation campaigns

The DOJ also announced the takedown of a web of connected terrorism financing campaigns conducted by al-Qaeda and associated groups the same day it announced the takedown of the AQB campaign. The key difference between the al-Qaeda and AQB cases is that it involved several groups launching a shared infrastructure for collecting donations. In most cases, the terrorist groups presented themselves online as Syria-focused charities, but many of their posts and private communications made it clear that donations would be used to purchase weapons for jihadist groups. The terrorist groups involved include:

- **Malhama Tactical**, a private military contractor from Uzbekistan that has provided training for and fought alongside several terrorist groups in Syria.
- **Al Sadaqah**, a Syrian organization active on social media that purports to be a charity but has been implicated in terrorism financing.
- **Al Ikhwa**, a terrorist organization with documented ties to terrorist groups like Hay'at Tahrir al-Sham.
- **Reminders from Syria**, a Telegram channel affiliated with terrorist groups that frequently interacts with and boosts content from Al Ikhwa on social media.
- **The Merciful Hands**, another Syrian organization active on social media that purports to be a charity but has been associated with armed groups in Syria.

From there, these groups used multi-layered transactions to obfuscate the movement of these donations to a central hub of addresses, from which funds are then redistributed to the individual groups. Through blockchain analysis, we identified that central hub as BitcoinTransfer, a cryptocurrency exchange based in Idlib, Syria. BitcoinTransfer purports to be a cryptocurrency exchange but has been [implicated in several terrorism financing schemes](#) and appears to be fully under the control of terrorist groups. BitcoinTransfer processed more than \$280,000 worth of Bitcoin between December 2018 and July 2020, much of it related to terrorism financing.



On the left, we see the addresses associated with the campaigns of the terrorist groups we listed earlier. Donations were consolidated at BitcoinTransfer, which we see in the middle, before moving to addresses at exchanges, where funds could be converted into cash or distributed elsewhere as needed.

In response to news of the takedown of this terrorism financing campaign, Kyrgyz political scientist Dr. Uran Botobekov published [an article](#) in Modern Diplomacy on several Central Asian jihadist groups' collection of Bitcoin donations (number five on our map). In addition to Malhama Tactical, the Uzbek group we cite earlier, Botobekov points to groups like Katibat Tawhid wal Jihad (KTJ), Katibat Imam al Bukhari (KIB) and the Islamic Jihad Group (IJG), whose members hail from Central Asia but have been active in Syria. Based on the transaction histories of the two Bitcoin donation addresses Botobekov provides in his article, these groups appear to have raised roughly \$16,000 worth of cryptocurrency in 2020.

The groups involved in the BitcoinTransfer donation network, as well as the additional groups Botobekov cites in his article, underscore an important reason cryptocurrency is a valuable tool for terrorist groups: It's an easy way to send money around the world. While these groups were all focused on getting money to Syria at the time of these campaigns, they're based in different parts of the Middle East and Central Asia. Cryptocurrency allows them to send money across borders and coordinate the financing of their operations, with



less chance of transfers being blocked — especially when they rely on non-compliant cryptocurrency exchanges and unlicensed MSBs. However, as the takedown shows, their plans are far from fool-proof.

Collaboration is the key to fighting cryptocurrency-based terrorism financing

Another important lesson from the BitcoinTransfer case comes from what happened in its aftermath. After U.S. agents pinpointed the Syrian service as a hub of terrorism financing activity, agencies in other countries around the world were able to investigate suspicious transactions associated with it and uncover more terrorism financing schemes. Jessi Brooks told us more about how terrorism investigations involving cryptocurrency foster collaboration between agencies and countries. “It’s one of the reasons I enjoy working on cryptocurrency cases,” she said. “Right now, U.S. agencies are at the forefront of blockchain analysis. That’s opened the door to more cooperation and allows our work to have an international impact.”

She also emphasized that it’s not just government agencies collaborating on these cases. It’s cryptocurrency exchanges and other industry players as well. “If a big bank suffers a cyberattack or inadvertently facilitates terrorism financing, other banks don’t really care. But if something like that happens to an exchange, it can affect Bitcoin’s value, so everyone has skin in the game,” she said. “The cryptocurrency world is smaller, so it’s much easier for normal users to interact with an address that has ties to terrorism financing if that address isn’t shut down, which creates problems for everyone. So partly for that reason, exchanges have responded really well and been helpful when we reach out for help on these cases.”

Domestic extremism case study: Alt-right groups and personalities involved in January 2021 Capitol riot received over \$500K in Bitcoin from French donor one month prior

Terrorism doesn’t originate solely overseas. In recent years, U.S. law enforcement agencies have made it a priority to fight domestic extremism too. We’re working alongside our government partners to investigate designated domestic terrorist groups’ usage of cryptocurrency and ensure digital assets aren’t used to fund acts of violence. The case study below is the result of our investigation into cryptocurrency donations received by figures and groups involved in the January 2021 riots at the U.S. capitol.



On January 6, 2021, Americans were shocked as a large group of Donald Trump supporters stormed the U.S. Capitol Building in protest of his 2020 election loss, following a rally that included a speech from Trump himself. Five people died, including two police officers, and significant damage was done to the building, including to many congressional representatives' offices. Several prominent members of the alt-right either took part in the raid or were present just outside the Capitol, including internet personality [Nick Fuentes](#).



Nick Fuentes outside the Capitol. Photo credit to [Nick Fuentes](#) on Twitter.

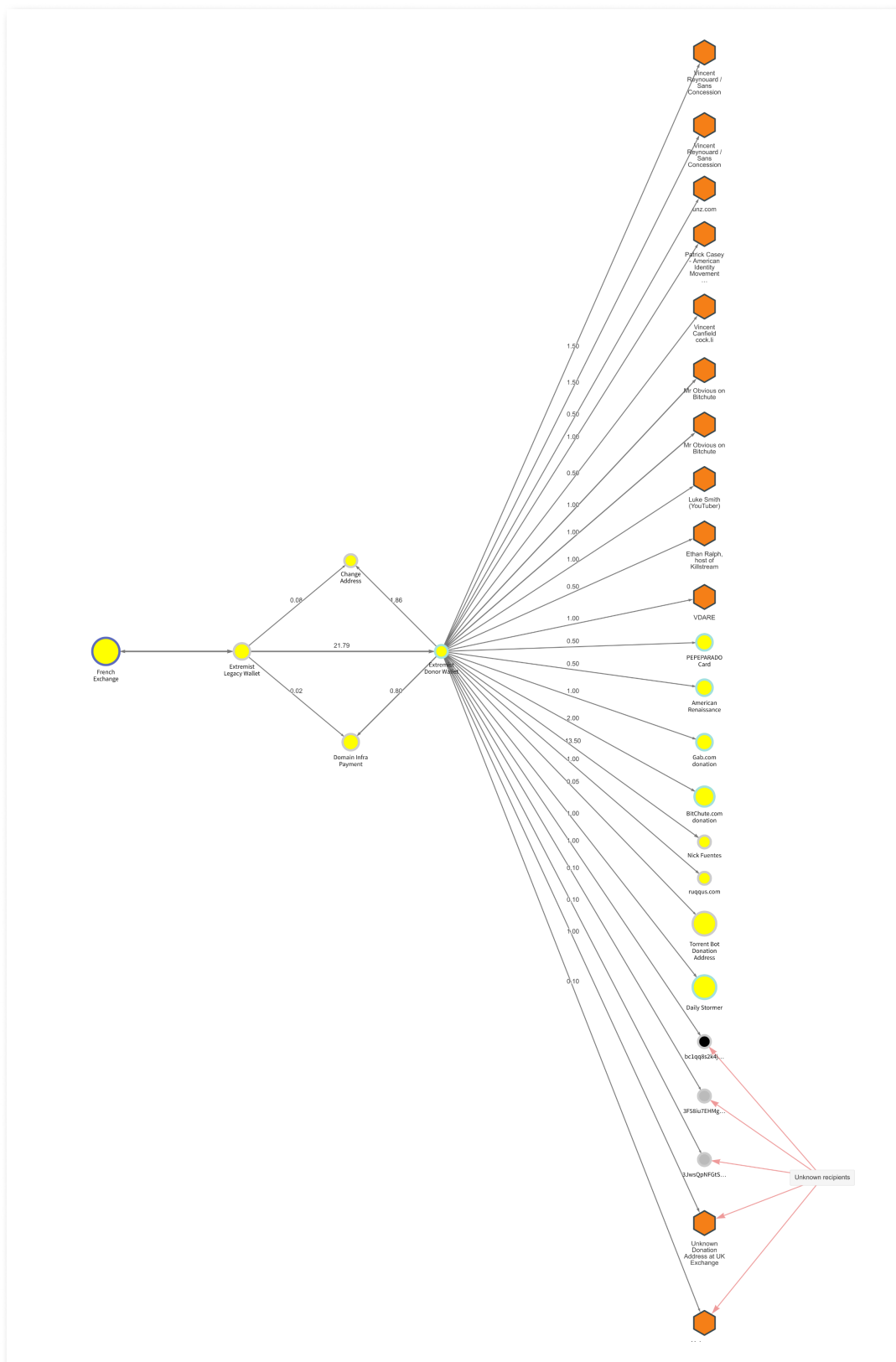
It's unclear to what degree the attack on the Capitol was planned in advance. [ProPublica reports](#) that in the weeks leading up, many Trump supporters discussed turning the event violent on Parler, a rightwing social media app [now banned](#) by most major tech platforms. However, we now have evidence that many alt-right groups and personalities, including Fuentes, received large Bitcoin donations in a single transaction that occurred a month before the riot on December 8. We have also gathered evidence that strongly suggests the donor was a now-deceased computer programmer based in France.

While we won't share the donor's identity publicly, we'll walk you through how we made the identification and provide details on the donations below. The information we've uncovered shows that domestic extremism isn't strictly domestic. International networks play a role as well, which we see reflected in the nationality of this donor. The donation, as well as reports of the planning that went into the Capitol raid on alt-right communication channels, also suggests that domestic extremist groups may be better organized and funded than previously thought.



The donations

On December 8, 2020, a donor sent 28.15 BTC — worth approximately \$522,000 at the time of transfer — to 22 separate addresses in a single transaction. Many of those addresses belong to far-right activists and internet personalities.

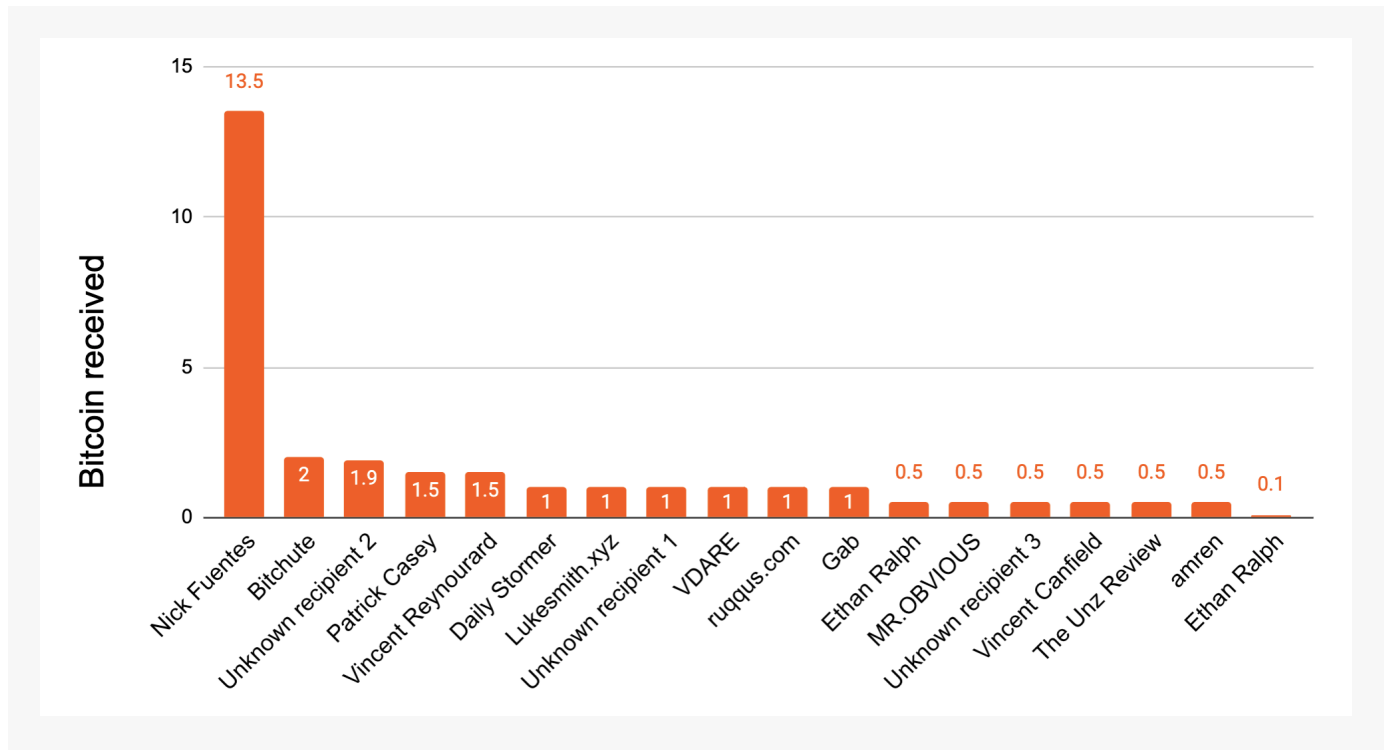




Here, we see that the donor sent Bitcoin to several alt-right organizations and online personalities. Unknown recipients are grouped in the lower right-hand corner.

Nick Fuentes received 13.5 BTC — worth approximately \$250,000 at the time of the transfer — making him by far the biggest beneficiary of the donation. However, several others received significant funds as well, including anti-immigration organization [VDARE](#), alt-right streamer [Ethan Ralph](#), and several addresses whose owners are as yet unidentified.

Who received funds from the December 8, 2020 extremist donation?

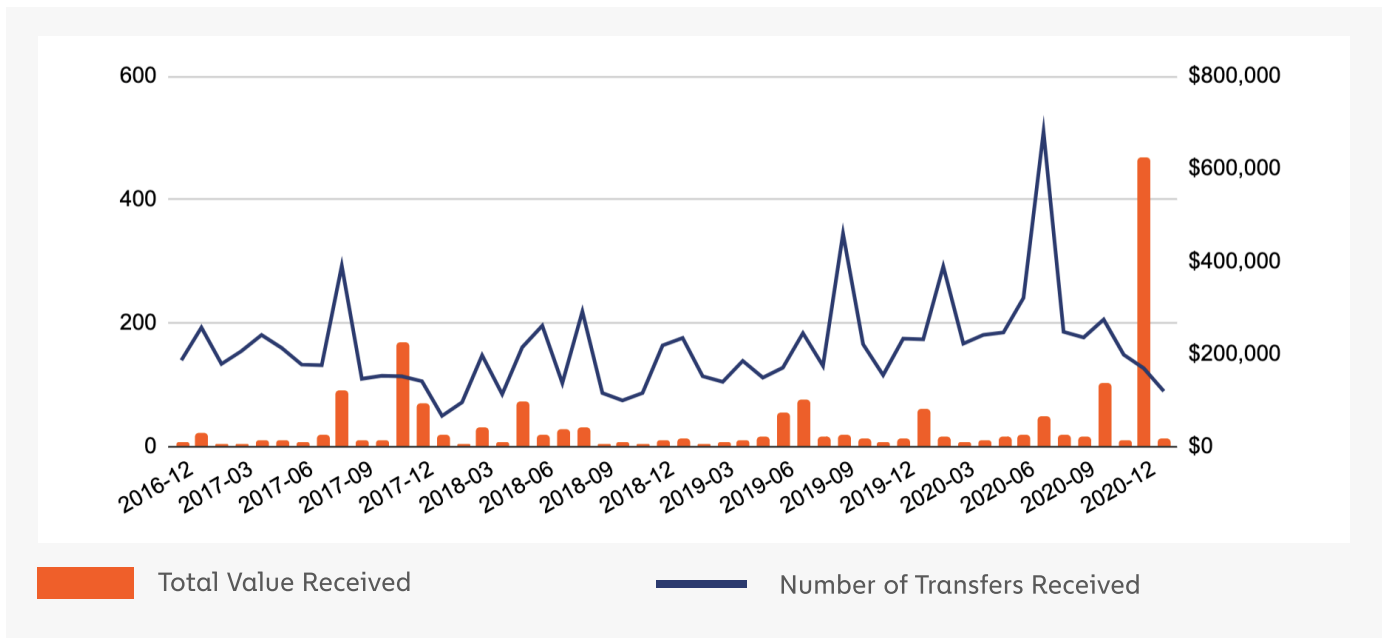


While there's no evidence yet that Fuentes entered the Capitol — in fact, he [explicitly denies](#) entering the building — he was present at the initial rally and seen outside the Capitol as the rioting began. Fuentes [promoted the rally](#) that preceded the violence in the month before on social media. [PBS notes](#) that in the days leading up, Fuentes encouraged his audience to engage in extreme behavior to prevent Joe Biden's election from being certified, even implying that they should kill state legislators. Fuentes had previously [been banned from YouTube](#) for hate speech, including Holocaust denial and promotion of other conspiracy theories.

The December 8 donation of over \$250,000 worth of Bitcoin is by far the largest cryptocurrency donation Fuentes has ever received. Previously, the most he had ever received in a single month was \$2,707 worth of Bitcoin.



Total Value Received by Domestic Extremists in Cryptocurrency

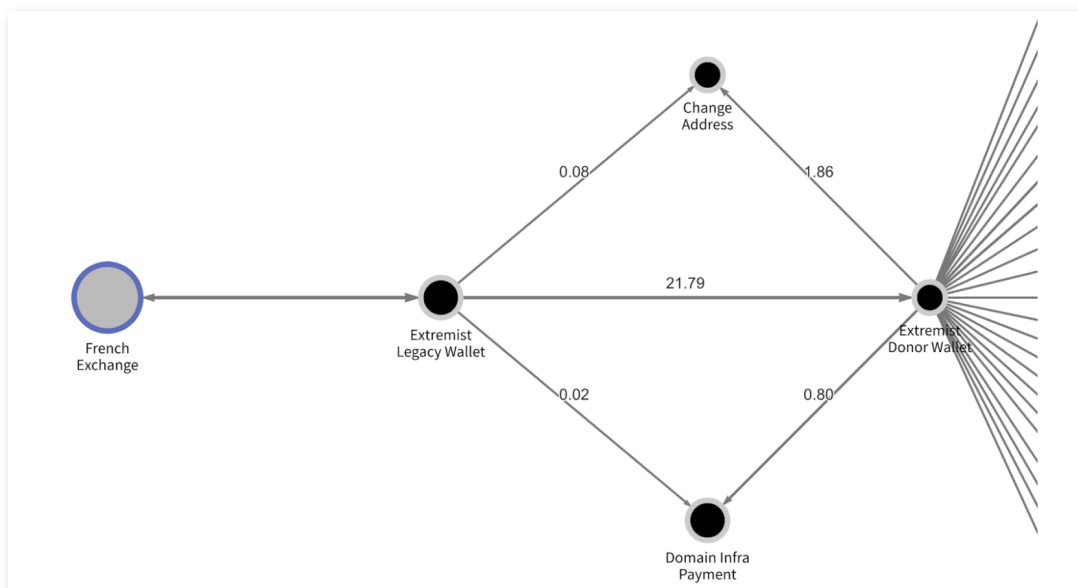


Currencies included: BTC

In fact, as we see in the graph above, this multi-recipient donation made December 2020 the single biggest month we've ever observed in terms of cryptocurrency received by addresses associated with domestic extremism. Still, this donation isn't a one-off. The data shows that domestic extremists have been receiving a steady stream of cryptocurrency donations since 2016.

Who is the extremist donor?

The extremist donor funded his donation wallet with cryptocurrency from a French exchange, which he moved to the donation wallet via an intermediary we've labeled "Extremist Legacy Wallet."





The Extremist Legacy Wallet first became active in 2013, suggesting that the extremist donor is a relatively early adopter of Bitcoin whose holdings have grown in value significantly. Using open-source intelligence, we discovered one BTC address associated with the Extremist Legacy Wallet is registered on NameID, a service that allows users to associate their online identity, email address, and other information with their Bitcoin address. In this case, the extremist donor associated his Bitcoin address with the pseudonym “pankkake.”

id/pankkake

The Namecoin identity `id/pankkake` has some public profile information registered:

Email `pankkake@...net`
OpenPGP `[redacted]`
Bitcoin `1[redacted]`

Copyright © 2013–2016 by [Daniel Kraft](#). NameID is free software under the terms of the [AGPL v3](#), check out the [source code](#)!

BTC: `1Nameid3brhZrbTN1M7t6afMAfVBiGioJT` | NMC: `NAmid5L2ZcaQFszYwk4sa929zbQymaaWa`

In addition to his Bitcoin address, the extremist donor also listed an email address and an OpenPGP signature.

Searching for information on the email address led us to a personal blog we believe belongs to the extremist donor, and which identifies him as a French computer programmer. They had been inactive since 2014 until a new post was published on December 9, 2020 – the day after the donations were made. Shockingly, the post appears to be a suicide note. You can read it in the screenshot below.

The End.txt

If you're reading this, I am deceased. This is a scheduled message made to be published in the future; thus there is no chance that I survived.

I suppose the first question that comes to mind is why I did end my life. I sincerely wonder if some people saw it coming, or if I managed to hide it. What you need to understand is the inevitable aspect of it. Let me explain:

About eight years ago, I started having multiple health issues. Some have been diagnosed, but much too late. Since then, my health has globally worsened, with its ups and downs. I am more and more handicapped in day to day life, and even though it's still possible to live correctly, I feel trapped. To be clear, I do not think degraded living conditions are enough to give up. The required condition tends to be lack of hope. In the case of my health, it has become clear a few years ago already, and that's at that time I realized my own mortality, and the length and probable end of my life.

I could list all my issues; however I doubt it would explain much more. Their consequences is being always tired (having a good night is now a distant memory), and the inability to enjoy my hobbies (e.g. timinutis). There's also the fact that ~~trigeminal~~ neuralgia is also known as the "suicide disease". Some of my issues are likely linked; in any case I feel that my body is under siege in multiple ways, always more powerful and numerous. Moreover, the temporary and unpredictable aspect leave me vulnerable and unable to achieve my goals. I am a prisoner of my own body that seem to be three times my age. I am actually wondering what an autopsy could reveal, which can seem paradoxical as I won't be there to see the results.

Thus, this isn't something I decided on a whim. Sure, I would have preferred doing it in a better planned way, but various factors pushed me to do it now. I will add that I don't take mood-altering medication. I even stopped one if the past for that reason. I made some rules during those eight years to avoid doing something too eagerly. So, for height years, I went on, trying to avoid thinking about the coming end. By lying, either to my peers but mostly to myself. Even though my life didn't change much, that isn't the case of my ideals.

I thought for a long time that I would become immortal through scientific progress. "Normal" people when exposed to that idea would say they'd be eventually bored. More me, it always seemed impossible. Coming back to reality was harsh. I could blame my current state on incompetence from some people, bad luck, but there's hedonistic choices I made that are not negligible. But it doesn't really matter and I can't do anything about it.

In other circumstances, I think I wouldn't have missed not having children. I am at least saddened I won't see the children of my family and friends. It's hard to explain, but now I get it. That's what brings tears to my eyes, more than my incoming death. There's some other things I regret, like the lack of religion, of meaning to my life. The time wasted on useless things. The rejection of nature.

As a matter of fact, I have a bittersweet feeling at this time. Deliverance awaits. But I'm still putting myself in the shoes of my peers and I think of the pain I'm going to cause. Even though I'm trying my best, in particular by not dying at home, and in a more interesting way that I would have thought. For those who will miss me, I don't regret these years by your side.

It's a selfish act, that I wouldn't have gone through if people really depended on me. However, I can't imagine myself spending my last days more and more diminished, not contributing to society, not fighting to preserve it. And that's one of the things that completely changed for me these last years: I care about what happens after my death. That's why I decided to leave my modest wealth to certain causes and people. I think and hope that they will make a better use of it.

I would like to go back to the second necessary condition to suicide, the lack of hope. After all, even when everything is wrong, there's no reason to end it if there is any chance things will get better. After all these years, I have no doubts about my health. However, there's another side to it.

Maybe it is because I am more aware, or because I identify more easily my degenerating body to other things; still, I can't avoid noticing the decline of Western civilization. It took me some time to accept it: maybe more than my own fate. I won't try to convince anyone here, or digress on ~~Bessond~~, building 7 or wooden doors. What I see is an almost worldwide Weimar republic, and the existence of Evil. Still, the enemy is within. It's the constant self-flagellation, the self-loathing, the rejection of our ancestors and our heritage. As for myself, while I am going to do something that might evoke it, I completely reject this way of thinking.

As some of you already knew, I wanted to go back to a simpler life, away from the industrial revolution and its consequences that have been a disaster for the human race. The sanitary panic, always more senseless, has been used to harm that, while propping up an industry that I was a part of but am now disgusted by. Still, I know well that IA couldn't have done it anyway due to my poor health.

While it's a long-term trend, this year in particular has shown how submissive the population can be, first when accepting unprecedented civil liberties violations on the pretense of a virus less dangerous than seasonal flu, then kneeling down for a career criminal who happened to die of an overdose while resisting arrest, or pretend to fight for freedom of speech while jailing people for their ideas. Oddly, as trust in media is at historic lows, the population has blindly accepted those reality distortions. To top it all, P9 has been pushed back to 2021.

But that's also the proof that things can change rapidly. For the worst here, but why not for the better in the future? We come back to my previous perspective, I see young people who give me hope, who understood sooner than me that we must secure the existence of our people and a future for our children. I feel the need to fight and the idea to passively watch decline now feels unbearable.

I've stressed the inevitable aspect for multiple reasons. One is that I wouldn't want anyone to donate to suicide prevention charities in my name. Better celebrate life, and think about your family's future and your own.

Some technical details:
- Most of the services I run are paid for at least a year.



French publication 20 Minutes [eventually confirmed](#) the death of a French computer programmer who appears to have been the owner of the Bitcoin wallet from which the extremist donations were sent in December, and the blog on which the suicide note was published.

Most of the note details the author's health difficulties, which he says prompted him to commit suicide, but the sections we've highlighted provide strong evidence that the author is the extremist donor. He mentions that he has "bequeathed [his] fortune to certain causes and certain people," and cites several alt-right talking points in his analysis of the world today. For instance, he states his belief that "Western civilization is declining," and claims that Westerners are encouraged to hate their "ancestors and heritage." He also seemingly alludes to his belief that George Floyd died of a drug overdose rather than due to the actions of the police officer who violently apprehended him. All of these are common beliefs on the alt-right, and paint a picture of the donor's motivations for sending cryptocurrency to so many far right extremist figures.

Standing together against domestic extremism

While we don't know if these donations directly funded the violent gathering at the Capitol or any associated activity, the timing certainly warrants suspicion. As the Biden administration gears up to fight [domestic extremism](#), these donations are a reminder of the need to track the cryptocurrency activity of all groups and individuals designated as terrorists, including those operating on U.S. soil. As mainstream payment platforms remove extremist groups and figures, we may see them embrace cryptocurrency more as a donations mechanism. Luckily, thanks to the inherent transparency of cryptocurrency blockchains, law enforcement can track these transactions in real time and work with cryptocurrency businesses to prevent funds from reaching violent groups who may use them to fund their operations and commit acts of violence. Chainalysis is actively looking to identify any additional extremist payments and activity and will keep our customers updated.



Conclusion



Crypto Crime Predictions for 2021

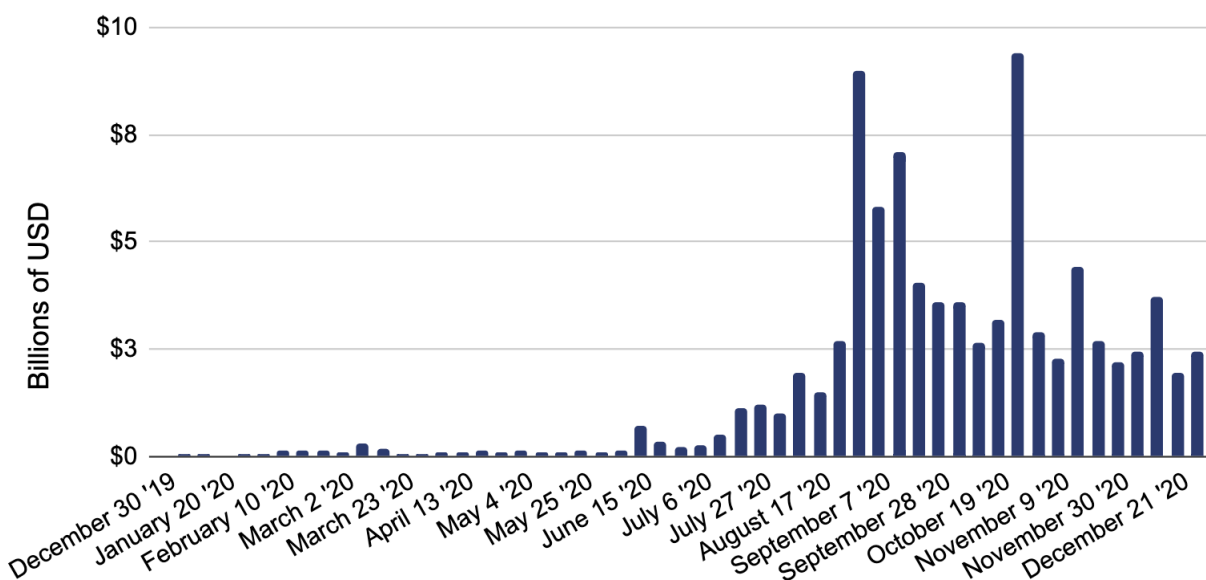
Cryptocurrency is an exciting industry because it's always evolving. In 2020, we've seen DeFi take off, institutional dollars flow in thanks in part to tailor-made platforms like [Coinbase Prime](#), and exchanges like Kraken become [chartered banks](#) following new regulatory guidance from the U.S. government. Perhaps most exciting is that all of this happened in the face of a global pandemic — a true test of cryptocurrency's value as a safe haven asset — during which Bitcoin's price surged.

However, just as the cryptocurrency industry is always evolving, so too are the bad actors who commit cryptocurrency-related crime. Below, we offer our predictions for how crypto crime will change in 2021.

DeFi will play a bigger role in crypto crime

As we alluded to above, DeFi, which stands for [decentralized finance](#), has skyrocketed in popularity this year.

Total Weekly Value Received by DeFi Platforms | 2020

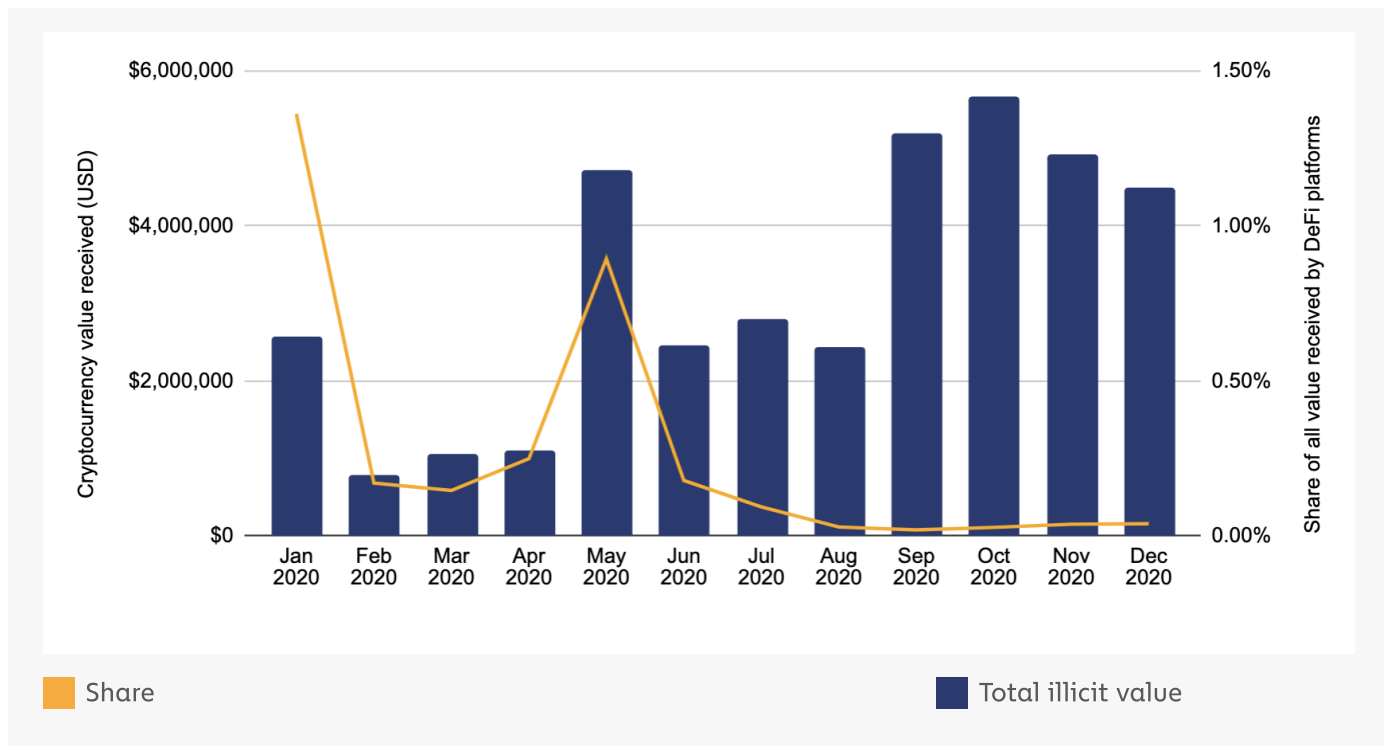




For context, DeFi platforms are decentralized apps built on top of smart contract-enriched blockchain platforms – primarily the Ethereum network – that let users automatically execute specific financial transactions such as trades and loans when certain conditions are met. DeFi platforms never take possession of a user's funds, and instead simply route them between users' wallets based on the conditions outlined in the underlying smart contracts without human intervention. Many believe that means they aren't subject to the same regulations as typical cryptocurrency businesses that take custody of users' funds. And because DeFi platforms can theoretically run without human intervention, there's often no team or organization keeping records or intervening when something goes wrong.

The potential lack of human intervention makes DeFi platforms appealing to users who value privacy, but potentially also to criminals looking to launder ill-gained funds. In the chart below, we approximate that activity thus far by looking at the volume of cryptocurrency that's moved from criminal addresses to DeFi platforms.

Total value and share of all value sent to DeFi platforms from criminal addresses | 2020



In total, more than \$38 million worth of illicit cryptocurrency moved to DeFi platforms in 2020, with the monthly figure generally rising throughout the year. The [KuCoin exchange hack](#) was a notable example of this, as the cybercriminals involved moved substantial portions of the \$275 million worth of cryptocurrency stolen to DeFi platforms – though in this case, luckily, the creators of the platforms in question retained enough control to freeze some of the transfers.

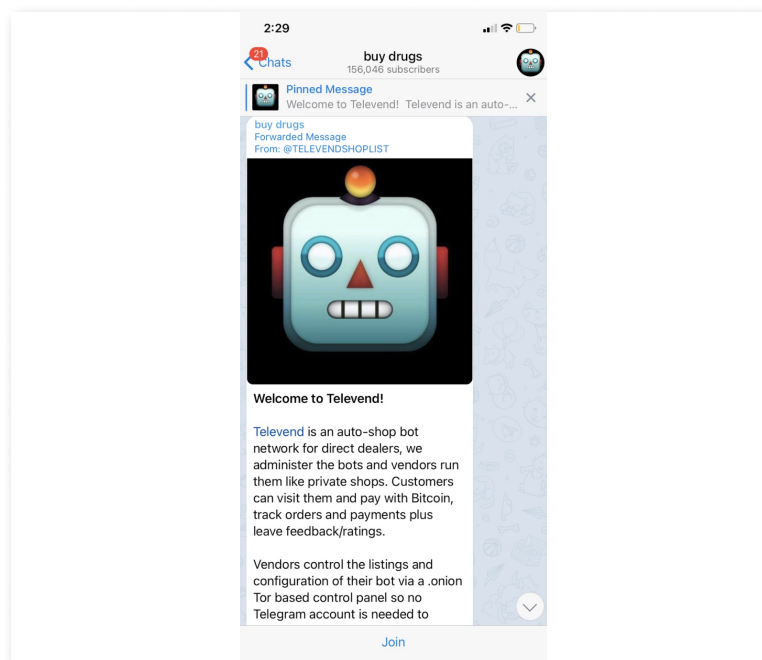


Still, we expect cybercriminal use of DeFi for money laundering to increase in 2021. DeFi platforms such as decentralized exchanges have existed for years, but took off in 2020 due in large part to improvements in user interfaces, which made them much easier for relatively inexperienced cryptocurrency users. This in turn led to greater liquidity, which made DeFi platforms even more appealing, creating a flywheel effect that led to even more growth. We expect those trends to continue in 2021, which will only make DeFi more attractive to criminals. The question that remains is whether the most popular platforms will be those where administrators retain enough control to prevent criminal transactions, as we saw in the KuCoin hack.

More decentralization in darknet markets

Darknet market decentralization is another trend we've seen pick up in 2020, and that we think will continue into 2021 and beyond. As we discuss elsewhere in this report, it's never been harder to run a darknet market. More markets went out of business than ever in 2020, and not due to Covid. Competition has intensified between darknet markets, with some [initiating denial-of-service \(DOS\) attacks](#) against rival markets, and several others exit scamming, which has significantly reduced buyer trust. At the same time, law enforcement is shutting down more markets and putting administrators in jail, leaving market administrators — who despite all the risk they take on receive roughly 5% commissions on sales — less willing to continue their work.

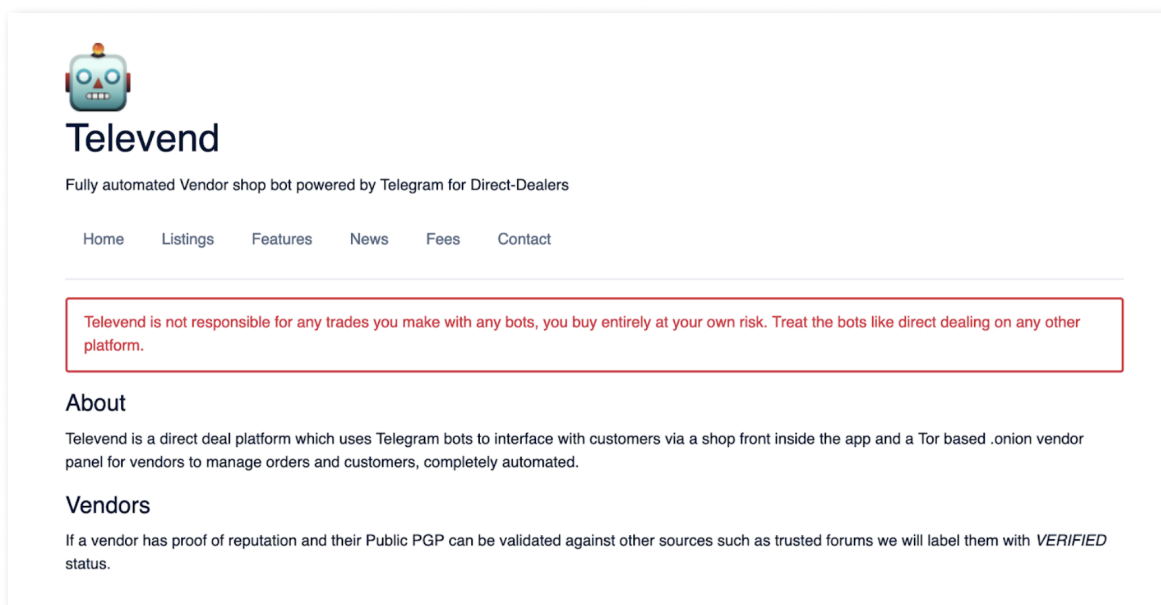
But a new decentralized model embodied by platforms like Televend may solve many of these problems for darknet markets. [Televend](#) is a Telegram-based platform with over 150,000 users where darknet market vendors can sell drugs through automated chatbots, whose communications with buyers are highly encrypted.



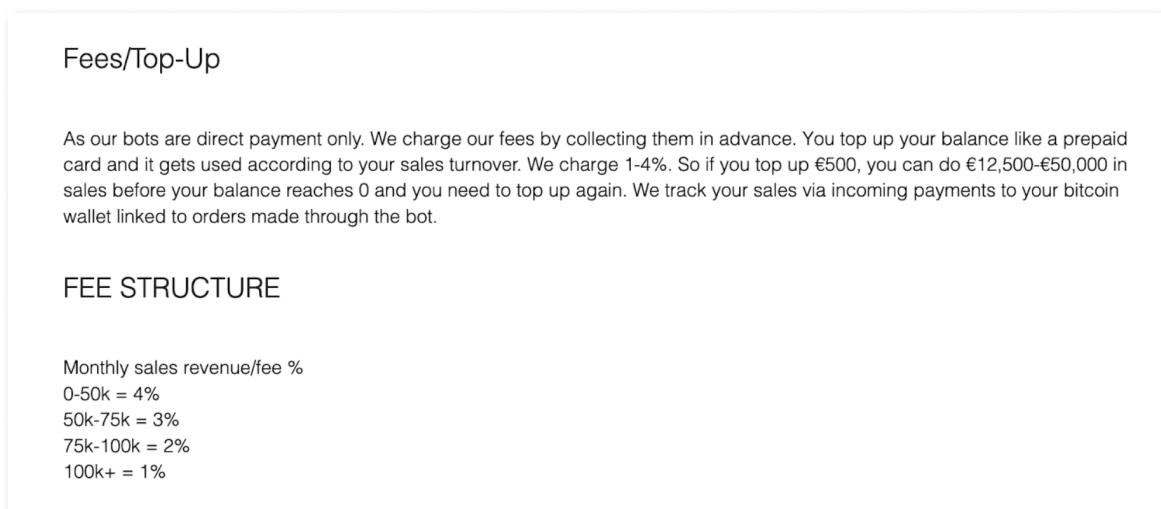
A screenshot of Televend



Buyers simply access Televend's Telegram group, where they find a directory of drug vendors broken down by region and products on offer. From there, they simply place orders with their chosen vendor's chat bot, receive an automatically-generated Bitcoin address to which they send payment, and wait for their drugs to arrive in the mail.



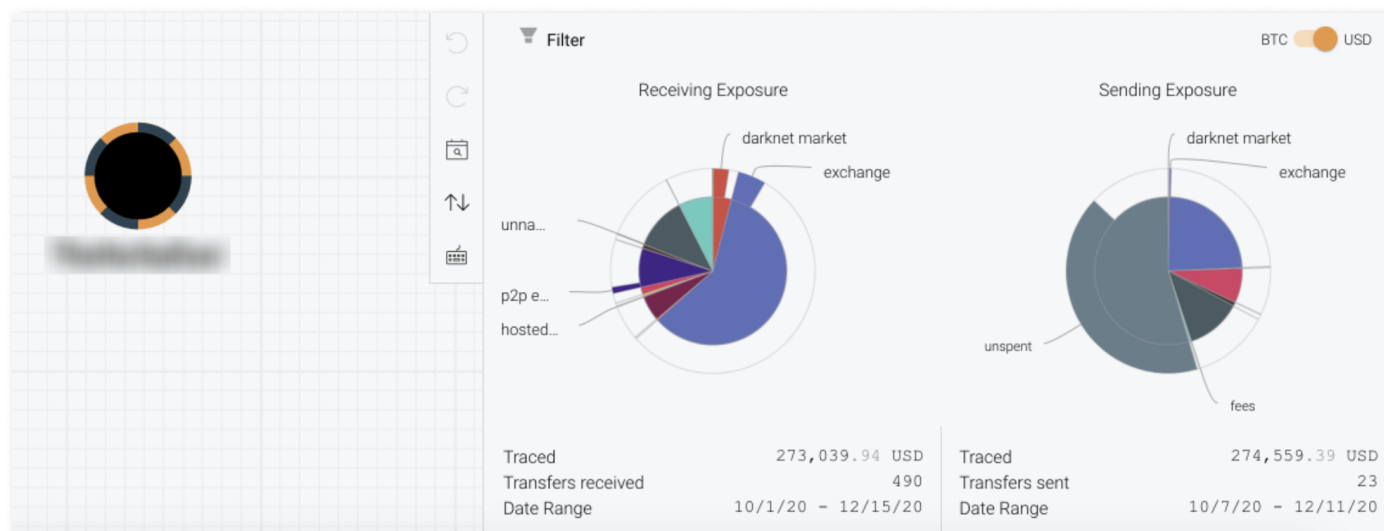
A screenshot from Televend's darknet site



Televend's fee structure explained

Televend receives commissions on each sale, but never actually touches the funds, so there's no central entity for law enforcement to track through blockchain analysis – the transactions blend in much more easily.

We studied the Bitcoin transaction history of one prominent Televend vendor, which you can see a summary of in the [Chainalysis Reactor](#) screenshot below.



Since Televend became active in October 2020, this vendor's wallet has received over \$270,000 worth of Bitcoin across nearly 500 transactions. Customers appear to have paid mostly through cryptocurrency exchanges, which is also where the vendor has sent most of the funds. However, while we don't show it above, this wallet has been active since June 2019 — Televend allows vendors to receive their earnings to any address of their choosing — and received an additional \$1.4 million worth of Bitcoin before Televend opened. It therefore appears likely that this vendor was active on traditional darknet markets before migrating to Televend. This vendor is one of over 150 active on Televend, though it's unclear if the others are bringing in as much revenue.

We expect platforms like Televend to grow and take in a larger share of total darknet market revenue in 2021, as their decentralized nature makes them more resilient to attacks from both law enforcement and rival markets. While future decentralized markets may run on platforms other than Telegram, Televend shows that the encrypted messaging platform can offer customers an easy buying experience.

Exchanges will treat other services with more scrutiny as risk-based compliance becomes the norm

Traditionally, too many exchanges have relied on other cryptocurrency services' (including other exchanges') publicly stated KYC and AML policies when assessing their riskiness. If the policy checked out, many exchanges would treat the service as if it were safe. But that won't cut it anymore in an era when [institutional dollars](#) are flowing into cryptocurrency like never before. Whether they're buying cryptocurrency of their own as an investment, offering custodial services, or accepting cryptocurrency businesses as banking clients, mainstream



financial institutions are going to need to enforce compliance more stringently than cryptocurrency businesses themselves have. That means they won't be taking compliance policies at face value. Instead, they'll insist on taking advantage of cryptocurrency's inherent transparency.

In a monetary system where every transaction is recorded on a public, unchangeable ledger, why wouldn't a financial institution aggressively analyze that information to ensure they're working with the safest possible businesses? Exchanges and other cryptocurrency businesses who want to work with these financial institutions will need to follow suit and [assess their own counterparties](#) with equal rigor. Increased compliance scrutiny by cryptocurrency exchanges will drive crypto crime down, as more wrongdoers will be reported to the authorities and stopped sooner than they otherwise would have been. In the long run, these efforts by exchanges will also remove some of the incentive to use cryptocurrency in criminal activity, as it will become much harder for cybercriminals to convert cryptocurrency into cash if they can't use exchanges.

The crypto crime outlook has never been better

Some of the upcoming advancements of cryptocurrency will make it more difficult for law enforcement and compliance professionals to detect and fight criminal activity. However, we remain confident that both groups, along with the institutional investors we discussed earlier, can come together to meet the challenge, and ultimately create a safer cryptocurrency ecosystem for all participants. Chainalysis looks forward to supporting their efforts.

Authors

Kim Grauer

grauer@chainalysis.com

Henry Updegrave

henry.updegrave@chainalysis.com

ABOUT CHAINALYSIS

Chainalysis is the blockchain analysis company. We provide data, software, services, and research to government agencies, exchanges, financial institutions, and insurance and cybersecurity companies in over 50 countries. Our data platform powers investigation, compliance, and risk management tools that have been used to solve some of the world's most high-profile cyber criminal cases and grow consumer access to cryptocurrency safely. Backed by Accel, Addition, Benchmark, Ribbit, and other leading names in venture capital, Chainalysis builds trust in blockchains to promote more financial freedom with less risk.

For more information, visit www.chainalysis.com.

GET IN TOUCH:

info@chainalysis.com

FOR MORE CONTENT:

visit blog.chainalysis.com

This document is not intended as legal advice. We recommend you consult your general counsel, chief compliance officer, and/or own compliance policies & procedures for regulatory, legal or compliance-related questions.

Building trust in blockchains

Appendix 2

Ending the Shell Game: Cracking Down on the Professionals who
Enable Tax and White Collar Crimes (OECD Report) - 2021



Ending the Shell Game

Cracking down on the Professionals
who enable Tax and White Collar Crimes

**Ending the Shell Game:
Cracking down on the Professionals who
enable Tax and White Collar Crimes**

This document was approved by the OECD Committee on Fiscal Affairs on 16 November 2020 and prepared for publication by the OECD Secretariat.

This document, as well as any data and map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Please cite this publication as:

OECD (2021), Ending the Shell Game: Cracking down on the Professionals who enable Tax and White Collar Crimes, OECD Publishing, Paris.

<http://www.oecd.org/tax/crime/ending-the-shell-game-cracking-down-on-the-professionals-who-enable-tax-and-white-collar-crimes.htm>

Photo credits: © Zenza Flarini – Shutterstock.com.

Corrigenda to OECD publications may be found on line at: www.oecd.org/publishing/corrigenda.

© OECD 2021

You can copy, download or print OECD content for your own use, and you can include excerpts from OECD publications, databases and multimedia products in your own documents, presentations, blogs, websites and teaching materials, provided that suitable acknowledgment of the source and copyright owner is given. All requests for public or commercial use and translation rights should be submitted to rights@oecd.org. Requests for permission to photocopy portions of this material for public or commercial use shall be addressed directly to the Copyright Clearance Center (CCC) at info@copyright.com or the Centre français d'exploitation du droit de copie (CFC) at contact@cfcopies.com.

Table of contents

Abbreviations and Acronyms	5
Executive summary	7
1 The role of professional enablers in tax and other financial crimes	10
1.1. Who are professional enablers	10
1.2. Services provided by professional enablers	11
2 Identifying professional enablers	22
2.1. Organisational awareness of professional enablers	22
2.2. Measuring the threat of professional enablers	22
2.3. Detection through development and analysis of professional enabler indicators	23
2.4. Data sources for identifying professional enabler activity	24
3 Disrupting professional enablers	27
3.1. Legal sanctions for professional enablers	27
3.2. Injunctions	30
3.3. Professional supervision and regulation	31
4 Deterring professional enablers	34
4.1. Preventing abuse	34
4.2. Disclosure facilities	38
4.3. Mandatory disclosure rules	39
5 Effective investigations: across government and across borders	40
5.1. Domestic whole-of-government approaches	40
5.2. International co-operation	42
5.3. JITSIC Data Leaks Group's work on the Intermediaries Disruption Strategy	45
References	47
Annex A. Other related work	51
Annex B. Example of template for Group EOI request	53

Boxes

Box 1. Foreign trusts used in ownership chains to hide beneficial ownership and financial flows	13
Box 2. Dividend structure to obscure beneficial ownership and investment income offshore	14
Box 3. Professional enablers setting up offshore structures targeted in a sting operation	14
Box 4. Use of offshore service provider for the purpose of concealing financial flows	15
Box 5. Falsified documents to evade taxation on income	16
Box 6. Falsified documents to obtain an unjustified tax refund	16
Box 7. Phoenix company fraud	17
Box 8. Dividend stripping and “cum-ex” arrangements	18
Box 9. Crypto-asset mixing service (CMS) case – Bestmixer.io seizure	21
Box 10. Possible indicators for use in risk assessment exercises for detecting involvement of professional enablers	23
Box 11. Scoring model to identify professional enablers in Country X	24
Box 12. Data sources in professional enabler investigations	24
Box 13. India’s use of data sources in professional enabler investigations	25
Box 14. Administrative sanctions against facilitators in France	28
Box 15. Legal reforms in Mexico to tackle professional enablers	28
Box 16. Investigation and prosecution of professional enablers in France	29
Box 17. India’s Task Force on Shell Companies	32
Box 18. The Australian Taxation Office – usage of taxpayer alerts to address new tax schemes	35
Box 19. HMRC’s “Promote and prevent” approach to encouraging compliance	36
Box 20. The United Kingdom’s legislation creating corporate responsibility to prevent criminal facilitation of tax crime	37
Box 21. The United Kingdom’s National Economic Crime Centre	42
Box 22. Coordinated day of action by the Joint Chiefs of Global Tax Enforcement	44
Box 23. BitClub network case	45

Abbreviations and Acronyms

AEOI Standard	Standard for Automatic Exchange of Financial Account Information in Tax Matters
AML	Anti-Money Laundering
ATO	Australian Taxation Office
CIN	Corporate Identification Number
CMS	Crypto-asset Mixing Service
CRS	Common Reporting Standard
CTF	Counter-Terrorism Financing
DLG	JITSIC Data Leaks Group
DIN	Director Identity Number
DNFBP	Designated Non-Financial Businesses and Professions
DOJ	Department of Justice of the United States
EU	European Union
FATF	Financial Action Task Force
FIOD	Dutch Fiscal Intelligence and Investigation Service
Global Forum	Global Forum on Transparency and Exchange of Information for Tax Purposes
HMRC	Her Majesty's Revenue and Customs
IAD	Income and Asset Disclosure
ICAI	Institute of Chartered Accountants of India
ICIJ	International Consortium of Investigative Journalists
IDS	JITSIC Intermediaries Disruption Strategy
IESBA	International Ethics Standard Board for Accountants
IMF	International Monetary Fund
IRS	Internal Revenue Service of the United States
J5	Joint Chiefs of Global Tax Enforcement
JITSIC	Joint International Taskforce on Shared Intelligence and Collaboration
NECC	National Economic Crime Centre of the United Kingdom
NFRA	National Financial Reporting Authority of India

OECD	Organisation for Economic Co-operation and Development
PAN	Permanent Account Number
PEPs	Politically Exposed Persons
StAR	Stolen Asset Recovery Initiative
STR	Suspicious Transaction Report
TFTC	OECD Task Force on Tax Crimes and Other Crimes

Executive summary

Over the last decades, the world has witnessed increasingly sophisticated financial crimes being perpetrated across borders – and the public interest in addressing such issues has also grown, as has been evidenced in the media through widely publicised leaks such as the Panama and Paradise Papers (ICIJ, 2020^[1]). These crimes are often facilitated by lawyers, accountants, financial institutions and other professionals who help engineer the legal and financial structures seen in complex tax evasion and financial crimes. The small segment of professionals that generate opportunities to facilitate the commission and / or concealment of such crimes undermine not only the rule of law, but their own profession, public confidence in the legal and financial system, as well as the level playing field between compliant and non-compliant taxpayers. Ultimately, this undermines the public interest in ensuring taxes are paid and available for public use. Therefore, targeting professional enablers and disrupting their activities is a key avenue for addressing criminal activity at the source.

The majority of professionals are law-abiding and play an important role in assisting businesses and individuals to understand and comply with the law and helping the financial system run smoothly. Such law-abiding professionals are to be differentiated from a small set of professionals who use their skills and knowledge of the law to actively promote, market and facilitate the commission of crimes by their clients. This report seeks to support policy makers and law enforcement authorities to address the actions of that small set of lawyers, tax advisors, notaries, financial institutions and other intermediaries that are “professional enablers,” intent on facilitating wrong-doing by their clients.

Professional enablers play an integral role in making it easier for taxpayers to defraud the government and evade their tax obligations, such as by offering non-transparent structures and schemes to conceal the true identity of the individuals behind the illegal activities undertaken. This type of activity has become a subject of international and domestic political significance and been covered extensively in the media. These scandals also reveal the broader problem of tax evasion in society: that it undermines public confidence as well as the public purse, and gives rise to an increasing sense of instability caused by inequality. In the wake of the COVID-19 pandemic, emerging risks continue to come to light, such as the potential role of professional enablers in perpetrating fraudulent access to pandemic support funding. This highlights the persistent risk professional enablers create in society.

Governments have therefore recognised the need to target the professional enablers who actively pursue opportunities for, and conceal the commission of, tax crimes and other financial crimes, in order to disrupt a crucial part of the planning and pursuit of criminal activity. This is not the only strategy that is needed to address all tax and financial crimes; however, it is one that can be cost-effective by reducing the accessibility of sophisticated means of tax evasion and fraud, thereby narrowing the opportunities for such crimes to take place.

Countries have reported, however, that while they recognise the importance of the issue, there are challenges in being able to effectively tackle professional enablers. This report explores different governmental strategies to detect, deter and disrupt the activities of professional enablers.

This report

This report sets out actions governments can take to address the issue of professional enablers in five key areas:

1. Understanding the role of professional enablers;
2. Methods for identifying professional enablers;
3. Legal and regulatory frameworks to disrupt professional enablers;
4. Strategies for deterring professional enablers; and
5. Domestic and international multilateral efforts to address professional enablers.

While professional enablers include a wide range of individuals, intermediaries and institutions providing an array of services that may vary in specifics from one country to another, this report highlights the common approaches used in combatting the use of professional enablers. This report is primarily targeted at authorities with responsibility over tax crimes, but it is also intended to be helpful to other law enforcement authorities, given the links between tax offences and other financial crimes such as money laundering or corruption and the commonalities in the ways these crimes are committed, and particularly insofar as it outlines the importance of multi-agency and multilateral action.

This report has been prepared by the OECD Task Force on Tax Crimes and Other Crimes, drawing on the experience of both OECD and non-OECD member countries.

Conclusions and recommended counter-strategies to combat professional enablers

This report fosters better understanding of the problem posed by professional enablers and the range of actions that can be taken in response, with a view to encouraging countries to establish a dedicated national strategy to tackle professional enablers who actively participate in tax crimes and other financial crimes.

This report calls on countries to consider adopting a strategy, or strengthen their existing strategy, for addressing professional enablers. In devising or strengthening their national strategy, countries should consider the recommended counter-strategies to combat professional enablers outlined in Table 1 below.

Table 1. Recommended counter-strategies to combat professional enablers

Recommendation	Key elements
Awareness <i>Ensure tax crime investigators are equipped with the understanding, intelligence and analytics skills to identify the types of professional enablers operating in their jurisdiction, and to understand the risks posed by the ways that professional enablers devise, market, implement and conceal tax crime and financial crimes.</i>	<ul style="list-style-type: none"> • Consider the need for a common definition of professional enablers, recognising the role and different levels of culpability within different sectors • Educate across government agencies about the types of services provided by professional enablers and why they pose a risk • Develop risk indicators for identifying professional enablers, drawing on a wide range of available data sources

Legislation	<ul style="list-style-type: none"> • Consider whether there is a need for a specific professional enabler liability regime, to further deter this behaviour • Assess whether the legal framework provides sufficient ability for prosecutors to prove the offence of acting as a professional enabler • Reflect on whether professional privilege poses a barrier to successful investigation and prosecution • Consider whether the ability of suspects to settle cases hinders the deterrent effect of the law • Explore whether professional supervisory or regulatory bodies can be used to stop professional enablers from operating
Deterrence and disruption	<ul style="list-style-type: none"> • Prevent abuse through communication with taxpayers and education of professionals • Leverage the role of, and information available to, professional supervisory bodies and regulators • Incentivise good corporate governance and a culture of compliance • Create voluntary disclosure, reporting and whistle-blowing facilities • Consider introduction of mandatory disclosure rules to require intermediaries to report on possible schemes early in the life cycle
Co-operation	<ul style="list-style-type: none"> • Use domestic whole of government mechanisms, such as reporting of suspicions, information sharing, cross-agency investigations, and other proactive co-operation mechanisms; • Use international co-operation mechanisms, including the broadest range of exchange of information (including on request and automatic, group requests, spontaneous exchange, and on-sharing with other agencies), as well as multilateral co-operation mechanisms.
Implementation	<ul style="list-style-type: none"> • Secure commitment from senior leadership in policy and law enforcement agencies to address and tackle professional enablers, contribute to the strategy, and implement the relevant aspects of the strategy; • Appoint a national focal point who will liaise among different government agencies and assess the needs, challenges and strengths of each government agency in regards to tackling professional enablers; • Engage in open discussions across government, businesses, the public, academia and professional associations to draw on experiences and opinions from all sectors; • Ensure appropriate resources are provided for effective implementation of the professional enabler strategy.

1 The role of professional enablers in tax and other financial crimes

1.1. Who are professional enablers

In general, professional enablers of tax crime and other financial crimes are intermediaries with specialised knowledge who play a specific role to facilitate the commission of a tax offence (and possibly other related financial crimes) by others. Professional enablers of tax crime and other financial crimes can include for example: tax professionals, lawyers and legal advisors, accountants, financial advisors, banks and financial institutions, company formation agents, registered agents, notaries, business trustees, trust and corporate service providers, and other promoters of tax evasion schemes.

1. Law-abiding professionals performing their duties in accordance with the law are an important part of the legal and financial system, and help ensure compliance with the law. Professional enablers are a distinct segment of professionals that intentionally and actively devise strategies to facilitate the commission of crimes (whether serving both legitimate clients and those engaging in tax crimes or other financial crimes). This report focuses on professional enablers who serve criminal clients whether on a fulltime or part-time basis.

2. A professional enabler is typically an individual or entity with professional expertise to perform a specific service to aid their customer in carrying out a tax offence or other financial crime.¹ Most countries do not have a specific definition of a “professional enabler”. However, the common attributes of a professional enabler include:

- Professional qualifications or training;
- Expertise in taxation, legal or financial processes;
- Experience in setting up tax structures, or structures with cross-border elements; and
- Experience setting up opaque structures for avoiding investigative scrutiny into the clients’ tax and economic activities.

3. For some countries, the concept of a professional enabler can be narrow and focus on the most proactive, intentional conduct; while others take a broader view and include those that know or have reason to know that their services are being misused. For example, there can be distinctions between:

- General enablers of tax offences through the provision of services such as those outlined in section 1.2;
- Promoters of tax evasion that actively design and market tax evasion schemes;

¹ An example of both individuals and financial institutions being prosecuted as professional enablers can be found at Box 16.

- Facilitators and service providers that implement aspects of the tax evasion scheme, but who may have a different level of knowledge or expertise and whose involvement is only one part of the bigger picture.

Depending on the country, these distinctions can lead to separate tax offences, different amounts of penalties, the use of civil (non-criminal) sanctions, or the criminalisation of certain higher-level aggravated offences but not others.

4. Professionals offer various legitimate business services to clients such as legal and accounting advice. They may also be experts on finding legal loopholes giving room for the creation of “tax-avoidance” strategies. These strategies operate in the so-called “grey areas of the law”, allowing professionals to use the inadequacies or ambiguities of a jurisdiction’s legal framework to maximise the tax outcomes for their client. The possibility of using “grey areas of the law”, while not technically illegal, should be limited by jurisdictions through the enhancement of their tax legislation and by fostering international co-operation. This is an area in which the OECD has been active over the years through the OECD/G20 Inclusive Framework on BEPS (OECD, 2020^[2]),² and is not the focus of this report.

5. Rather, this report focusses on the situations when the services and advice provided by professionals go beyond the interpretation and search for legal loopholes, and reach the point where professionals enable the commission of tax fraud and tax evasion through active support and participation. The difference between legitimate legal counsel or professional advice, and participation in the commission of a crime, resides in the type of advice offered by the professional and whether illegal activities derive from it.

6. This report assumes a wide definition of such professional enablers, who have the hallmarks of being trained professionally or having specific expertise within key professions. Professional enablers are skilled professionals who use their knowledge for facilitating the commission of tax and economic crimes, usually in large scale and through sophisticated means. This wide definition of professional enablers allows authorities to develop a strategy that is comprehensive, both focussing on professional enablers of tax crime that are actively enabling the commission of tax offences, whilst also recognising that facilitators of tax crimes who are less cognisant of their complicity remain an issue (either by being wilfully blind or where they would reasonably be expected to know of the risks they pose).

1.2. Services provided by professional enablers

Professional enablers can offer a number of services, many of which are legitimate business services. However, these legitimate services can be used to facilitate the commission of tax crimes and other financial crimes.

7. The following examples illustrate the most common or problematic services provided by professional enablers as identified by the TFTC. The mere provision of these services is not an indication that the service provider is a professional enabler and several of these services themselves are not only legal, but essential parts of the global financial system. However, where it is combined with an intent that the service be a part of a scheme for committing a tax crime, or where the service provider is wilfully blind or would reasonably be expected to know that their services were being sought for this purpose, they may be a professional enabler.

² The OECD/G20 Inclusive Framework on BEPS has over 135 countries committed to tackling tax avoidance, improving the coherence of international tax rules and ensuring a more transparent tax environment.

8. While the types of illegal services provided by professional enablers vary in each jurisdiction, common trends emerge from comparative experience. Some examples include:

- Hiding income or disguising the character and source of profits, for the purpose of tax evasion;
- Obscuring beneficial ownership of assets, often through complex legal structures involving several jurisdictions, with the purpose of avoiding investigative scrutiny;
- Offering advice on how to evade tax obligations using falsified transactions, documents or filings.

9. The following sections outline different types of services identified by countries as common services provided by professional enablers. Many of these activities may not only facilitate tax crime, but also other financial crimes such as money laundering, necessitating multi-disciplinary approaches as discussed in chapter 5 below.

1.2.1. Setting up companies, trusts and other business structures

10. Most countries contributing to this report highlighted the prevalence of the companies, trusts and other corporate entities and arrangements in tax fraud and financial crime cases. Corporate structures are attractive to criminals for two main reasons: because they provide an air of legitimacy (IMF, 2019^[3]); and, because they are separate from the individuals behind the corporate veil, they provide the ability to shield the identity of the beneficial owner, as discussed below (Halter et al., 2011^[4]). For example, criminal funds can be disguised within legitimate business transactions by merging legal and illegal profits, which can be transferred either to other business entities or to domestic or foreign bank accounts. As such, professional services for the formation of such entities and arrangements, while itself an important and legal activity, can also be an area of interest for investigators where such vehicles are then used for illegal activities.

11. Use of business structures for illegal purposes is facilitated by an environment where quick, low-cost and easy incorporation is available. While the speed of incorporation is often designed to reduce the compliance burden on legitimate business owners and to encourage national economic growth, this can also create vulnerabilities to abuse by criminals. Easy availability or formation of new companies negates the need for criminals to infiltrate established businesses. In many cases, fraudsters make use of corporate structures spanning multiple jurisdictions in order to hinder investigations and to best present a legitimate front. For example, an onshore jurisdiction can be used when setting up the “front” company, whereas accounts and assets are then located in offshore jurisdictions. Furthermore, the choice of the type of legal entity can be deliberate, in order to exploit legal arrangements where the separation of legal ownership and beneficial ownership of assets is designed to pose an impediment to investigators identifying, or recovering assets from, the owner.

12. Several countries cited this as an area where they have specific projects looking into the use of company formation agents or trust and corporate service providers, due to the prevalence of these professional enablers in establishing the corporate structures used for tax evasion schemes or hiding beneficial ownership and income. Such professional enablers’ services can include for example:

- Assisting in the opening of shell companies by registering in the name of other legal persons, or assisting in the opening of bank accounts in names that obscure the ownership, both domestic and foreign;
- Safe custody of incriminating data;
- Managing or assisting in investing unaccounted funds which are the proceeds of crime in overseas jurisdictions;
- Referral services to other counterpart service providers, e.g. in an offshore jurisdiction, in order to create a cross-border structure which makes detection by law enforcement authorities more difficult.

Box 1. Foreign trusts used in ownership chains to hide beneficial ownership and financial flows

This example is provided by New Zealand

In the wake of certain revelations in the Panama Papers, New Zealand became aware of the possible misuse of New Zealand trusts by trust and company service providers. This misuse was centred on shielding the beneficial ownership of the ultimate controllers, whilst trading off New Zealand's good reputation internationally as a robustly regulated jurisdiction. Thus, New Zealand trusts were being interposed as a further layer in international chains of ownership to make it more difficult for authorities to readily trace both ultimate beneficial ownership and financial flows, and this activity was enabled by trust and company service providers through the establishment and administration of foreign trusts.

Once this information came to light, the New Zealand government moved quickly to strengthen the disclosure rules for foreign trusts. New rules were introduced to require foreign trusts (i.e. trusts settled by non-residents) to be registered with Inland Revenue, including full particulars of settlors, trustees, beneficiaries or persons with power in relation to the trust or trustee. Trust deeds and supporting or amending documentation must also be provided on registration. There is an ongoing obligation to provide full details of settlements on the trust to Inland Revenue, along with annual disclosures to maintain registration as a foreign trust.

The information collected under these new rules is stored in a register maintained by Inland Revenue. This information can be shared with the Police Financial Intelligence Unit, as well as the Department of Internal Affairs, which supervises trust and company service providers for anti-money laundering purposes. Relevant details of foreign trusts are also provided to New Zealand's tax treaty partners on request under exchange of information instruments.

The introduction of these strengthened disclosure requirements for foreign trusts was designed to provide the transparency necessary to deter misuse of foreign trusts, particularly by those trust and company service providers relying on light disclosure to be effective. These predictions have proven to be correct with a major reduction in the number of foreign trusts now administered in New Zealand – a full 75% decline in the number of foreign trusts from 11 671 (as at 31 May 2016) to 2 965 (as at 31 May 2019).

1.2.2. Setting up offshore structures to hide beneficial ownership and income

13. Professional enablers are commonly cited as a concern in connection with their involvement in the establishment of offshore structures. In particular, offshore structures can be utilised to hide beneficial ownership or income / assets. Offshore structures to obscure the beneficial ownership can be used, for example, to conceal the proceeds of crime (such as income on which tax is evaded, or a bribe), or to attempt to evade tax reporting obligations (such as under the Standard for Automatic Exchange of Financial Account Information in Tax Matters (AEOI Standard)). Where a number of corporate entities or arrangements are interposed in different jurisdictions, such as a string of shell companies with complex ownership and control structures, it makes it more difficult for investigators to quickly and accurately identify the person who owns the assets and, if that person is a criminal offender, to recover those assets.

14. Countries have also cited that professional enablers specifically facilitate the creation of instruments that can be used to obscure beneficial ownership such as bearer shares and nominee directors or shareholders. In these cases, the professional involved is key to enabling the creation of these instruments to be used to conceal the identity of those involved in tax or other financial crimes. An example of this can be where “dummy” directors, trustees, shareholders etc. are provided by the professional enabler to disguise their client's beneficial ownership. The simplest use of a nominee carries the risk of

significantly obscuring the beneficial ownership of the entity or assets. This is because nominee arrangements are often private agreements between individuals, and the existence of the arrangement may not be apparent to an investigator. Furthermore, a nominee can itself be a company, which adds a further layer of opacity and complexity for investigators seeking to identify the persons with the ultimate ownership and control. Use of nominee directorships can therefore be viewed as a risk indicator for criminal activity and professional enablers.

Box 2. Dividend structure to obscure beneficial ownership and investment income offshore

This example is provided by the Netherlands

A Dutch taxpayer engages in an aggressive tax planning structure. The taxpayer sells his sole proprietorship of a closely held business to an alleged third party. This third party is often a Dutch legal entity whose shares are held by an entity established in an offshore jurisdiction, which is actually managed by the Dutch taxpayer through nominee directors. Payments are made from the offshore entity to the ultimate beneficial owner; however, the payments are disguised as gifts or loans with favourable loan conditions instead of a dividend payment that would normally have taxation implications. This entire scheme is perpetrated by the Dutch taxpayer to deliberately conceal and evade taxes on taxable dividend payments.

As the amounts are transferred to a foreign bank account of the ultimate beneficial owner and the foreign bank account is not declared in the Dutch taxpayer's income tax return, the Dutch tax authorities are not able to detect the tax evasion unless they receive intelligence on the tax evasion scheme, such as information on the Dutch taxpayer's foreign bank account received through the Automatic Exchange of Financial Account Information in Tax Matters.

Box 3. Professional enablers setting up offshore structures targeted in a sting operation

This example is provided by the United States of America (DOJ, 2014^[5])*

Company A, a boutique investment company based in an offshore jurisdiction, was involved with money management and investment strategies for high net worth individuals. Government officials received information suggesting the investment firm was recruiting United States citizens to invest offshore. It was unknown whether Company A was instructing the US citizens to report the offshore accounts to the government, as legally required.

Undercover agents contacted Company A's investment advisors and communicated they were interested in investing offshore, and wished to meet in person to discuss some of the "sensitive" money they controlled. The undercover agents told the investment advisors that they had orchestrated a bank fraud scheme and therefore had USD 2 million they needed to move offshore to avoid a bank's "lookback period audit" and evade detection from law enforcement officials.

The investment advisors said they typically did not take US clients, but encouraged the officials to meet with an attorney in another offshore jurisdiction to create an offshore foundation. Therefore, it would be the offshore foundation that would become their client and not the US citizens, and the offshore foundation would serve as an entity to conceal true beneficial ownership.

These undercover agents travelled to this other offshore jurisdiction and paid USD 5 000 to create an offshore entity. Subsequently, funds were transferred from the United States to the first offshore

jurisdiction where the funds were commingled with other corporate accounts, before being transferred to the second offshore jurisdiction under the management of Company A. Throughout this operation, Company A's investment advisors were fully aware of their role in managing funds that were untaxed and proceeds of a purported bank fraud.

After a few months, the officials contacted the investment advisors to say they were interested in liquidating their account. The funds were diverted through their offshore entity and returned to their home country, committing money-laundering offences as the investment advisors knowingly invested "dirty money" and used a shell corporation to conceal the true origin and ownership of the funds.

When arrests were made, those arrested co-operated with government officials. The subjects were sentenced to federal prison and spin-off investigations were developed based on the intelligence provided by the professional enablers. Observations and learnings include that targeting the promoters of fraud is much more beneficial and leads to more wide reaching investigatory outcomes than targeting individual investors moving money overseas.

* Note: This example is provided through publicly available information sources.

Box 4. Use of offshore service provider for the purpose of concealing financial flows

This example is based on fact patterns provided by Sweden and the United Kingdom

An offshore service provider was observed providing package services to its clients, which included anonymous offshore-prepaid cards and offshore structures, associated with offshore bank accounts. These services were all advertised online. The clients were encouraged to use encrypted email domain to communicate with the offshore service provider to ensure secrecy. The clients were able to use various methods to add credit to their offshore-prepaid cards including sending cash via a money service business and routing funds through various correspondent banks before reaching the offshore service provider's account. The offshore service provider held bank accounts with several different banks, which were frequently changed to avoid detection by law enforcement authorities.

1.2.3. Providing false documentation

15. Many countries reported that professional enablers provide false documentation as a key service to clients. Their professional knowledge is used to either produce false documents that appear genuine, or fraudulently alter genuine documents, which allows their clients to commit tax evasion supported by false or altered information. Whilst many legal and regulatory obligations such as requirements to provide annual tax returns, statutory accounts, or underlying source documentation for transactions for incorporated companies would normally act as barriers to the ability to commit tax crimes and other financial crimes, countries identified that professional enablers were providing false paperwork to either allow their clients to evade their tax responsibilities, or to provide organised criminals with an image of legitimacy and to dupe investors, suppliers, customers and investigators.

16. Another difficulty identified by several countries is that sometimes not all parties involved will be aware of or acting in concert with the professional enabler that has falsified or manipulated documents. This puts bona fide third party purchasers at risk of being deceived or defrauded. It is therefore all the more important to have sanction regimes targeting the professional enabler specifically.

Box 5. Falsified documents to evade taxation on income

A tax adviser sets up structures for a high net worth individual, Ms X, to help her evade paying taxes on her income. The tax adviser is known for marketing a specific tax evasion scheme, whereby he advises clients to emigrate from their home country to a foreign jurisdiction, but to deliberately stay shorter than the minimum amount of days required for them to establish tax residency in the foreign jurisdiction. The tax adviser then files an income tax return on Ms X's behalf in her home country, with falsified information and documents apparently showing that Ms X has emigrated and has no further personal connection with her home country. This creates the fiction of Ms X being a tax nomad who is then not taxed on her worldwide income either in her home country or in the foreign jurisdiction. In reality, Ms X continues her usual residence in her home country, and is able to evade taxes on her income through a legal fiction created by her tax adviser and his forging of documents for the tax authorities.

Box 6. Falsified documents to obtain an unjustified tax refund

This example is provided by the United States of America (IRS, 2020^[6])*

Federal income tax returns are due to the Internal Revenue Service (IRS) annually. Many US citizens choose to pay an accountant or tax return preparer to prepare and file their federal income tax returns instead of preparing their tax returns themselves. The IRS authorises accountants and federal tax return preparers to enrol and become an authorised e-file provider. Unfortunately, a very small percentage of tax return preparers utilise their expertise for perpetrating fraud instead of assisting US citizens with legitimately preparing and filing their federal income tax returns.

In this example, the tax return preparer, unbeknownst to their clients, reported fake business losses and charitable contributions on their clients' federal income tax returns. The false information (manufactured business losses and charitable contributions) resulted in lowering a person's taxable income and thus increasing their federal tax refund. The clients of the return preparer became loyal customers because their federal tax refunds were generally higher than if they went to another return preparer.

The fraudulent information reported on the tax returns, for all clients over three filing periods, resulted in a tax due and owing for criminal purposes that exceeded USD 1 million. The tax return preparer was sentenced to 37 months in prison and will not be permitted to operate a tax business.

* Note: This example is provided through publicly available information sources.

1.2.4. Assisting in insolvency, bankruptcy and liquidation

17. Insolvency provides an opportunity for individuals who, assisted by professional enablers, can abuse the system to evade investigation and payment of tax and other debts. Insolvency related fraud occurs when a company is trading fraudulently and often takes place prior to the anticipated insolvency of the company. Although bankruptcy applies to the financial status of an individual, the victims are often the businesses that have provided the individual with credit, and the tax authority that is owed taxes.

18. "Phoenix company fraud" or "phoenixing" occurs when the assets of a failing company are transferred to a new company (the phoenix company). The failed company is then wound up, leaving a

trail of debts and out-of-pocket creditors, including tax authorities, behind it. The new company is often the same or similar to the former one but is able to trade with a clean record.

19. It is legal to form a new company from the remains of a failed company, but fraud happens when directors abuse the phoenix company arrangement by transferring the assets of the failing company below their market value, usually to another company beneficially owned by them or a related party, before insolvency. By doing this, the directors fraudulently reduce the funds available to creditors when the original company becomes insolvent.

20. Professional enablers may step in to create a company nominally controlled by a third party (which may or may not be fictitious), facilitating the creation of a beneficial ownership structure through which the controllers of failing companies can channel assets before liquidation. As a result, the creditors are left out of pocket, including the tax administration, which is a creditor for the outstanding tax liabilities. Some countries have legal provisions that allow liquidators or creditors to take action against those individuals personally who try to shelter behind the corporate veil of the company.

21. Below is an anonymised case of convicted phoenixing fraud.

Box 7. Phoenix company fraud

Mr X and his accomplice Mr Y ran a pre-appointment insolvency business. Mr Y created a fictitious identity – known as Mr Z – and provided those details to Mr X who used the fictitious Mr Z to:

- Lodge false and misleading documents appointing Mr Z as a company director;
- Replace a real person acting in the role of director with the fictitious identity, and backdating the director appointment by 18 months, and
- Create other false corporate records using the fictitious identity including taxation and employment records.

Mr X used the fictitious identity to facilitate deeds of company arrangement for debts owed by three companies in external administration. By creating the fictitious Mr Z, the professional enablers Mr X and Mr Y were able to claim that the new phoenix company was in Mr Z's control, even though it was effectively in the beneficial ownership of the failing companies' owners. This arrangement allowed the professional enablers to wrongfully strip assets from the failing companies to the fictitious Mr Z's company, before the failing companies were liquidated.

Mr Y and Mr X had previously provided pre-appointment insolvency advice to the directors of these companies and four other companies. The investigation was launched after a report of misconduct was received from an external liquidator of one of the failing companies.

1.2.5. Enabling tax fraud through cum-ex arrangements

22. An example illustrating the differences between legal and illegal practices carried out by professional enablers is the so-called “Cum-ex Files Scandal”, which came to prominence in the mid-2010s. Tax advisors and lawyers have employed for decades a “tax-optimisation” strategy known as “dividend stripping”, or “cum-cum”, which consists of transferring stocks to a foreign entity to avoid paying dividend tax, and then re-selling them to the original owner. Dividend stripping is in the “grey area of the law”; moving stocks to a jurisdiction where dividends are not taxed right before the day when dividends are paid is not illegal in many countries.

23. When dividend stripping was prohibited in Germany, professional enablers devised a new strategy, known as “cum-ex”. Cum-ex was an illegal tax fraud scheme that involved a sophisticated patchwork of

intermediaries and corporations that exchanged stocks multiple times for a very short period of time around dividend payment day. A stock is exchanged so many times and so quickly, that revenue agencies can no longer tell which owner paid taxes on the stock and which one did not, and ends up refunding taxes it never collected. The professional enablers devised this fraudulent tax scheme and actively marketed it to sophisticated clients, including several major banks, and implemented it knowing that it was a criminal offence under the laws of several jurisdictions. Cum-ex behaviour constitutes tax fraud in most jurisdictions, and as such is an illegal activity in which the professionals who enabled it have criminal liability. Therefore, these professional enablers deliberately avoided deploying the scheme in countries where they knew they would most likely be prosecuted.

24. While dividend stripping is not illegal under the laws of many European Union member states, it is a harmful practice that has cost EU member states over EUR 55 billion in unpaid taxes over the past 15 years, most notably Austria, Belgium, Denmark and Germany. The cum-ex fraud scheme cost the German government at least EUR 7.2 billion in lost revenue between 2005 and 2012.

25. The following is an example of dividend stripping and the fraudulent “cum-ex” tax arrangement.

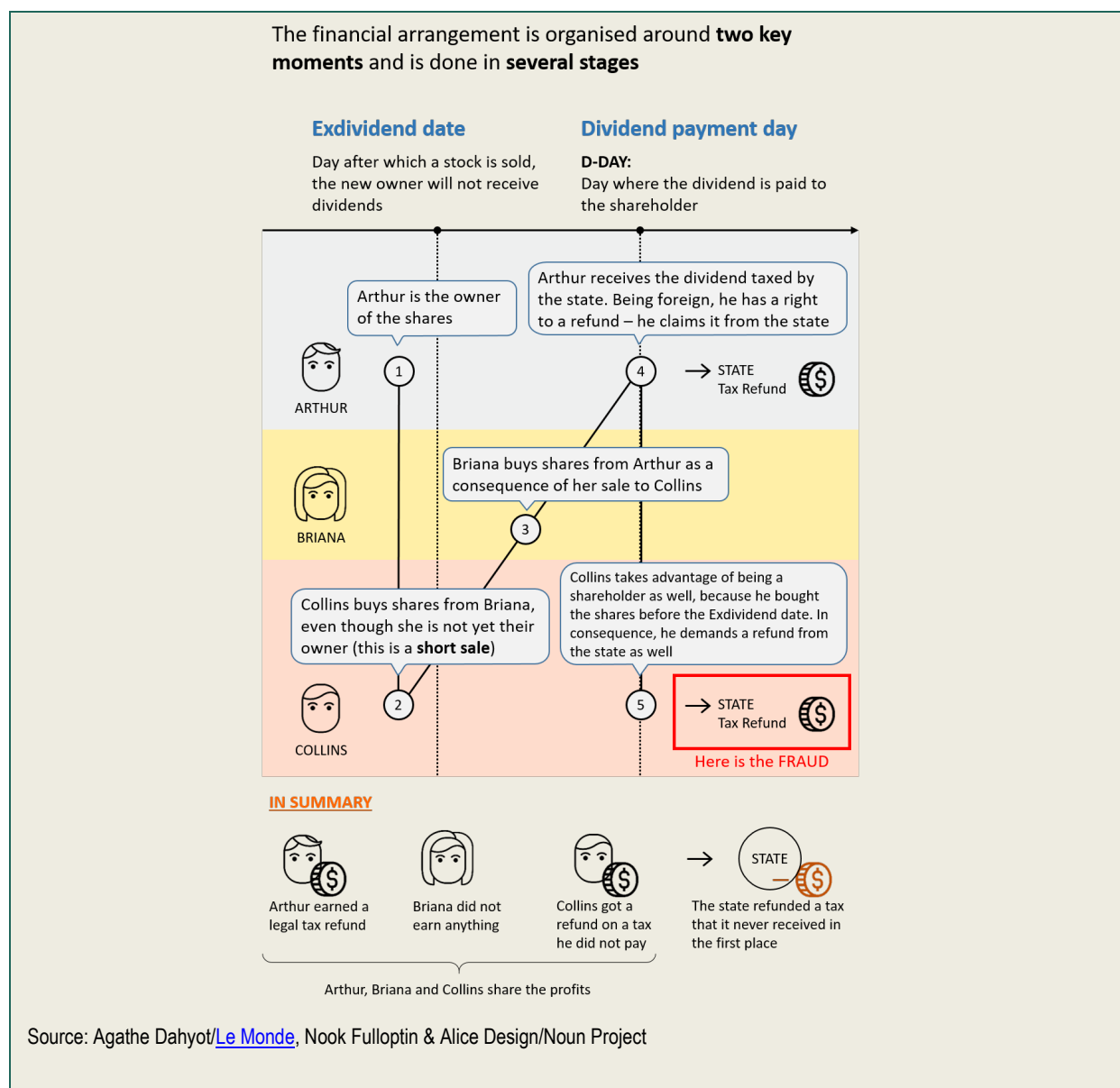
Box 8. Dividend stripping and “cum-ex” arrangements

Dividend stripping

Before dividends are paid, Andrew, shareholder of a French company resident in the United States, transfers his stocks to Boris, another shareholder based in Dubai. On the dividend payment date, the dividends are paid to Boris in Dubai. In accordance with the convention between France and the United Arab Emirates, dividends paid to Boris are not taxed. After the dividend payment date, Boris returns his shares to Andrew, together with the dividends earned. Thanks to this “dividend stripping” strategy, Andrew manages to avoid paying tax on his dividends.

Cum-ex

The illegal cum-ex scheme is more sophisticated than traditional dividend stripping strategies, as shown in the diagram below. In the diagram, the professional enablers Arthur, Briana and Collins work together, and will share the gains from this fraud.



1.2.6. Enabling financial crime through crypto-assets

26. Virtual assets are a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes (FATF, 2012-2019^[7]). This definition encompasses virtual assets that are both convertible and non-convertible to fiat currency (FATF, 2014, p. 4^[8]). For the purposes of this report, the term “crypto-asset” refers to virtual assets in the form of tokens that are convertible to fiat currencies such as the US dollar or the euro (for example Bitcoin, Ethereum, Litecoin, etc.). The term “wallet” refers to crypto-asset accounts that can be used to store crypto-assets either online or offline. Furthermore, virtual asset service providers refers to natural or legal persons, who provide services, such as the exchange, transfer, safekeeping, or other participation in the provision of financial services (FATF, 2012-2019, p. 127^[7]).

27. The risks posed by crypto-assets in enabling financial crime have been highlighted by the FATF since 2014 (FATF, 2014^[8]) (2019^[9]). However, the role of professional enablers in crypto-asset enabled financial criminality is not currently well documented and continues to evolve. It is possible that skilled

professional enablers, who engage in traditional models of financial criminality, may also utilise crypto-assets as part of their criminal schemes. As noted in the OECD's *Money Laundering and Terrorist Financing Awareness Handbook for Tax Examiners and Tax Auditors*, crypto-asset traders who agree to exchange crypto-assets face-to-face for fiat currency may play an important role in money laundering operations, with the potential to act as professional enablers (OECD, 2019^[10]). The fact that crypto-assets are a type of tokenised virtual asset that often has lower levels of regulation and visibility by authorities than fiat currencies, which can allow for a higher degree of anonymity in transactions and obfuscation of financial flows, are all factors that make crypto-assets attractive to tax evaders and other criminals.

28. Professional enablers in the crypto-asset environment may also include operators of black marketplaces on the dark-web (e.g. the now-defunct Silk Road). These marketplaces enable criminals to buy and sell contraband, such as stolen goods, drugs, child pornography, weapons or other illegal items and services. Because the operation of these marketplaces requires a very high degree of technical expertise, the operators of these services can be characterised as professional enablers of criminal activities including, but not limited to, financial crime. The use of these marketplaces also necessitates technical expertise on the side of its customers to be able to access the marketplace on the dark-web with anonymity, which professional enablers may also facilitate. This means that professional enablers can also serve as intermediaries between the operators of the marketplace, sellers of illegal goods and services and the end customer who transacts through it. Dark-web marketplaces utilise crypto-assets as the primary payment method for their transactions in order to exploit enhanced anonymity and the ability to facilitate transactions that circumvent safeguards within the traditional regulated financial system.

29. Most crypto-assets based on a public blockchain (such as Bitcoin) operate with a high level of token flow transparency. All transactions are made available to the public through blockchain explorer services, allowing anyone to “follow the tokens” and audit any transactions occurring on the public blockchain. This means that when e.g. Bitcoins are stolen from an exchange, they become “tainted”, because other users can track the origin of the proceeds. As a result, in order to conceal the tainted nature and traceability of the Bitcoins, stolen crypto-assets must first be laundered, before they can be withdrawn from the system (converted to other crypto-assets or to fiat currency).

30. Professional enablers may facilitate the laundering of proceeds of crime through the use of a crypto-asset mixing service (CMS).³ A CMS is a paid service that has the potential to allow criminal actors to mix their criminally derived crypto-assets with legitimate crypto-assets of other users, in order to obscure the token trail and attempt to launder “tainted” crypto-assets through anonymisation.⁴ After pooling the assets together, the CMS sends them back to its users, usually into newly-created wallets. This would allow criminals to obtain untainted crypto-assets in fresh wallets, making it extremely difficult to uncover their criminal origin. It is worth noting that there is no limit on the number of wallets a crypto-asset user can create. Furthermore, unlike with creating a user account on most crypto-asset exchanges, there are no customer due diligence requirements for a new wallet to enter the blockchain. Therefore, criminal actors can create and use thousands of wallets in order to obscure their transactions and activity on public blockchains.

31. A CMS can therefore make it easier for users to conduct criminal activity on the dark-web, as well as to launder proceeds stolen during for example a crypto-asset exchange attack. In this case, the professional enablers may be the companies that intentionally operate this service using their proprietary algorithms to facilitate money laundering, or other facilitators who manage the process of anonymising criminally derived assets through a CMS. As this is an emerging technology that may pose risks of financial crime and be a new avenue of activity by professional enablers, it is an area for countries to continue to

³ These services are also known as crypto-asset tumblers, blenders or Bitcoin mixers.

⁴ A “tainted” crypto-asset refers to tokens that can be linked to a specific transaction that indicates a crime (e.g. theft of crypto-assets from an exchange).

consider in terms of risk, supervision, and regulation. In recognition of the risk of financial crimes posed by virtual assets and virtual asset service providers, the FATF has revised its standards to recommend that countries should ensure that virtual asset service providers operating in their jurisdiction are able to manage and mitigate the risks of engaging in activities that involve the use of anonymity-enhancing technologies (FATF, 2019, p. 28^[9]). A CMS is typically a virtual asset service provider within purview of the FATF standards, as they facilitate exchanges and transfers of virtual assets.

Box 9. Crypto-asset mixing service (CMS) case – Bestmixer.io seizure

Bestmixer.io was launched in 2018 and soon became one of the top three largest crypto-asset mixing services. By 2019, the company achieved a turnover of approximately 27 000 Bitcoins, worth roughly USD 200 million.

Since June 2018, the Dutch Fiscal Intelligence and Investigation Service (FIOD) has collaborated with the internet security company McAfee to investigate the service and determine whether it is laundering criminal proceeds.

The investigation has shown that many of the mixed crypto-assets on Bestmixer.io had a criminal origin or destination, meaning that the service was probably used to conceal and launder criminal proceeds. On May 22, 2019, six servers of Bestmixer.io were seized by the FIOD, EUROPOL and Luxembourg authorities. FIOD gathered information on all the interactions on the platform between 2018-2019, including IP addresses, transaction details, Bitcoin addresses and chat messages. This information is currently being analysed, in collaboration with EUROPOL.

On February 17, 2020, FIOD arrested a 31 year old man, suspected of laundering over EUR 100 000 with two accomplices. The arrest was made in connection with the investigation into Bestmixer.io. The suspect was discovered through his IP address, which was linked to a Bitcoin wallet that used the CMS to launder criminal proceeds. FIOD stated that more arrests are possible in connection with its investigation into Bestmixer.io.

As of 2020, there are numerous CMS operating in the crypto-asset environment, posing significant risk of money laundering using crypto-assets.

2 Identifying professional enablers

To be able to address the threats and risks posed by professional enablers, processes need to be in place to identify and capture relevant information about them.

2.1. Organisational awareness of professional enablers

32. Professional enablers are likely to be encountered across a number of different functions involved in a tax authority's compliance activity, from those business areas involved in promoting voluntary compliance, to those undertaking audits or investigations, through to those leading on enforcement activity such as civil penalties and criminal prosecution. If staff across the tax authority are not aware of what a professional enabler is, then it is likely that professional enabler threats may be missed.

33. Establishing and raising staff awareness is therefore crucial to improving the overall understanding of the threats and risks posed by professional enablers. In the United Kingdom for example, electronic learning packages have been created for tax authority staff to explain what is meant by the term 'professional enablers' and what to do if they identify one. Another approach is to designate a lead official in each organisation who is responsible for the issue of professional enablers. This person can serve as a key contact point for staff members to raise questions and share feedback on cases involving professional enablers. This person could also have responsibility for raising awareness in the organisation through briefings, meetings and training sessions, and serve as a member of a broader national team responsible for implementing the professional enabler strategy.

2.2. Measuring the threat of professional enablers

34. Once a country has defined the parameters of its professional enabler definition, it can consider how to identify, record and measure professional enabler activity. Measuring the threats and risks posed by professional enablers is important, as understanding the size and nature of the problem will then help to determine the best approach to addressing it.

35. Not all countries have taken the same approach to tackling professional enabler issues. Some countries have chosen to focus resources on specific types of professional enablers or professional enablers in higher risk sectors, with multiple and concurrent strategies depending on the area of focus. Therefore, the appropriate measure will depend on the scope and objectives of a country's professional enabler strategy.

36. Measuring the size and nature of the professional enabler issue will involve identifying all the potential data sources, which may contain references to enablers or their clients, and then developing methods for detecting the risks that they pose. This may involve identifying indicators within existing data such as suspicious patterns of behaviour in a sector that may indicate enabling of tax crime, or creating new indicators such as the capture of internal management information to show when a professional enabler is being investigated. For example, in the United Kingdom, internal information management systems now allow staff members involved in open investigations to indicate if a professional enabler is

suspected of involvement in a case or not. This information is collected and recorded in one place, which allows the authorities to have a single overview of enabler cases. The type of measures and indicators for each country will naturally depend on the type of data available, and may require multiple strategies for different risk areas. Creating this baseline of understanding is important, as it will provide the foundation for measuring the success of any subsequent strategy for tackling professional enablers.

2.3. Detection through development and analysis of professional enabler indicators

37. Use of data and intelligence is an essential tool to help identify specific professional enablers, as well as the broader pattern of schemes and structures they use. However, because professional enablers are a sub-set of professionals, operating in a range of transactions that may be overseen by different regulatory or investigative bodies (e.g. professional regulatory bodies, financial regulators, financial intelligence units, and tax administration), intelligence is often held in different databases and systems both within and across organisations. This makes it difficult to identify trends and patterns or even repeat offenders. Improved risk analysis of individual professional enablers is one way in which to grow the pipeline of investigations and interventions, and build up effective coordinated disruption and deterrence efforts.

38. Many countries have dedicated teams focused on compliance work specifically relating to a known problem area, such as targeting enablers that are associated with multiple shell companies or that market the use of offshore structures. For example, many countries have collected information on professional enablers connected to offshore service providers or firms for the purpose of utilising it in data analytics and audit strategies. Feedback from countries show that offshore jurisdictions known as “hotspots” of activity for specific evasion structures are often utilised repeatedly by the same professional enablers. Once a particular structure or nefarious service provider is uncovered, this gives tax authorities the ability to target other structures established by the same professional enablers. However, feedback from countries also shows that these hotspots can fluctuate, for example in response to detection or where a new strategy is devised, and therefore national professional enabler strategies need to be flexible to adapt to new information and intelligence received. Box 10 highlights some of the indicators identified from case studies from TFTC countries, which could be used for risk assessment exercises. Box 11 is an anonymised case study of a scoring model system developed to identify professional enablers through specific professional services targeted by Country X.

Box 10. Possible indicators for use in risk assessment exercises for detecting involvement of professional enablers

- A company is not found at the declared premises
- Addresses of entities or directors which are not traceable
- Multiple shell companies from the same address
- Multiple companies with directors in common
- Company’s address registered at a P.O. Box address known for illegitimate businesses
- Professionals with a high turnover of business relating to liquidation of small companies
- Professionals that promote tax schemes on the basis of premium or contingent fees, or contractual protection that guarantees coverage of any financial liabilities resulting from the tax strategy

- Where one individual is attributed as a director multiple times, the extent to which the provision of substantial and meaningful directorship services could not be feasible
- Tax intermediaries with poor tax compliance and filing history
- Persons with association to known professional enablers
- Persons with association to known tax evasion structures
- Persons with association to known offshore structures that obscure beneficial ownership to facilitate fraudulent behaviour

Box 11. Scoring model to identify professional enablers in Country X

The country providing this case study has requested to remain anonymous

Country X does not have a defined class of professional enablers that it targets in its strategy. Instead, Country X's methodology utilises a scoring model to find professional enablers who offer tax evasion products with a cross-border element aimed at evading taxation in Country X or rendering detection of tax evasion difficult for the authorities (based on an assumption that these professional enablers advertise their products). The methodology uses the tax authority's own internal systems and also internet searches to locate offerings of such professional advisory services with a correlation to Country X. The searches are conducted based on 60+ keywords to detect these specific professional services, with a scoring model that assigns different weighting for countries, behaviour patterns, and trigger words, on a risk basis. This scoring model is therefore able to yield Country X a risk-weighted result of service firms and professional enablers to focus on for investigation.

Subsequent investigations can include analysing money transfer data to and from particular service providers or enablers identified through the above scoring model. This allows Country X's authorities to garner a picture of the type and breadth of clients utilising the enabler's services, and identify patterns and trends. It also informs further investigations on the individual clients, enablers, and firms involved.

2.4. Data sources for identifying professional enabler activity

39. The following methods listed in the box below were highlighted by countries as useful in identifying wrongdoing by professional enablers.

Box 12. Data sources in professional enabler investigations

- Data mining information from offshore leaks, looking for links to professionals active in the jurisdiction, common clients of those professionals, and common structures
- Analysing information from suspicious transaction reports (STRs), including STRs on international electronic funds transfers, to identify repeat transactions, professions or persons that are the subject of the reports
- Creating a reporting mechanism for officials across the tax administration to report suspicions or queries with respect to intermediaries that are involved in suspect structures or transactions
- Information from voluntary disclosure programmes

- Anonymous or whistle blower reports
- Information on the internet advertising tax schemes or offshore structures
- Statistics on companies that have been struck off and cross-matching that information to companies served by the same service provider
- Statistics on disqualified directors and cross-matching that information to those that work for the same service provider
- Creating an internal database of shell companies, suspicious addresses, suspicious directors and persons etc. to query or use for data mining
- Creating a database of known professional enablers and known associates
- Validating the authenticity of documents with relevant government agencies (e.g. passport office, company registrar, financial regulators, other law enforcement authorities etc.)
- Validating the identity of taxpayers through signatures, photos or fingerprints in tax authority or government records
- Consulting the OECD ATP Directory, a confidential database of over 400 aggressive tax planning schemes (OECD, n.d.^[11])

40. An example from India of how data mining was used to find fraudulent taxpayers, directors and other professional enablers is included below.

Box 13. India's use of data sources in professional enabler investigations

In 2017, the government of India set up a special task force dedicated to the identification and eradication of shell companies. Shell companies are recognised as a risk to the tax base due to their usage in the commission of tax crimes and other financial crimes.

As a country with a large population, information in India on individuals, taxpayers, corporations and directors are held in different databases by separate government departments and ministries. Information on individuals is maintained by the Unique Identification Authority using “Aadhaar” numbers, a biometric-based unique identification number for individuals. Information on taxpayers is held by the Income Tax Department through permanent account numbers (PANs), a unique taxpayer identity number that is mandatory for all taxpayers (but not necessarily all individuals). Finally, the Ministry of Corporate Affairs manages the register for corporate entities and directors through the registering of corporate identity numbers (CINs) and director identification numbers (DINs).

One of the key tasks in identifying shell companies was to be able to perform data analytics across the information held by the three different government departments and data-mine between the three databases. The results of this triangulation of information between government departments were dramatic. By linking the information between Aadhaar numbers and PANs, many ghost PAN holders, duplicate PAN holders or fake PANs were identified and removed from the system. Cases of fraudulent non-quoting of PANs were also identified, which was previously a common way for fraudsters to remain undetected by the Income Tax Department, leading to high value transactions being concealed and fraudsters escaping investigation or audit. The crosschecking of information with DINs and CINs also revealed the identify of fraudulent directors and shell companies. This was evident when anomalies were found for companies that had filed financial statements but failed to file an annual tax return, or vice versa, where companies had filed an annual tax return but failed to file financial statements, as required. This resulted in the disqualification of 309 000 directors, and 226 000 companies being struck-off by the Ministry. Furthermore, in the process of this crackdown on fraudulent activity by directors,

fraudulent PANs and companies, approximately 400 professional enablers were identified as responsible.

This straightforward action of combining information and databases that were already in the Indian government's possession, was able to root out thousands of cases of basic fraud and non-compliance by individuals, companies, directors and other professional enablers such as accountants. In particular, the triangulated information also gave the Indian authorities a clearer picture of where wrongdoing was being perpetrated by the same sets of persons repeatedly, which indicated where professional enablers might be involved and further investigation would be warranted.

3

Disrupting professional enablers

Lawyers, tax advisors, notaries and accountants are valued gatekeepers to a sound legal and financial system. Their unique sets of skills, together with the professional privileges awarded to them by statutes, put them in a special place within societies. They are experts who are in a position of trust, and enjoy certain rights that are not shared by other professions. Jurisdictions should ensure that advisors perform their tasks in accordance with the law, and penalise those few who use their skills, expertise and privileges to design structures with the purpose of breaking the law. This requires that countries have in place a legal framework to support criminal investigators and the justice system in addressing and punishing professional enablers that engage in and facilitate the commission of such crimes.

41. For the most grievous offenders, it is important that countries have in place criminal sanctions for professional enablers to penalise them for their wrongdoing. Countries have also reported the use of civil penalties, injunction mechanisms or disbarment through professional supervisory and regulatory bodies as secondary and tertiary methods for authorities to disrupt, deter and penalise offenders, which may be more appropriate in reflecting the different types of involvement of professional enablers. Ensuring that a cascading range of legal sanctions and disruption tools are available to government authorities allows law enforcement agencies to have the flexibility and framework to address the risks posed by professional enablers.

3.1. Legal sanctions for professional enablers

Countries have reported a variety of legal approaches to sanctioning the actions of professional enablers. Jurisdictions should address the issue of criminalising the conduct of professional enablers in accordance with their domestic legal frameworks. In general, countries do not separately criminalise professional enabler behaviour, but address it through provisions criminalising accessories to tax crime, or as an aggravated accessory offence where an enabler is involved in a tax crime. Some countries also have civil penalty regimes that specifically target professional enablers and promoters.

42. Professional enablers represent a distinct type of secondary offenders, whose actions can be criminalised by being defined as the aiding, abetting, facilitating or enabling of a tax offence. Professional enablers can also be treated by some countries as special accessory offenders with regard to tax crimes and other financial crimes, who are liable to a higher penalty than regular aiders or abettors.

43. Some countries have reported that such accessory offence provisions have been well utilised to prosecute the actions of professional enablers in the commission of a tax crime or other financial crimes. In other countries, authorities have experienced difficulties in using accessory criminal offences against enablers due to lack of precedent, high levels of administrative burden to prove the offence, or inability to successfully prosecute the primary offence. Some countries, such as Australia, France, and the United Kingdom, also have significant civil penalty provisions that target professional enablers or promoters of tax

evasion schemes, and an example of the administrative sanctions for facilitators in France can be found in Box 14 below.

Box 14. Administrative sanctions against facilitators in France

Law No. 2018-898, of 23 October 2018, introduced a new tax fine for intermediaries who are facilitators of serious breaches by taxpayers. A new administrative sanction was also introduced; separate from criminal sentencing, which is applicable to persons who, through their services, contribute to the preparation of fraudulent or abusive arrangements.

The law sets the list of services that can be punished, including:

- Allowing the taxpayer to conceal his or her identity by providing a fictitious identity or a nominee or by using a natural or legal person or any foreign-based organisation, trust or comparable institution;
- Allowing the taxpayer to conceal his situation or activity by a fictitious or fictitious act or by the intervention of a fictitious entity;
- Allowing the taxpayer to wrongly benefit from an income deduction, a tax credit, a tax reduction or an exemption from tax by the improper issuance of documents;
- Carrying out on behalf of the taxpayer any action intended to mislead the administration.

The amount of the fine is set at 50% of the income derived from the service provided to the taxpayer, but may not be less than EUR 10 000.

44. Where countries are considering introducing specific criminal law provisions to address professional enablers, key elements to be considered could include:

- Defining professional enablers as accessory offenders to tax and economic crimes in accordance with the technical features of each national legal framework;
- Enactment of legislation that specifically targets and penalises enablers of tax crimes and other financial crimes;
- Extending sanctions beyond imprisonment and fines (e.g. disqualification) and applying different types of sanctions according to the different levels of intent;
- Lifting professional privilege in regards to privileged evidence of professional enablers when being directly investigated for the commission of a tax or economic crime;
- Setting appropriately lengthy statutes of limitations and grounds for its interruption and suspension that acknowledge the time-consuming and complex nature of these types of investigations;
- Ensuring there is a legal basis for co-operation of professional oversight bodies with investigators;
- Ensuring investigative agencies have adequate legal tools for engaging in complex investigations regarding professional enablers (e.g. powers to seize evidence and assets, and to interview witnesses and suspects).

Box 15. Legal reforms in Mexico to tackle professional enablers

Mexico has introduced multiple legal reforms in recent years to combat the increasing prevalence of professional enablers and their vast networks and operations in Mexico.

These legislative reforms included amending federal laws to formally include tax crimes in the catalogue of organised crime offenses, which were specifically intended to encompass and target the activities of

professional enablers. The prosecution of professional enablers under the Organised Crime Law carries a sentence of up to 16 years imprisonment, in addition to any penalties applicable for the prosecution of the underlying tax crime. Furthermore, the legislative powers under the Organised Crime Law allows for the confiscation of assets relating to organised crime offences even where there is not yet a verdict in a criminal trial, as a pre-emptive step to discontinue the activities of the professional enabler and ensure that assets that give rise to or are a product of tax crime are adequately secured.

The reforms expanded the application of the United Nations Convention against Transnational Organized Crime to tax crimes under Mexican national law, allowing Mexican authorities to have further recourse to special investigation techniques such as undercover operations, witness protection measures, and the intervention of private communications, including in cases of crimes facilitated by professional enablers.

Furthermore, the Law of National Security was amended to add certain aggravated tax crimes to the catalogue of acts against national security, for example where falsification of documentation is facilitated by a professional enabler. This legislation allows the Mexican courts to order imprisonment as a preventive measure to those accused of partaking in an aggravated tax crime as a professional enabler, and enhances resources available to the Mexican Fiscal Prosecutor in such cases.

Finally, the Federal Criminal Code has been amended to extend the application of criminal responsibility for the majority of tax crimes to corporate entities as well, to ensure that entities that enable tax crimes are caught within the net of the Criminal Code.

The suite of legislative reforms enacted by Mexico reflect the seriousness of this issue for the Mexican government, and the necessity for authorities to have the appropriate powers enshrined in legislation in order to investigate, prosecute, sanction and deter the activities of professional enablers in their country.

45. It is important that sanctions against professional enablers of tax crimes and other financial crimes have a deterrent effect. One important aspect of deterrence is having in place strong penalties. Penalties should be sufficiently dissuasive, whether monetary fines, confiscation of assets or imprisonment, such that professionals would be deterred in practice from engaging in enabling behaviour.

46. As aforementioned, criminal sanctions should be applied to the most egregious of professional enabler offences, to underscore to the public that those who commit serious tax crimes face serious consequences, in recognition of the harm to society that the actions of such professional enablers cause. For such cases, these professional enablers should be publicly and openly prosecuted to have the appropriate reputational and deterrent effects in society, and promote a strong culture of tax compliance and tax morale. An example of a successful criminal prosecution of professional enablers in France is provided below in Box 16. It will be up to each country to decide on whether criminal prosecution or civil sanctions provide the best approach, and these options should form part of a country's strategy for dealing with professional enablers.

Box 16. Investigation and prosecution of professional enablers in France

In October 2008, a specialised inspection squad of the French tax administration organised a raid at the business premises of a company service provider, suspected of facilitating tax fraud. The search disclosed a vast scheme allowing French clients to avoid paying their taxes and launder money, uncovering evidence for both tax and financial offences. The documents discovered revealed that the French businessperson contacted hundreds of French clients to sell ready-made shell companies incorporated in financial centres or non-European low tax jurisdictions.

The evidence showed that the suspected French businessperson, who once promised “tax haven for all”, had helped tax evasion to become easier and cheaper among ordinary taxpayers and small businesses in France.

The French Office of the Public Prosecutor began a criminal investigation into this matter in July 2011. The investigative results showed that the business was staffed by two French lawyers, a foreign director and nominee shareholder, as well as support staff located in Paris and abroad. The tax evasion schemes utilised foreign banks, which provided private bank accounts and credit cards to the French clients, especially one European bank in the Baltic area. The criminal investigations also identified that the perpetrators organized “large-scale” tax evasion through a network of offshore companies, in connection with offshore company service providers as well. The true beneficial owners of the shell companies were not revealed to the local company registry. Furthermore, the French professional enabler himself evaded tax on his own earnings through the same offshore tax evasion schemes.

In addition to the professional enablers of this fraud, customers that utilised the tax schemes also became the subject of tax proceedings. The French tax administration led tax audits on all the clients identified by the investigations.

The French criminal court sentenced the French organiser of this vast scheme and his accomplices as follows:

- The main perpetrator was found guilty of tax fraud, forgery of documents, fraud, money laundering and criminal association. He received a jail sentence, five years imprisonment with two years probation and a fine of EUR 3 000 000. He was also prohibited to conduct any further business and management consultancy activities.
- One of the French lawyers who assisted in the operations of the schemes was convicted of aggravated money laundering and was sentenced to three years suspended imprisonment and a penalty of EUR 50 000.
- One of the banks involved was found guilty of money laundering and was sentenced to a fine of EUR 80 000 000, and prohibited from conducting business in France for five years.

The coordinated action between the French tax administration, criminal investigation and prosecution services was able to successfully investigate, prosecute and sanction the French professional enabler and his accomplices. This case was openly prosecuted and highly publicised in the media. The criminal sanctions applied were effective to disrupt the illicit activities of the enablers, and underscore to the public that serious penalties apply for professional enablers of tax fraud and money laundering, to both individuals and financial institutions alike.

47. In practice, lower level cases of professional enablers may require different approaches for a number of reasons: there may be administrative reasons such as limited resources available for authorities to prosecute only the most serious of professional enabler crimes, or the nature of involvement by the professional may not warrant a criminal or civil sanction. The following sections therefore look at other methods available to authorities to disrupt the actions of professional enablers.

3.2. Injunctions

Court orders and injunctions against practicing law, accounting or advisory services have been cited as tools that countries can use to disrupt professional enabler’s behaviour. Depending on the country and the profession involved, injunctions can be used to require, or restrain an enabler from, specific behaviour upon

application to the courts, or can be used to remove professional enablers from operating in their area of expertise all together.

48. For example, in the United States, fraudulent tax return preparers and tax-fraud promoters can be addressed through both civil and criminal enforcement tools. A civil injunction program, administered by the United States Department of Justice Tax Division, can bar individuals or businesses from engaging in specified misconduct or from preparing tax returns for others. Any individuals or businesses found in breach of the injunction can have further criminal action taken against them. Furthermore, any fraudulent individuals or businesses that have been shut down by the Department of Justice (DOJ) via an injunction are listed publicly on the DOJ's website ([12]) ([13]). This makes all taxpayers and tax professionals aware of the identity of unscrupulous tax preparers and businesses, makes it clear that professionals who facilitate illegal conduct will be stopped, and acts as a deterrent in the industry to increase tax morale and a positive compliance culture.

3.3. Professional supervision and regulation

Most countries have regulatory and supervisory bodies for AML and CFT purposes, and professional bodies that self-govern their members through a code of conduct or similar set of ethical obligations. This could include for example, a bar association or law society for lawyers, or a chartered accountancy or international ethics and standards board for accountants (IESBA, n.d.[14]). These regulatory and professional bodies may receive reports of misconduct or criminal behaviour on the part of members of the profession, and may have the ability to impose sanctions and suspend or remove licences for businesses to legally trade, or the ability to expel members or firms from membership in the professional association. These bodies should be part of the strategy for addressing the behaviour of professional enablers.

49. A country's strategy and legal framework for professional enablers should therefore include co-operation with and the usage of regulatory and professional bodies or other supervisory bodies to ensure disbarment or disqualification of enablers where there is misconduct, so that these enablers can no longer continue their harmful services.

3.3.1. Supervision and regulation

50. Countries should have a robust supervisory and regulatory framework that puts in place the relevant FATF standards for anti-money laundering and counter-financing of terrorism. In particular, the FATF standards require the regulation and supervision of designated non-financial businesses and professions (DNFBPs) which includes lawyers, notaries, accountants, other independent legal professionals and trust and company service providers. The FATF has also produced guidance to support effective risk based supervision of the sector.⁵ Having in place appropriate regulation and supervision of these sectors is important as it can have a deterrent and awareness-raising effect for enablers, whilst regular supervision will help countries to monitor and enforce the AML and CTF obligations for professionals and understand any ongoing and evolving enabler risks through continued dialogue with each sector. Such regulatory frameworks also allow for easier reporting and detection of suspicious enabler activity.

⁵ See Annex A of this report.

3.3.2. Sanctions through regulatory or professional bodies

51. Supervisory and regulatory bodies may also have the ability to impose sanctions or suspend and remove licences of businesses or professionals that do not meet AML and CTF standards, and can be an additional tool in disrupting professional enablers of tax crime. An example provided by the United Kingdom is the use of supervision requirements under anti-money laundering and counter-terrorism financing rules to remove professionals in money service businesses or trust and company service providers that are not of a “fit and proper” status. This has been a quick and effective way to remove the ability of the business to legally trade, and stop professional enablers in their tracks, to limit criminal activity and further losses to tax revenue. Some countries utilise sector supervisors or professional boards to administer sanctions and regulate offences, as those bodies can hold an individual accountable to civil rather than criminal standards. These investigations can result in business closures and suspension or loss of licenses. While this means the subject will not be incarcerated, it does prevent the professional enabler from continuing to commit crimes by abusing his/her professional licence.

52. Using professional and supervisory boards also allows for greater publicity within a professional enabler’s sector if the enabler’s conduct and punishments are published in the profession’s journal, on their website, or membership list. The following case study from India highlights the new administrative body it has put in place to strengthen the independence of oversight and the ability to execute professional disciplinary action.

Box 17. India’s Task Force on Shell Companies

In 2017, the government of India set up a special task force dedicated to the identification and eradication of shell companies. As outlined in the case study contained in Box 13, India, using available data, was in the process of a crackdown on fraudulent activity by directors and fraudulent companies, whereby approximately 400 professional enablers were identified as responsible.

The list of 400 professional enablers was then shared with the Institute of Chartered Accountants of India (ICAI), for disciplinary action of its members. However, due to conflicts of interest with members of the ICAI, disciplinary proceedings stalled and never proceeded. The ICAI was a previously self-regulating professional accounting body. A new oversight body for the accounting and audit professions was legislatively provided for by parliament in 2013, but was not properly implemented until the recent creation of the National Financial Reporting Authority (NFRA) under the auspices of the 2013 legislation. The NFRA is charged with powers to investigate matters of professional misconduct by chartered accountants or chartered accountancy firms, with the ability to impose penalties, and debar the chartered accountant or firm for up to 10 years. As an independent regulator, the NFRA is now able to properly review the conduct of the professional enablers identified by the Task Force on Shell Companies, and take appropriate disciplinary action or debar accountants found to be guilty of misconduct.

3.3.3. Disqualification of company directors

53. Most countries reported having some form of disqualification process for directors of companies suspected of enabling crime. The process varies in each country, but the government authority responsible for governing corporate entities typically has the power and mechanisms for removal and disqualification of directors. The reasons prescribed for disqualification can differ, but the most common reason for disqualification is where directors fail to act at a time when they should have done so, whether it be filing for insolvency or taking action that will mitigate the losses of their companies, etc. The consequences of disqualification and the time period in which a person is barred from acting as a director vary widely

between jurisdictions. In some jurisdictions,⁶ for serious offences, a disqualified director is barred from acting as a director forever.

54. Some jurisdictions also have public registers that list disqualified directors and are easily accessible. This has been noted as a useful tool for government authorities, as the disqualification of a director in one country does not prevent the same individual from acting as a director in another country. Public registers of disqualified directors, and increased sharing of intelligence among government authorities, allows authorities the ability to identify collectively any directors that are fraudulent professional enablers operating in multiple jurisdictions.

55. Although rules on company directors can vary significantly between jurisdictions, the following are some common safeguards that can be put in place by countries with regard to company directorships:

- Require that the director be resident in the jurisdiction. This can improve access to an accountable person in case of investigations, and also be a significant disruptive factor for criminals seeking to distance themselves from the crime.
- Require that directors pass a “fit and proper” test or equivalent threshold. This could include being subject to credit checks, and requirements to disclose previous directorships, any disqualifications both in the jurisdiction and abroad, any outstanding court judgments or criminal convictions, etc.

⁶ For example Australia, India and the United Kingdom.

4 Deterring professional enablers

Targeting the actions of intermediaries before they become professional enablers can help to swiftly prevent growth of professional enabler risks, and communication and education can be key. Once professional enabler activity is occurring, mechanisms to deter and intercept it are necessary, such as leveraging the role of professional bodies and regulators, as well as creating mechanisms for voluntary or mandatory reporting and whistleblowing. This chapter describes the range of mechanisms countries can consider as part of their disruption strategy.

4.1. Preventing abuse

Professional enablers can be deterred from criminal activity through a number of methods, and an effective prevention strategy is generally more efficient than investigation in many cases. Countries use a range of communication, engagement and education, corporate responsibility and governance approaches to ensure would-be professional enablers are aware of the risk the misuse of their services can entail, and promote a culture of voluntary compliance.

4.1.1. Communication

56. A key prevention strategy is to provide clear and accessible guidance on the operation of the tax and criminal laws. Some countries also have dedicated teams to look at deterrence through communication activities, and develop strategies to create a culture of voluntary compliance. Communication should take place throughout the life cycle of a particular risk posed by professional enablers: before the professional enabler decides to pursue the activity; once a particular scheme is known; and after the successful prosecution of a professional enabler.

Before the professional enabler decides to pursue the activity: pre-emptive action

57. Pre-emptive communication strategies can include clear communication and guidance on the parameters of tax rules and consequences for non-compliance, regular engagement with tax professionals and taxpayers, helpful reminders of filing requirements, etc. These communication strategies can all promote a higher compliance culture and reduce opportunities for “grey areas” to be exploited.

58. Examples of pre-decision communications tools include:

- Online information through government websites: this can include publishing factsheets, guidance, public rulings, media releases, news articles and alerts
- Targeted emails to registered businesses, filtered by sector and location: for example, in the United Kingdom, a “welcome” email is sent to all newly registered businesses with links to relevant web pages and information to promote tax compliant behaviour

- Face-to-face events: regular engagement through presentations or dialogue with businesses, peak industry bodies, intermediaries and tax professionals, etc.
- Webinars: online, live presentations where tax professionals can take part in a live, interactive online workshop to raise greater awareness of their responsibilities and have the opportunity to ask questions. These have proved popular in some countries, especially with businesses in particular sectors where common questions can be addressed, and is a cost effective way to reach a large audience
- Regular podcasts to communicate to tax professionals new messages, concerns, or services provided by the tax authority
- Joint campaigns: working with other government departments and law enforcement agencies to help businesses understand their responsibilities
- YouTube video clips to educate customers and registered businesses including visuals. The aim is to support customers with regard to key services such as income tax or information technology registration to make voluntary compliance easier and more accessible.

Once a particular scheme is known: targeted action

59. Once a specific risk is known, targeted communication tools can also be used, such as communicating requirements under the law to boost compliance in areas with low levels of compliance or in areas of emerging risk. In the following, Box 18 is an example showing the Australian Taxation Office's usage of taxpayer alerts to warn taxpayers and tax advisers of emerging high-risk arrangements that the Australian Taxation Office is concerned about, and Box 19 contains an example from the United Kingdom's Her Majesty's Revenue and Customs approach to encouraging compliance in response to a known risk.

Box 18. The Australian Taxation Office – usage of taxpayer alerts to address new tax schemes

This example is provided by Australia

The Australian Taxation Office (ATO) publishes taxpayer alerts regarding new or emerging high-risk tax schemes. Where intelligence is received by the ATO of a risky arrangement that may not be compliant with the law, the ATO is able to respond with immediacy to warn the community. Through taxpayer alerts, the ATO is able to share with tax practitioners and taxpayers its concerns regarding an arrangement that is legally ineffective, involves exploitation or a deliberate misapplication of the law, or which may constitute tax evasion or tax fraud. Furthermore, the ATO can indicate what the applicable penalties are for taxpayers who use the tax scheme, or enablers who promote usage of the tax scheme.

The ATO's experience shows that the practice of using taxpayer alerts has the effect of preventing uptake of illegal tax schemes and preventing proliferation of a tax scheme's usage by further providers. In general, fewer mass-marketed schemes have been observed in this climate as a result.

Box 19. HMRC’s “Promote and prevent” approach to encouraging compliance

This example is provided by the United Kingdom

HMRC has a number of “promote and prevent” approaches where, in addition to responding to identified risks, it proactively promotes compliance in specific customer groups or business sectors where those risks have occurred, in order to prevent future non-compliance.

- One-too-many approach: one message is sent to a wide audience (individuals and businesses) about a specific issue relevant to their type of business/tax responsibilities.
- Nudge: broad messaging to try to encourage a change in behaviour. This might be a change in the way a form is worded to encourage greater compliance, for example “Please can you do this” versus “You have to do this” versus “If you don’t do this then the consequences will be this”.

After the successful prosecution of a professional enabler: publicising outcomes

60. Finally, an effective deterrent measure is to publicise thoroughly all high-profile tax crimes committed, the enablers involved, and the punishments that criminals receive such as incarceration, penalties, and loss of license or business. This is important to underscore to the public that individuals who commit tax crimes face consequences, and reinforces fair taxation principles and the public’s trust in the tax system, thereby contributing to higher tax morale (OECD, 2019^[15]). It is common that countries do not disclose information about allegations and ongoing investigations until the case has been completed. However, upon case completion, there often is some form of publication about the criminal acts and the consequences of the offender’s criminal behaviour. These successful prosecutions can be publicised via press releases by the law enforcement agency, along with appropriate communication strategies to ensure media coverage by other news sources, blogs, and professional journals. Making the public aware of the consequences of these behaviours is crucial to deterring similar actions in the future.

4.1.2. Engagement and awareness raising

61. Tax administrations can tackle non-compliant behaviour through engaging directly with professions that may be vulnerable to being professional enablers. By working with these sectors and their industry representative bodies, countries can develop a greater understanding about the business practices involved and deliver targeted education. This increased visibility for authorities can also allow countries to develop bespoke strategies to target high-risk enabler sectors if need be. In the prevention stage, where possible, this education is most effective when productive working relationships are fostered between taxpayers, their intermediaries, and tax administration colleagues.

62. Awareness raising activities in high-risk professional enabler sectors has produced positive results in some countries. Through industry engagement, consultative and educational activities, professional enablers who are less cognisant of their part in facilitating wrongdoing are made more aware regarding their role and the risk of their behaviour having legal ramifications. Furthermore, the raised awareness of the tax authority’s scrutiny into an industry sector will typically have a deterrent effect, whilst giving government authorities greater visibility into the professional services industry behaviour and norms.

4.1.3. Promoting corporate responsibility and good governance

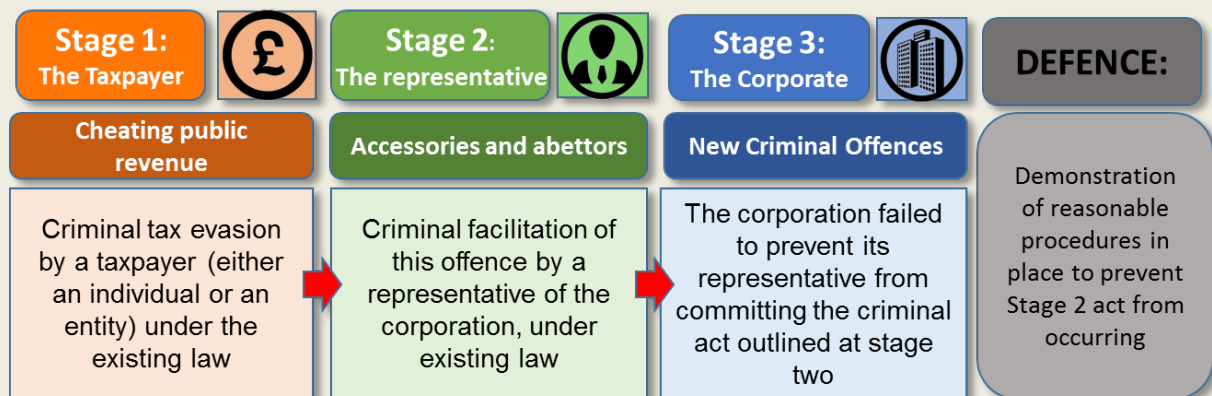
63. Professional enablers commonly provide services for or on behalf of a corporation. Here, the role of professional enablers can be shaped by the corporate culture of the organisations they work for and a

company's attitude towards tax compliance can directly affect the behaviour of a professional enabler providing services on behalf of that company. For example, behaviour may be influenced by direct incentives such as bonus systems that encourage risk-taking, deficiencies in systems such as employee training, or a culture that turns a blind eye to certain practices such as poor know-your-customer practices, or a lack of clarity from top-level management on refusing to engage in tax fraud. This is an issue identified in the United Kingdom, which has legislated to attribute liability to companies that have not prevented facilitation of tax crime within their organisations, as illustrated in the below example.

Box 20. The United Kingdom's legislation creating corporate responsibility to prevent criminal facilitation of tax crime

In the United Kingdom, for those professional enablers who provide services for or on behalf of a corporation, issues were identified in its law enforcement's capability to tackle the corporation's role in the facilitation of tax fraud. Attributing criminal liability to the corporation meant establishing proof that its senior members were involved in and aware of the illegal activity. This made it difficult to hold large multinational organisations to account (given their structures) and may have driven poor behaviours i.e. senior members of an organisation ignoring criminal acts committed by its representatives in order to protect their organisation from criminal liability.

Recognising this as an issue, the United Kingdom introduced new legislation in 2017 which holds those corporates to account which fail to prevent its associated persons (i.e. professional enablers) from criminally facilitating tax crime, referred to as the Corporate Criminal Offences (CCO). These offences seek to address the issues of attributing criminal liability to legal persons and places the responsibility on the corporate to take responsibility for improving its systems, controls and culture. The offences do not alter what is criminal at the individual level, but rather allows the corporation to be liable for failing to prevent an individual from committing acts that were already criminal.



CCO is a strict liability offence, meaning that if a tax crime has been committed (stage 1) and that fraud has been criminally facilitated by an enabler (stage 2) then the corporate would be liable under the new corporate offences, unless it can demonstrate that it has put in place reasonable procedures to prevent the facilitation of tax evasion by persons providing services for or on its behalf. This is the in-built defence of the offences and is designed to encourage corporates to take responsibility for putting in place systems and controls to prevent their representatives from facilitating tax evasion.

64. A country's professional enabler strategy should look to incentivise corporations to take responsibility for the behaviour of their organisation as a whole, including their representatives, and put in place appropriate systems and controls. Promoting a culture of good governance and corporate

responsibility is essential to support the public perception of the rule of law applying to large corporations. This is important to maintain trust in the tax system and have a strong culture of tax compliance and tax morale in a country. Maintaining a socially responsible corporate image is important to most businesses for reputational reasons, which in turn affects profits. Therefore, this ought to encourage corporates to be selective in the tax professionals and intermediaries they hire to ensure there is no association with recalcitrant professional enablers.

4.2. Disclosure facilities

4.2.1. Voluntary disclosure programmes

65. Voluntary disclosure programmes give taxpayers an opportunity to submit to tax authorities details of any previously fraudulent behaviour they have committed, such as not appropriately declaring income, inappropriately claiming deductions, credits or benefits, or falsehoods or omitted information from previous tax returns. Taxpayers are typically incentivised to make voluntary disclosures through such programmes due to offers of leniency or discounts on penalties and tax liabilities where a taxpayer makes a voluntary disclosure, or if they know that tax authorities will likely be made aware of their fraudulent tax affairs through transparency and exchange of information measures, such as the Standard for Automatic Exchange of Financial Account Information in Tax Matters (the AEOI standard). Voluntary disclosure programmes can operate indefinitely or for a limited time, and can be general or targeted towards disclosures of a specific type, for example the US Offshore Voluntary Disclosure Programs.

66. The results of such voluntary disclosure programmes can bring significant amounts of revenue to tax administrations, some figures of which are highlighted in the latest 10th Anniversary Report of the Global Forum on Transparency and Exchange of Information for Tax Purposes (OECD, 2019, p. 32^[16]):

As of November 2019, voluntary disclosure programmes and tax investigations helped to identify about EUR 102 billion in additional revenue (tax, interest, penalties). Voluntary disclosure programmes have been the largest contributor to this figure with nearly 40 jurisdictions having reported some form of disclosure between 2009 and 2019. For instance, voluntary disclosures brought EUR 462 million in Australia, EUR 13.6 billion in Brazil, nearly EUR 6 billion in Germany, EUR 29 million in Hungary, EUR 54 million in Luxembourg and over EUR 900 million in Mexico. Over 1 million of taxpayers have come forward to voluntarily disclose their assets.

67. Voluntary disclosure facilities are not just an opportunity to increase compliance amongst taxpayers and improve revenue receipts, but they can also be an opportunity to identify professional enablers. Information collected can be analysed to identify prolific enablers suitable for investigation, as well as increasing understanding of the scale and nature of the threats. Analysis of the structures used in disclosed affairs can be used for risking and for improving regulation and legislation, for example by closing loopholes. There is also the additional deterrent effect if professionals know that their names could be disclosed through such facilities and action potentially taken against them.

4.2.2. Whistleblowers, anonymous sources and other reporting mechanisms

68. Anonymous tip-offs and whistle-blowers have led to successful investigations in many countries, and continue to be a useful source of intelligence in an environment where there is increasing public discontent with tax evaders and those who enable them. In Australia, a publicly accessible tip-off mechanism was created to specifically report on tax evasion schemes and their promoters (ATO, 2019^[17]). This voluntary reporting mechanism is openly available online, and creates the opportunity for tax authorities to receive increased intelligence on newly marketed tax schemes or new promoters, as well as a range of other issues. The prospect of being reported upon can result in a decrease in mass-marketed tax schemes, especially by bigger firms concerned with reputational risk.

69. Some countries also provide incentives to those who come forward with information that assists in the successful investigation of a case, such as through a reward or percentage of assets recovered from a successful prosecution, or immunity from prosecution for the whistle-blower. For example, in Mexico, the National Code of Criminal Procedure was amended to allow whistle-blowers to be granted immunity from prosecution, even where the person has participated in a tax or financial crime, if the whistle-blower provides essential information for the prosecution of the ultimate beneficiaries of crimes. To enable these informants to come forward, countries are recommended to have easily accessible mechanisms for sources to make their reports, and appropriate legal and administrative safeguards to protect the anonymity of the individual and the confidentiality of the information provided (OECD, 2017^[18]).

4.3. Mandatory disclosure rules

Mandatory disclosure rules are laws put in place by countries that require intermediaries or taxpayers to report to the authorities if they have marketed, implemented or engaged in transactions or arrangements with particular hallmarks. These hallmarks can be designed to capture information such as cross-border aggressive tax planning, offshore structures, and arrangements that circumvent reporting under the AEOI Standard or conceal beneficial ownership.

70. With timely reporting on these arrangements through mandatory disclosure rules, tax authorities are able to intervene earlier on in the life cycle of the commission of tax crimes, before arrangements have been implemented and harmful effects have taken place. Furthermore, the mandatory requirement to report on such arrangements has a disruptive effect on professional enablers who must actively contemplate their actions in the context of the reporting requirements, or who may be deterred from pursuing illegal arrangements due to the reporting requirements. Failure to report can also serve as the basis for specific criminal or civil action. It can also act as a deterrent to clients, if they are informed that the contemplated arrangement will be reported to the tax authority.

71. The 2018 OECD report on Model Mandatory Disclosure Rules for CRS Avoidance Arrangement and Opaque Offshore Structures contain model frameworks and best practices that can assist countries in designing a disclosure regime that fits their needs.⁷

72. For example, since the adoption of *Council Directive (EU) 2018/822* by EU Member States, most EU countries have now either put in place or are in the process of putting in place national legislation for mandatory disclosure rules, which contain significant penalties for failures to comply. Under the Directive, there will also be periodic automatic exchanges of information between EU member states, which can be fed into domestic professional enabler risk assessments and analytics.

73. Where mandatory disclosure is reported to the tax administration, this information should be shared with the relevant tax crime investigators so that they can assess whether there is a scheme that is of a potential criminal nature that ought to be investigated and pursued. If this is in a separate agency, a mechanism for sharing this information should be put in place, as part of the whole-of-government approach set out in chapter 5 below.

⁷ Although designed in a different context, the 2015 OECD BEPS Action 12 report on Mandatory Disclosure Rules may also provide useful background.

5 Effective investigations: across government and across borders

No single law enforcement agency acting alone can comprehensively tackle the issue of professional enablers, who operate across a range of fields and across borders. To close the gap, silo approaches need to be discarded, and instead tax crime authorities must work collaboratively with other agencies in their own jurisdiction as well as with other agencies internationally. This chapter highlights whole-of-government and multilateral approaches specifically tackling professional enablers.

5.1. Domestic whole-of-government approaches

Different government agencies are involved at various stages of tackling financial crimes, including the prevention, detection, investigation and prosecution of offences and the recovery of the proceeds of crime (OECD, 2017^[19]). As such, different agencies will have interactions with, supervision of, or active investigations into professional enablers. This can include tax authorities, financial regulators, financial intelligence units, police and prosecutors.

74. In order to have the most coherent and robust approach to preventing, identifying, disrupting and prosecuting professional enablers, mechanisms should be in place to enable information sharing between the relevant agencies. To start with, this should include mechanisms for reporting and sharing suspicions that an intermediary is a professional enabler. It should also include the broadest possible forms of information sharing, from spontaneous sharing of intelligence, exchanging detailed case information where requested, and, for relevant sets of data, automatic direct access to information (such as a register of disqualified directors, list of known professional enablers or associated actors, or list of known schemes marketed by professional enablers).

75. To implement this most effectively, countries should:

- Put in place legal gateways for reporting and information sharing between agencies;
- Map the existing information held by each agency in connection with professional enablers, in order to determine what types of information will be of relevance to other agencies;
- Train and increase awareness of the role of, and information held by, other agencies as concerns professional enablers, to inform the ability to effectively share information;
- Identify a lead contact in each agency for receiving and disseminating reports of suspicions of professional enabler activity;
- Provide operational guidance for how to request information from, and share information with, other agencies, such as describing the relevant procedures, and developing standard templates in which information should be shared to facilitate easy and efficient information sharing;

- Have a monitoring mechanism for sharing feedback on the results of the shared information, to inform revisions to the operational guidance;
- Have the ability in law and in practice to protect the confidentiality of information and the integrity of work carried out by other agencies.

76. Beyond information sharing, more active, case-specific mechanisms for implementing a whole of government approach to professional enablers are important. These should include:

- **Joint investigation teams:** these enable agencies with a common interest to work together in an investigation. This enables a multi-disciplinary approach, allowing investigators to draw on a wider range of investigatory expertise, skills and experience. Joint investigations may also help to avoid duplication arising from parallel investigations, and increase efficiency by enabling officials from each agency to focus on different aspects of an investigation. For example, where a professional enabler was devising schemes to commit tax evasion by creating fraudulent refund claims, and then creating false business transaction records to launder the money, a joint tax and money laundering investigation could assist in gathering all relevant evidence efficiently to secure both the tax evasion and money laundering conviction, and raise awareness between the agencies of the mutual links between these crimes.
- **Inter-agency centres of intelligence:** these centralise information gathering and analysis from a number of agencies. They can gather and analyse existing data held by a range of agencies as well as conduct their own research. Centralising these activities allows for the development of expertise in one area, and can reduce costs of duplication. For example, a centre of intelligence could be tasked with analysing data from offshore leaks to identify high-risk professional enablers operating in the jurisdiction, which could be shared with all relevant agencies to inform future investigations.
- **Secondments and co-location of personnel:** these arrangements allow the temporary reassignment of officials to other agencies. It is an effective way of transferring skills, building contacts to assist co-operation in the future, and cross-fertilising relevant experience and specialist knowledge. This can be particularly effective in informing officials of the information and powers available to the counterpart agencies, and can make the other forms of information sharing and co-operation more effective.
- **Whole-of-government training programmes:** Training programmes that bring together officials from a range of agencies provide an important opportunity for building personal relationships and sharing experiences in dealing with common problems. Targeted whole of government training programmes focusing on professional enablers is a way to share information on trends, guidance on investigative techniques, best practice in managing cases and methods for identifying concerns of relevance to another agency.

77. In devising their professional enabler strategy, countries should seek to make the most use possible of a whole-of-government approach to the issue.

Box 21. The United Kingdom's National Economic Crime Centre

Formed in November 2018, the National Economic Crime Centre (NECC) is a collaborative, multi-agency centre that has been established to deliver a step change in the response to tackling economic crime and illicit finance. The NECC brings together law enforcement agencies, prosecutors, government departments and regulatory bodies in the United Kingdom, and sets priorities that informs operational activity.

As an example, in mid-2019, the NECC, in response to the threat from professional enablers, created the Enabler Practitioners Group. This multiagency forum promotes the identification of cases and encourages investigators and prosecutors to use the full range of legislative and regulatory powers. Strategically, the NECC facilitates information sharing with the private sector, which is strengthening the United Kingdom's understanding of the threat and is informing policy on these enablers of financial crime.

5.2. International co-operation

Financial crimes, including tax crimes, are a global problem that needs a global solution. With globalisation, the ability for professional enablers to operate cross-border and arrange transactions that send funds abroad instantly has increased. However, law enforcement authorities have less knowledge of activity outside their borders. International co-operation is therefore an essential aspect of tackling professional enablers. This includes traditional exchange of information channels, as well as newer forms of real-time international co-operation.

5.2.1. Exchange of information

78. Over 160 jurisdictions worldwide have joined the Global Forum on Transparency and Exchange of Information for Tax Purposes (Global Forum) and made a commitment to ensure an effective implementation of the international standards on transparency and exchange of information for tax purposes. The networks for exchanging information have expanded at unprecedented speed, and the ability to request information from almost any country around the world has been made possible through bilateral and multilateral exchange of information and co-operation agreements, such as the Multilateral Convention on Mutual Administrative Assistance in Tax Matters which now covers more than 130 jurisdictions (OECD, 2020^[20]).

79. Over the last ten years, the volume of the information exchanged between tax authorities, both on request and automatically, has significantly increased, with more than 250 000 requests being made in this time. In addition, nearly 100 jurisdictions are exchanging information automatically on financial assets held around the world. Nearly 100 countries carried out automatic exchange of information in 2019, enabling their tax authorities to obtain data on 84 million financial accounts held offshore by their residents, covering total assets of EUR 10 trillion. This represents a significant increase over 2018 – the first year of such information exchange – where information on 47 million financial accounts was exchanged, representing EUR 5 trillion. The growth stems from an increase in the number of jurisdictions receiving information as well as a wider scope of information exchanged (OECD, 2020, p. 5^[21]).

80. This shows that a commitment to using the exchange of information tools, supported by the accountability mechanism of the Global Forum, opens up an enormous possibility for international co-operation, as well as creating deterrence for professional enablers. In this era of tax transparency, studies

show that there has been a marked effect in the global decline of foreign-owned bank deposits in international financial centres, which fell by 24% (USD 410 billion) between 2008 and 2019 (O'Reilly, Parra Ramirez and Stemmer, 2019^[22]).

81. It also means that professional enablers have much more limited scope to operate outside the purview of tax authorities. As part of a professional enabler strategy, countries should be seeking to make the most of this powerful tool, and should continue to provide swift assistance to their counterpart authorities to reduce globally the impact of professional enablers. Countries should also look to broaden their use of exchange of information where possible. For example, most exchange of information agreements allow for:

82. **Group requests:** countries can request information from a counterpart tax authority about a group of taxpayers even if they are not individually identified. This can be particularly relevant where a professional enabler in the counterpart country has actively contributed to tax evasion on the part of resident taxpayers in a country, but the identity of the individual clients are unknown. See Annex B for a template group request form, created by the OECD Forum on Tax Administration's JITSIC programme. An example from the OECD Model Tax Convention illustrates this (OECD, 2017, p. 493^[23]):⁸

Financial service provider B is established in State B. The tax authorities of State A have discovered that B is marketing a financial product to State A residents using misleading information suggesting that the product eliminates the State A income tax liability on the income accumulated within the product. The product requires that an account be opened with B through which the investment is made. State A's tax authorities have issued a taxpayer alert, warning all taxpayers about the product and clarifying that it does not achieve the suggested tax effect and that income generated by the product must be reported. Nevertheless, B continues to market the product on its website, and State A has evidence that it also markets the product through a network of advisors. State A has already discovered several resident taxpayers that have invested in the product, all of whom had failed to report the income generated by their investments. State A has exhausted its domestic means of obtaining information on the identity of its residents that have invested in the product. State A requests information from the competent authority of State B on all State A residents that (i) have an account with B and (ii) have invested in the financial product. In the request, State A provides the above information, including details of the financial product and the status of its investigation.

83. **Spontaneous exchange of information**, which allows a tax authority to share information that may be of relevance to a counterpart. This can be powerful in speeding up the disruption of professional enablers, in that it alerts a counterpart to risks that they may otherwise be unaware of, or only uncover years later after conducting their own investigations. For example, spontaneous exchange could be relevant when a tax authority has uncovered the identify of a professional enabler that is operating in the counterpart jurisdiction, has become aware of a particular scheme being marketed to or implemented in the counterpart jurisdiction, or has identified a professional enabler's clients that are resident in the counterpart jurisdiction.

84. **On-sharing of tax information with other law enforcement agencies:** the Multilateral Convention, and certain bilateral tax treaties, generally restrict the use of internationally exchanged information to tax purposes only. However, recognising the links between tax crimes and other financial crimes such as money laundering and corruption, it is possible for the information received by one party to be on-shared with other agencies and used for other purposes, provided that:

- Such information may be used for those other purposes under the laws of the sending country; and
- The competent authority of that sending country authorises such use.

⁸ Commentary on Article 26 paragraph 8(h) in OECD (2017), *Model Tax Convention on Income and on Capital: Condensed Version 2017*, OECD Publishing, http://dx.doi.org/10.1787/mtc_cond-2017-en. See also paragraphs 5.2 and paragraphs 8(e) – 8(h) and 8.1

85. This type of on-sharing can be agreed on a bilateral basis, and can be an effective way of ensuring the advances made in ensuring effective international tax information sharing that has taken place in recent years can also be leveraged, where appropriate, by other law enforcement agencies in disrupting and prosecuting professional enablers. In pursuing this extended potential of exchange of information, due regard must be given to the need to ensure recipient agencies can protect the confidentiality of the information received.

5.2.2. OECD Common Reporting Standard (CRS) Disclosure Facility

In 2017, the OECD launched a disclosure facility on the Automatic Exchange Portal to allow open reporting of potential schemes to circumvent the CRS. This facility is part of a wider process that the OECD has put in place to deal with schemes that purport to avoid reporting under the CRS, so that any actual or perceived loopholes can be systematically analysed and addressed. This disclosure facility continues to be a useful information source to track potential enabler activity in the peddling of CRS avoidance schemes. Where the OECD Secretariat is made aware of a potential enabler risk pertinent to a particular country, this information is shared with the relevant governments.

5.2.3. Joint Chiefs of Global Tax Enforcement (J5)

86. The Joint Chiefs of Global Tax Enforcement (the “J5”) is an operational alliance between Australia, Canada, the Netherlands, the United Kingdom and the United States, formed to lead the fight against international tax crime and money laundering, including tackling crypto-currency threats, cybercrime, and targeting the professional enablers who make global tax evasion possible. The group brings together leading tax experience and offshore, crypto and cyber expertise from these countries to share intelligence at speed, build capacity and ultimately carry out joint operational activities. An example of this is contained in Box 23, where the Netherlands and the United States of America hosted “challenge” events, bringing together experts, investigators and data scientists to combine their skills and capabilities collaboratively, which culminated in the prosecution of a fraudulent crypto-asset network scheme.

87. The J5 was formed in 2018 in response to a call to action from the OECD for countries to do more to tackle the enablers of tax crime (HMRC & OECD, 2017^[24]). Professional services provided by enablers are constantly evolving, utilising modern technology and increasingly complex ways to hide wealth and illicit gains through the exploitation of offshore structures and financial instruments. All five countries face similar threats from organised crime groups and wealthy offshore tax evaders. The J5’s pooled resources and collective efforts means that there is increased insight, data and analytical capability available to the authorities of all five countries, enhancing the individual capabilities of each country simultaneously.

88. The J5 has a work stream specifically dedicated to combatting professional enablers. Each country has shared intelligence on targets they have operating in their own country where there is a multi-jurisdictional interest. These investigations involve sophisticated international enablers of tax evasion, such as global financial institutions and their intermediaries who help taxpayers to hide their income and assets. These highly harmful, high-end enablers of tax evasion were previously thought to be beyond the reach of the member countries.

Box 22. Coordinated day of action by the Joint Chiefs of Global Tax Enforcement

The first major operational activity for the Joint Chiefs of Global Tax Enforcement took place in January 2020 in which a globally coordinated day of action into suspected facilitation of offshore tax evasion was undertaken across the United Kingdom, the United States, Canada, Australia and the Netherlands.

The action occurred as part of a series of investigations in multiple countries into an international financial institution located in Central America, whose products and services were believed to be facilitating money laundering and tax evasion for customers across the globe. It was believed that through this institution, a number of clients were potentially using a sophisticated system to conceal and transfer wealth anonymously to evade their tax obligations and launder the proceeds of crime.

The coordinated day of action involved evidence, intelligence and information collection activities such as search warrants, interviews and subpoenas. Significant information was obtained as a result and investigations ensued, with the potential for further criminal, civil and regulatory action to arise from these actions in each country.

Box 23. BitClub network case

Example of crypto-asset fraud facilitated by a professional enabler (IRS, 2020^[25]) (DOJ, 2020^[26])*

From April 2014 through December 2019, the BitClub Network was a fraudulent scheme that solicited money from investors in exchange for shares of purported crypto-asset mining pools and rewarded investors for recruiting new investors into the scheme. The crypto-asset mining scheme was worth at least USD 722 million in damages to investors.

IRS Criminal Investigation (IRS-CI) special agents worked the case under the umbrella of the Joint Chiefs of Global Tax Enforcement (J5). In November 2019, IRS-CI hosted a crypto “Challenge” in Los Angeles, bringing together investigators, crypto-asset experts and data scientists from the five J5 countries in a co-ordinated push to track down individuals perpetrating tax crimes around the world. During the Challenge, the Dutch Fiscal Intelligence and Investigation Service (FIOD) worked collaboratively with IRS-CI to develop leads in the BitClub Network case.

On July 9, 2020, a Romanian citizen living in Germany has admitted to conspiring to engage in wire fraud and offering and selling unregistered securities in connection with his role in the BitClub Network. He assisted in the creation and operating of the BitClub Network and served as its programmer. In this capacity, he used his professional skills to falsify figures displayed as Bitcoin mining earnings to make it appear that the BitClub Network was earning more than what was actually being mined, effectively acting as a professional enabler for crypto-asset fraud.

The defendant now faces a maximum penalty of five years in prison and a fine of USD 250 000 (twice the pecuniary gain to the defendant or loss to the victims). Several other co-conspirators in the scheme are also being prosecuted.

* Note: This example is provided through publicly available information sources.

5.3. JITSIC Data Leaks Group’s work on the Intermediaries Disruption Strategy

89. The Joint International Taskforce on Shared Intelligence and Collaboration (JITSIC) brings together 40 of the world’s national tax administrations that have committed to more effective and efficient ways to deal with tax avoidance. Although the scope of this work is quite different to this report, which focusses on tax crimes, the model of international co-operation used by JITSIC, and particularly the work undertaken on the intermediaries disruption strategy, can be instructive for similar initiatives that could be undertaken by agencies responsible for tax crimes and law enforcement.

90. The JITSIC platform enables its member countries to share intelligence, actively collaborate on investigations, and conduct joint compliance activities. Members of JITSIC are able to share information and intelligence in an expedited manner through the JITSIC procedures and existing legal frameworks under the appropriate bilateral or multilateral legal instruments.

91. The JITSIC Data Leaks Group (DLG) arose out of the work of the JITSIC Paradise Papers Initial Assessment Group (PPIAG). The DLG was established in 2018 to continue the compliance risk assessment of the Paradise Papers data, released by the International Consortium of Investigative Journalists (ICIJ), with a focus on delivering practical results and to facilitate or recommend actionable compliance strategies for JITSIC members. The DLG was also mandated to collaboratively analyse anticipated and future data leaks on a needs basis.

92. JITSIC's work in this area has identified intermediaries as a high-risk group that would benefit from targeted multilateral compliance efforts. Intelligence gained from the JITSIC Panama Papers project and the PPIAG is that intermediaries often promote and put a number of taxpayers into the same structures. By targeting intermediaries, members can identify a number of similar arrangements more effectively, whilst minimising proliferation and maximising risk detection, treatment and mitigation strategies. Accordingly, the DLG has commenced work on the JITSIC Intermediaries Disruption Strategy (IDS) to target intermediaries through multilateral compliance action.

References

- ATO (2019), *Report schemes and promoters*, <https://www.ato.gov.au/General/Tax-planning/Report-schemes-and-promoters/> (accessed on 4 March 2020). [17]
- DOJ (2020), *Romanian Programmer Admits That He Helped Create Bitclub Network, A Fraud Scheme Worth At Least \$722 Million*, <https://www.justice.gov/usao-nj/page/file/1293331/download> (accessed on 17 September 2020). [26]
- DOJ (2014), *Caribbean-Based Investment Advisor Sentenced for Using Offshore Accounts to Launder and Conceal Funds*, <https://www.justice.gov/opa/pr/caribbean-based-investment-advisor-sentenced-using-offshore-accounts-launder-and-conceal> (accessed on 8 January 2021). [5]
- DOJ (n.d.), *Civil Employment Tax Injunctions*, <https://www.justice.gov/tax/civil-employment-tax-injunctions> (accessed on 4 March 2020). [13]
- DOJ (n.d.), *Program to Shut Down Schemes and Scams*, <https://www.justice.gov/tax/program-shut-down-schemes-and-scams> (accessed on 4 March 2020). [12]
- FATF (2019), *Best Practice on Beneficial Ownership for Legal Persons*, Financial Action Task Force, <https://www.fatf-gafi.org/publications/methodsandtrends/documents/best-practices-beneficial-ownership-legal-persons.html>. [31]
- FATF (2019), *Guidance for a Risk-Based Approach for Legal Professionals*, Financial Action Task Force, <https://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Legal-Professionals.pdf>. [35]
- FATF (2019), *Guidance for a Risk-Based Approach for the Accounting Profession*, Financial Action Task Force, <https://www.fatf-gafi.org/media/fatf/documents/reports/RBA-Accounting-Profession.pdf>. [36]
- FATF (2019), *Guidance for a Risk-Based Approach for Trust & Company Service Providers (TSCPs)*, Financial Action Task Force, <https://www.fatf-gafi.org/media/fatf/documents/reports/RBA-Trust-Company-Service-Providers.pdf>. [37]
- FATF (2019), *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, Financial Action Task Force, <http://www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html>. [9]
- FATF (2018), *Concealment of Beneficial Ownership*, Financial Action Task Force, <https://www.fatf-gafi.org/publications/methodsandtrends/documents/concealment-beneficial-ownership.html>. [32]

- FATF (2018), *Professional Money Laundering*, Financial Action Task Force, <https://www.fatf-gafi.org/publications/methodsandtrends/documents/professional-money-laundering.html>. [33]
- FATF (2014), *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*, Financial Action Task Force, <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>. [8]
- FATF (2013), *Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals*, Financial Action Task Force, <https://www.fatf-gafi.org/fr/documents/documents/mltf-vulnerabilities-legal-professionals.html>. [34]
- FATF (2012-2019), *International Standard on Combating Money Laundering and the Financing of Terrorism & Proliferation*, <https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>. [7]
- Halter, E. et al. (2011), *The Puppet Masters: How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do About It*, Stolen Asset Recovery (StAR) initiative. World Bank, <http://documents.worldbank.org/curated/en/784961468152973030/The-puppet-masters-how-the-corrupt-use-legal-structures-to-hide-stolen-assets-and-what-to-do-about-it>. [4]
- HMRC & OECD (2017), *Closing Statement of the Fifth OECD Forum on Tax and Crime*, <https://www.oecd.org/tax/crime/closing-statement-oecd-forum-on-tax-and-crime-november-2017.pdf>. [24]
- ICIJ (2020), *Offshore Leaks Database*, <https://offshoreleaks.icij.org/> (accessed on 18 September 2020). [1]
- IESBA (n.d.), *International Ethics Standard Board for Accountants*, <https://www.ethicsboard.org/> (accessed on 4 March 2020). [14]
- IMF (2019), *Chapter 2. Curbing Corruption*, International Monetary Fund, <https://www.imf.org/en/Publications/FM/Issues/2019/03/18/fiscal-monitor-april-2019>. [3]
- IRS (2020), *Examples of Abusive Return Preparer Investigations - Fiscal Year 2017*, <https://www.irs.gov/compliance/criminal-investigation/examples-of-abusive-return-preparer-investigations-fiscal-year-2017> (accessed on 14 April 2020). [6]
- IRS (2020), *Romanian programmer admits that he helped create Bitclub network, a fraud scheme worth at least \$722 million*, <https://www.irs.gov/pub/irs-utl/j5-media-release-07-09-2020.pdf> (accessed on 17 September 2020). [25]
- O'Reilly, P., K. Parra Ramirez and M. Stemmer (2019), "Exchange of information and bank deposits in international financial centres", *OECD Taxation Working Papers*, No. 46, OECD Publishing, Paris, <https://dx.doi.org/10.1787/025bfebe-en>. [22]
- OECD (2020), *Base Erosion and Profit Shifting*, <https://www.oecd.org/tax/beps/> (accessed on 18 September 2020). [2]
- OECD (2020), *Convention on Mutual Administrative Assistance in Tax Matters*, <https://www.oecd.org/tax/exchange-of-tax-information/convention-on-mutual-administrative-assistance-in-tax-matters.htm> (accessed on 4 March 2020). [20]

- OECD (2020), *OECD Secretary-General Tax Report to G20 Finance Ministers and Central Bank Governors - July 2020*, OECD, <http://www.oecd.org/tax/oecd-secretary-general-tax-report-g20-finance-ministers-july-2020.pdf>. [21]
- OECD (2019), *Money Laundering and Terrorist Financing Awareness Handbook for Tax Examiners and Tax Auditors*, OECD Publishing, <https://www.oecd.org/tax/crime/money-laundering-and-terrorist-financing-awareness-handbook-for-tax-examiners-and-tax-auditors.pdf>. [10]
- OECD (2019), *Tax Morale: What Drives People and Businesses to Pay Tax?*, OECD Publishing, <https://www.oecd.org/tax/tax-morale-f3d8ea10-en.htm>. [15]
- OECD (2019), *Transparency and Exchange of Information for Tax Purposes: Multilateral Co-operation Changing the World*, OECD Publishing, <https://www.oecd.org/tax/transparency/global-forum-10-years-report.pdf>. [16]
- OECD (2018), *Model Mandatory Disclosure Rules for CRS Avoidance Arrangements and Opaque Offshore Structures*, OECD Publishing, <https://www.oecd.org/tax/exchange-of-tax-information/model-mandatory-disclosure-rules-for-crs-avoidance-arrangements-and-opaque-offshore-structures.htm>. [30]
- OECD (2018), *Standard for Automatic Exchange of Financial Account Information in Tax Matters: Implementation Handbook*, OECD Publishing, <https://www.oecd.org/ctp/exchange-of-tax-information/implementation-handbook-standard-for-automatic-exchange-of-financial-account-information-in-tax-matters.htm>. [27]
- OECD (2017), *Effective Inter-Agency Co-Operation in Fighting Tax Crimes and Other Financial Crimes - Third Edition*, OECD Publishing, <https://www.oecd.org/tax/crime/effective-inter-agency-co-operation-in-fighting-tax-crimes-and-other-financial-crimes.htm>. [19]
- OECD (2017), *Model Tax Convention on Income and on Capital: Condensed Version 2017*, OECD Publishing, http://dx.doi.org/10.1787/mtc_cond-2017-en. [23]
- OECD (2017), *The Detection of Foreign Bribery, Chapter 2. The Role of Whistleblowers and Whistleblower Protection*, OECD Publishing, <http://www.oecd.org/corruption/anti-bribery/OECD-The-Role-of-Whistleblowers-in-the-Detection-of-Foreign-Bribery.pdf>. [18]
- OECD (2016), *Exchange of Information on Request: Handbook for Peer Reviews 2016-2020 Third Edition*, OECD Publishing, <http://www.oecd.org/tax/transparency/global-forum-handbook-2016.pdf>. [28]
- OECD (n.d.), *Co-operation and exchange of information on ATP*, <https://www.oecd.org/ctp/aggressive/co-operation-and-exchange-of-information-on-atp.htm> (accessed on 5 June 2020). [11]
- OECD/FATF (2011), *Identification and Quantification of the Proceeds of Bribery: A joint OECD-StAR Analysis*, OECD Publishing, <https://star.worldbank.org/publication/identification-and-quantification-proceeds-bribery>. [41]
- OECD/IDB (2019), *A Beneficial Ownership Implementation Toolkit*, OECD Publishing, <http://www.oecd.org/tax/transparency/beneficial-ownership-toolkit.pdf>. [29]

- StAR (2012), *On the Take: Criminalizing Illicit Enrichment to Fight Corruption*, World Bank Publications, <https://star.worldbank.org/publication/take-criminalizing-illicit-enrichment-fight-corruption>. [38]
- StAR (2012), *Politically Exposed Persons: Preventive Measures for the Banking Sector*, World Bank Publications, <https://star.worldbank.org/publication/politically-exposed-persons>. [40]
- StAR (2012), *Public Office, Private Interests: Accountability through Income and Asset Disclosure*, World Bank Publications, <https://star.worldbank.org/publication/public-office-private-interests>. [39]
- StAR (2011), *Asset Recovery Handbook: A Guide for Practitioners*, World Bank Publications, <https://star.worldbank.org/publication/asset-recovery-handbook>. [45]
- StAR (2011), *Barriers to Asset Recovery: An Analysis of the Key Barriers and Recommendations for Action*, World Bank Publications, <https://star.worldbank.org/publication/barriers-asset-recovery>. [44]
- StAR (2010), *Stolen Assets Recovery: Towards a Global Architecture for Asset Recovery*, Stolen Assets Recovery Initiative, <https://star.worldbank.org/publication/towards-global-architecture-asset-recovery>. [42]
- StAR (2009), *Stolen Asset Recovery: A Good Practice Guide for Non-conviction-based Asset Forfeiture*, World Bank Publications, <https://star.worldbank.org/publication/towards-global-architecture-asset-recovery>. [43]
- StAR (2009), *Stolen Asset Recovery: Management of Returned Assets*, StAR, <https://star.worldbank.org/publication/management-returned-assets>. [46]
- The Egmont Group (2013), *The Role of Financial Intelligence Units in Fighting Corruption and Asset Recovery: An Egmont Group White Paper*, The Egmont Group, https://egmontgroup.org/en/filedepot_download/1661/55. [47]
- The Egmont Group (2011), *Enterprise-wide STR Sharing: Issues and Approaches*, The Egmont Group, https://egmontgroup.org/en/filedepot_download/1661/47. [48]
- UNODC (2017), *Effective management and disposal of seized and confiscated assets*, United Nations Office on Drugs and Crime, https://www.unodc.org/documents/corruption/Publications/2017/17-07000_ebook_sr.pdf. [49]
- UNODC (2012), *Manual on International Cooperation for the Purposes of Confiscation of Proceeds of Crime*, United Nations Office on Drugs and Crime, https://www.unodc.org/documents/organized-crime/Publications/Confiscation_Manual_Ebook_E.pdf. [50]
- UNODC (2011), *Handbook on Identity-related crime*, United Nations Office on Drugs and Crime, https://www.unodc.org/documents/treaties/UNCAC/Publications/Handbook_on_ID_Crime/10-57802_ebook.pdf. [51]

Annex A. Other related work

This report is intended to be a contribution to the work of the international community to building strong, inclusive and fair societies, by strengthening the ability of policy makers and law enforcement authorities to address risks that undermine society. Significant work has been undertaken by other bodies, which will also be of relevance in this area. This includes:

In the tax area:

- the work of the Global Forum on Transparency and Exchange of Information, including to drive the effectiveness of exchange of information tools between tax authorities, as well as improving transparency (OECD, 2018^[27]) (OECD, 2016^[28]) particularly in the area of beneficial ownership (OECD/IDB, 2019^[29]);
- the work of the Committee on Fiscal Affairs, including to provide guidance on the available legal mechanisms for exchange of information and multilateral co-operation in tax matters, such as its recent work on model mandatory disclosure rules (OECD, 2018^[30]);
- the work of the Forum on Tax Administration, including its Joint International Taskforce on Shared Intelligence and Collaboration (JITSIC) which provides a mechanism for tax administrations to exchange information, actively collaborate on investigations, and share strategies and intelligence on operational risks and issues, including its working group on the Data Leaks.

In anti-money laundering, the work of the Financial Action Task Force, including:

- guidance and best practices on beneficial ownership (FATF, 2019^[31]);
- concealment of beneficial ownership (FATF, 2018^[32]);
- techniques and tools used by professional money launderers (FATF, 2018^[33]);
- guidance for legal professionals on vulnerabilities for involvement in money laundering and terrorist financing (FATF, 2013^[34]);
- guidance for a risk-based approach for legal professionals (FATF, 2019^[35]), accountants (FATF, 2019^[36]) and trust and company service providers (FATF, 2019^[37]).

In anti-corruption, the work of the World Bank's (WB) and the United Nations Office on Drugs and Crime's (UNODC) joint Stolen Asset Recovery Initiative (StAR), including:

- guidance and best practices on the criminalisation of illicit enrichment of public officials (StAR, 2012^[38]);
- examining the core design features and implementation challenges of income and asset disclosure (IAD) regimes (StAR, 2012^[39]);
- examining the forms of beneficial ownership structures involving high-level public officials and providing recommendations on formulating an anti-corruption strategy (Halter et al., 2011^[4]);
- formulating policy recommendations for banks and regulatory authorities to improve preventive measures that address money laundering risks posed by Politically Exposed Persons (PEPs) involved in corruption (StAR, 2012^[40]);
- OECD / StAR study on the identification and quantification of the proceeds of active bribery in international business transactions (OECD/FATF, 2011^[41]).

In enforcement, the work of

- StAR on asset recovery, including a series of publications on; the role of the international community and national authorities (StAR, 2010^[42]), guidance for non-conviction based asset forfeiture (StAR, 2009^[43]), the key barriers to asset recovery in foreign jurisdictions and good practices to counter them (StAR, 2011^[44]), approaches to recovering proceeds of corruption located in foreign jurisdictions and their underlying challenges (StAR, 2011^[45]), and the management of successfully recovered stolen assets (StAR, 2009^[46]).
- Egmont Group of Financial Intelligence Units (Egmont) on; the role of financial intelligence units (FIU) fighting corruption and asset recovery (The Egmont Group, 2013^[47]), and guidance for cross-border suspicious transaction report (STR) sharing regime (The Egmont Group, 2011^[48]).
- UNODC on enforcement issues including; management and disposal of seized and confiscated assets (UNODC, 2017^[49]), guidance on international co-operation in asset recovery (UNODC, 2012^[50]), and criminalisation and enforcement of identity-related crime (UNODC, 2011^[51]).

Annex B. Example of template for Group EOI request

Request for Information under the TIEA/DTC/MAC⁹ applicable between [jurisdiction] and [jurisdiction]

The completed form constitutes a confidential communication between the competent authorities governed by [legal basis if applicable].

1.	To: ¹		
2.	From: ²		
3.	Contact point ³	Name:	
		Email:	
		Telephone:	
		Language skills:	
4.	Legal Basis:		
5.	Reference numbers and related matters	Reference number: ⁴	
		Initial request:	Please tick: <input type="checkbox"/> yes <input type="checkbox"/> no If no, please provide reference number(s) and date(s) of any related request(s) and/or response(s):
		Number of attachments to the request:	
		Total number of pages for all attachments:	
6.	Urgency of reply	Date, if any, after which information would no longer be useful:	

⁹ Please verify that the title corresponds to your agreement and please contact the requested jurisdiction prior to the sending of a group or bulk request.

		Urgent reply required due to:	Please check the box: <input type="checkbox"/> Statute of limitation; date: <input type="checkbox"/> Suspected criminal tax matter <input type="checkbox"/> Court case <input type="checkbox"/> Other reasons (please specify):
7.	Summary ⁵		
8.	Identity of subject/group under examination or investigation: ⁶		
9.	Tax period/s under investigation or taxable event for which or in relation to which the information is sought: ⁷		
10.	Tax(es) to which the request relates: ⁸		
11.	Purpose in accordance with the applicable EOI instrument, for which the information is requested:		Please check one or more boxes: <input type="checkbox"/> determination, assessment and collection of taxes of civil/administrative tax matters ⁹ , <input type="checkbox"/> investigation or prosecution of criminal tax matters, <input type="checkbox"/> other (please specify):
12.	Relevant background: ¹⁰		
13.	Explanation to confirm that all possible domestic means have been pursued to obtain the information requested, except those that would give rise to disproportionate difficulties: ¹¹		
14.	Reasons why the information requested is foreseeably relevant for the tax purpose indicated/investigation: ¹²		
15.	Information requested: ¹³		

16.	Grounds for believing that the requested information is held in the requested jurisdiction or is within the possession or control of a person within its jurisdiction:	
17.	Name and address of any person believed to be in possession of the information requested (to the extent known):	
18.	Request to refrain from notifying the persons under investigation or concerned:	<p>Please tick: <input type="checkbox"/> yes <input type="checkbox"/> no</p> <p>Please indicate reasons:</p> <p><input type="checkbox"/> If yes, the authority responsible in the requesting state confirms that it would be able to guarantee this course of action in similar circumstances.</p>
19.	Form, if any, in which information is requested: ¹⁴	<p>In the case of the production of copies, authentication is required:</p> <p>Please tick: <input type="checkbox"/> yes <input type="checkbox"/> no</p> <p>If yes, which ones:</p> <p>Further requirements, such as translation of reply:</p> <p>Please tick: <input type="checkbox"/> yes <input type="checkbox"/> no</p> <p>If yes, which ones:</p>
20.	<p>In making the request, the requesting competent authority states that:</p> <p>(a) all information received in relation to this request will be kept confidential and used only for the purposes permitted in the agreement which forms the basis for this request;</p> <p>(b) the request is in conformity with its law and administrative practice and is further in conformity with the agreement on the basis of which it is made;</p> <p>(c) the information would be obtainable under its laws and in the normal course of its administrative practice in similar circumstances.</p>	

Date

Authorised signature of requesting competent authority

Foonotes for sending country guidance only. Please remove before sending.

¹ Please add name and address of the competent authority of the requested jurisdiction.

² Please add name and address of the competent authority of the requesting jurisdiction.

³ The contact point having the authority to exchange information.

⁴ Please provide a reference number that the requested competent authority could use in case of questions and that allows retrieving the request and the related file.

⁵ Please give a short and concise request description regarding the tax purpose of the investigation and the purpose of request.

⁶ Please refer to the commentary to Article 26 of the OECD Model Convention (DTC), especially to the paragraphs related to group request, e.g. paragraphs 5.2 and paragraphs 8(e) – 8(h) and 8.1.

⁷ Please verify that the applicable EOI instrument is in place and in force for the period of the request and the period under review. For older years, if prosecution or assessment would ordinarily be proscribed by the applicable statute of limitations, please describe how the limitations period is held open, or is expected to be held open.

⁸ Please review the applicable EOI instrument and add the name of the tax(es), e.g. corporate income tax. Add also the type of tax(es) (personal, corporate etc.) if the name of the tax(es) is not sufficiently indicative of the type of tax.

⁹ It is understood that the investigation of civil/administrative tax matters falls under this heading.

¹⁰ Please provide the necessary background information, which would typically include a brief summary of the ongoing examination or investigation and how the requested information relates to this examination or investigation. The background information should if applicable mention the link regarding a project or other source of information assessed as useful for the administration of the request by the requested jurisdiction. Insert any other factual basis for request, such as information from similar taxpayers' examinations, interviews, or other research, if applicable, as well as the model of behaviour regarding the group. Where any other persons (e.g. individuals, companies, partnerships, trusts, etc.), including foreign persons, are relevant to the examination or investigation and the request, please specify, to the extent known, their relationship to the taxpayer and provide information sufficient to identify these persons.

Please insert an enclosure showing the scheme/structure, if applicable.

If preferred, please refer to an attachment to provide the Relevant Background alternatively include a summary of the Relevant Background with the full description in an attachment enclosed.

¹¹ Please provide the necessary information to confirm that all means available within your territory have been pursued to obtain the information, except those that would give rise to disproportionate difficulty. In case you have abstained from using any means available in your own territory to obtain the information because this would give rise to disproportionate difficulties, please provide a description of the means and of the disproportionate difficulties.

¹² Please insert reasons for believing that the information requested is relevant to your investigation. Please refer to the definition of foreseeable relevance in the commentary to Article 26 of the OECD Model DTC, especially to the paragraphs related to group request, i.e. paragraphs 5, 5.1 and 5.2 and 8h, as well as Articles 1 and 5(5) OECD Model TIEA and accompanying commentary. The requirements to meet the standard of "foreseeable relevance" implies the detailed description of the group subject to the request, the facts and circumstances that have led to the request as well as a clear factual basis supporting the reasons to believe that the taxpayers of the group have been non-compliant. Typically, such factual basis could emanate in previous investigations or voluntary disclosure programs. This could include an explanation of the applicable tax law or criminal law, and why there is reason to believe that the taxpayers described have been non-compliant and how the information would assist in determining compliance of the taxpayers described.

¹³ The requested information should be foreseeable relevant and in concordance with the information provided in the previous sections, e.g. Relevant Background. Please be as specific as possible about the information you are requesting, as it will form the basis for any domestic information gathering measures

taken by the requested jurisdiction. For group requests, please consider whether only data/information (no documents) could be sufficient. Please give numbers/letters to the questions to ease their administration.

¹⁴ Please specify the format in which the information is requested and whether any translation of reply, including to which language, or any authentication procedure is needed, as well as the reasons therefore. Please consider the additional time and costs, which might need to be agreed upon, relating to authentication of documents and translation.

Ending the Shell Game: Cracking down on the Professionals who enable Tax and White Collar Crimes

White collar crimes like tax evasion, bribery, and corruption are often concealed through complex legal structures and financial transactions facilitated by lawyers, accountants, financial institutions and other “professional enablers” of such crimes. These crimes have significant impacts on government revenue, public confidence and economic growth, including the recovery from COVID-19. This report sets out a range of strategies and actions for countries to take to tackle professional intermediaries who enable tax evasion and other financial crimes on behalf of their criminal clients. The report highlights the damaging role played by these intermediaries and the importance of concerted domestic and international action in clamping down on the enablers of crime, and includes recommended counter-strategies for deterring, disrupting, investigating and prosecuting the professionals who enable tax and white collar crimes.



For more information:



ctp.contact@oecd.org



www.oecd.org/tax/crime



[@OECDtax](https://twitter.com/OECDtax)

Appendix 3

The Challenges of Implementing Anti-Money Laundering
Regulation: An empirical Analysis by Dr. Illaria Zavoli and Dr.
Colin King - 2021

The Challenges of Implementing Anti-Money Laundering Regulation: An Empirical Analysis

Dr Ilaria Zavoli and Dr Colin King¹

Modern Law Review, DOI: 10.1111/1468-2230.12628

Link: <https://onlinelibrary.wiley.com/share/author/JZCV4KEI2XGDUMK6IVI3?target=10.1111/1468-2230.12628>

We thank Liz David-Barrett, Saskia Hufnagel, Amir Paz-Fuchs, Clive Walker, Peter Whelan and the reviewers for their helpful comments on an earlier draft. This research was supported by a British Academy 'Tackling the UK's International Challenges' grant (ref: IC160112).

Abstract

For over three decades, money laundering has been an area of concern for policymakers and law enforcement, with significant efforts undertaken at national and international levels to combat it. Recently, laundering of criminal proceeds using real property has attracted increased attention amongst policymakers. Various efforts are now being undertaken to tackle money laundering in the UK property market, but there are still significant difficulties in its practical implementation. Drawing upon semi-structured interviews with estate agents and compliance officials, this study identifies critical aspects of AML compliance that are particularly problematic for those involved in it. In so doing, this article delivers a new perspective, by analysing data gathered with the first empirical study on the implementation of AML obligations in practice (in the UK property market) since the introduction of the 2017 Money Laundering Regulations.

Keywords: anti-money laundering, real estate, compliance, UK, regulation

¹ University of Leeds and University of London, respectively. Contact email: colin.king@sas.ac.uk

Introduction

The creation of any anti-money laundering (AML) regime brings with it expectations as to its outcomes² and specific issues with its implementation in practice, including the need to have a robust set of rules and obligations that can be relied upon by public and private actors.³ In this context, the development of AML in the UK has seen a varied approach where, although the regulation and provisions are the same for all regulated sectors (e.g. financial, real estate, luxury goods), there are different levels of engagement with AML rules and mixed results for their implementation. Moreover, despite the comprehensive nature of the UK AML regime, which applies to all designated subjects with no distinction as to the regulatory burden imposed on them, some sectors show more variations than others as to their compliance approaches and responses.⁴ This is due to the existence of multiple subjects within a single sector that share the same AML obligations, but that in fact represent very distinctive positions and, therefore, have quite dissimilar functions.

These elements of difference (and perhaps inconsistency) across and within sectors play an important role in the implementation of AML regulation, and they are particularly evident when considering the real estate sector. Indeed, estate agents are a particularly apt case study given the expanding AML demands imposed on these actors.⁵ Further, compared to other sectors, the real estate sector includes many subjects who perform very different functions (such as buying, selling, letting). As such, the real estate sector provides important insights as to the challenges of implementing AML regulation. However, despite the potential for investigation, the literature has considered the real estate sector only marginally, with no empirical analysis of the challenges that UK AML regulation creates for those operating in the sector.

Drawing upon semi-structured interviews with estate agents and compliance officials, this study provides a better understanding of the dynamics of AML within the UK real estate sector, and it identifies critical aspects of AML compliance that are particularly problematic for those involved in it. In so doing, this article delivers a new perspective, by analysing data gathered with the first empirical study on the implementation of AML obligations in practice (in the UK property market) since the introduction of the 2017 ML Regs.⁶ The rationale underpinning this analysis, namely the focus on lived realities, draws upon research that demonstrates that compliance with the law is influenced by people's (subjective) perceptions about the fairness of procedures.⁷

² For wider discussion about effectiveness, see K. Getz, 'The Effectiveness of Global Prohibition Regimes: Corruption and the Antibribery Convention' (2006) 45 *Business and Society* 254. In the specific context of AML see, for instance, R.F. Pol, 'Anti-money laundering effectiveness: assessing outcomes or ticking boxes?' (2018) 21 *Journal of Money Laundering Control* 215; B. Unger et al, *The Economic and Legal Effectiveness of the European Union's Anti-Money Laundering Policy* (Edward Elgar, 2014).

³ On the compliance activities of actors in the AML regime, see A. Verhage, *The Anti Money Laundering Complex and the Compliance Industry* (Oxon: Routledge, 2011).

⁴ On AML compliance in different sectors and countries, see C. Verdugo Yepes, 'Compliance with the AML/CFT International Standard: Lessons from a Cross-Country Analysis' (2011) *IMF Working Papers* 1; A. Verhage, *The anti money laundering complex and the compliance industry* (Oxon: Routledge, 2011).

⁵ For an overview of the current framework and how it relates to estate agents, see HMRC, *Estate agency business guidance for money laundering supervision* (Updated October 2020).

⁶ Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.

⁷ T.R. Tyler, *Why People Obey the Law* (New Haven: Yale University Press, 1990); J. Sunshine and T.R. Tyler, 'The Role of Procedural Justice and Legitimacy in Shaping Public Support for Policing' (2003) 37 *Law & Society Review* 513. For scepticism on whether there is correlation between procedurally just

Thus, there is significant value in considering the views of those who have personal experiences of the AML regime.⁸ Given significant concerns as to the effectiveness of AML regulation,⁹ exploring such experiences is timely.

From the foregoing, this study represents a significant examination of AML implementation, specifically in the UK real estate sector, which relies upon original empirical data and identifies key aspects of AML regulation, including its limitations and more challenging features for compliance. In this sense, this research provides relevant inputs into the discourse on AML implementation in the UK (even beyond the real estate sector) and for future legislative and policy-oriented initiatives that need to take into account the practice of AML.

This article is divided into five parts. The next three sections set out, respectively, the theoretical and legislative context of AML in relation to the real estate market, the methodology used in the study, and the provisions regulating estate agents and the UK AML regime. Then, the article provides a critical examination of two themes that emerged from the interviews relating to the implementation of AML obligations: (i) Customer Due Diligence; and (ii) reporting suspicions. The analysis of these themes provides important insights into the operation of AML in practice. Without wishing to advocate that the views of regulatees be determinative,¹⁰ it is nonetheless valuable to consider the challenges associated with the implementation of regulation from the perspective of these actors. This article demonstrates that practical issues arise in central aspects of the AML regime and, in so doing, it illustrates the (negative) impact of AML obligations on businesses, which creates discrepancies in AML implementation and a sense of frustration among regulatees. These discrepancies also point out key differences between the law on paper and the law in action, and they reinforce concerns as to the legitimacy of the UK AML regime. In this regard, the practical issues encountered by regulatees could lead to resistance to AML compliance by estate agents who would otherwise comply with the AML regime.

treatment and perceived legitimacy/compliance, see D. Nagin and C. Telep, 'Procedural Justice and Legal Compliance' (2017) 13 *Annual Review of Law and Social Science* 5. In response, Tyler affirms that procedural justice is the 'best available model' and is supported by empirical research. He argues that from a policy perspective widespread reliance on procedural justice is justified: T.R. Tyler, 'Procedural Justice and Policing: A Rush to Judgment?' (2017) 13 *Annual Review of Law and Social Science* 29.

⁸ A related consideration is whether people question the legitimacy of relevant laws, such as AML. For wider discussion, see K. Murphy, T.R. Tyler, and A. Curtis, 'Nurturing Regulatory Compliance: Is Procedural Justice Effective When People Question the Legitimacy of the Law?' (2009) 3 *Regulation and Governance* 1.

⁹ P. Alldridge, *What Went Wrong with Money Laundering Law?* (London: Palgrave Macmillan, 2016); A. Verhage, 'Great Expectations But Little Evidence: Policing Money Laundering' (2017) 37 *International Journal of Sociology and Social Policy* 477; P. van Duyne, J. Harvey, and L. Gelemerova, *The Critical Handbook of Money Laundering: Policy, Analysis and Myths* (London: Palgrave Macmillan, 2018).

¹⁰ In the AML context, it is increasingly recognised that private actors 'are not only responsible for implementing AML rules but also affect the content of governance'. See E. Tsingou, 'New Governors on the Block: The Rise of Anti-Money Laundering Professionals' (2018) 69 *Crime, Law and Social Change* 191. Moreover, there have been some concerns that regulators have adopted a light-touch approach in supervision and enforcement (though contrast recent activity, partly as a response to such criticism and concerns regarding the property sector: HMRC, *Estate agents targeted in money laundering crackdown* (March, 2019)). While it is important that policymakers and regulators do take into consideration the experiences of regulatees, not least to ensure legitimacy of the AML regime, the views of such actors ought not necessarily be determinative.

Contextualising AML in the Real Estate Sector

AML regulations have been in force for over three decades, yet there is still scepticism as to such efforts and their success. The modern AML regime is widely considered to exist since the establishment of the Financial Action Task Force (FATF) in 1989,¹¹ and the issuing of the FATF 40 Recommendations a year later.¹² In 1991, the EU issued its First Money Laundering Directive (MLD),¹³ choosing a twin-track approach based on criminalisation and prevention of money laundering. When the Second MLD was adopted in 2001,¹⁴ AML obligations were extended beyond credit and financial institutions to non-financial businesses and professions. In particular, Article 1 of the Second MLD also included auditors, external accountants and tax advisors; real estate agents; notaries and other independent legal professionals (in defined circumstances); high-value dealers; and casinos.¹⁵ These obligations encompassed carrying out customer due diligence (CDD) and know-your-customer (KYC) checks. Further, there are obligations to file suspicious activity reports (SARs) in certain circumstances.

Two decades on from the extension of the AML regime to estate agents (EAs), there continue to be developments. At various times, AML efforts have been driven by the fight against drugs and organised crime (more generally), but also by anti-corruption and anti-terrorism plans (particularly after 9/11). For example, the global anti-kleptocracy agenda¹⁶ has resulted in significant advancements, particularly amongst developed jurisdictions. As Sharman argues,

Although many more corrupt leaders get away with their crimes than face justice, the rise of the expectation from shortly after the turn of the century that host countries have a duty to take action to block or seize their illicit funds is a new and in many ways remarkable development.¹⁷

¹¹ G7, *Economic Declaration*, Paris Summit (16 July 1989), para 53. Examples of earlier AML efforts include, *inter alia*, the US Money Laundering Control Act 1986; the Vienna Convention 1988; and the Basel Committee, *Prevention of Criminal Use of the Banking System for the Purpose of Money-Laundering* (December 1988).

¹² These Recommendations were subsequently revised, and their current form is: FATF, *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation* (2012-2020).

¹³ European Council, Council Directive of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering, 91/308/EEC, OJEC L166/77, 28 June 1991.

¹⁴ Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering, OJ L344/76, 28 December 2001.

¹⁵ The list of regulated sectors continues to expand. For example, the Fifth MLD extends AML obligations to, *inter alia*, letting agents, art dealers, providers engaged in exchange services between virtual and fiat currencies, and custodian wallet providers. See Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, OJ L156/43, 19 June 2018, Art 1.

¹⁶ See, for example, UN Office on Drugs and Crime, United Nations Convention against Corruption, UN GA Res 58/4, 31 October 2003, entered into force 14 December 2005.

¹⁷ J. Sharman, *The Despot's Guide to Wealth Management: On the International Campaign against Grand Corruption* (Ithaca: Cornell University Press, 2017) 6-7.

Confronting the question as to why focus on developed jurisdictions (such as the UK), rather than on countries that are the source of corruption, Sharman states: ‘The best guess is that the bigger the financial center, the more dirty money flows through it, including the proceeds of foreign corruption’.¹⁸ Therefore, it is axiomatic that any attempt to tackle grand corruption cannot merely focus on the source, but must also encompass destination (or ‘host’) countries.

The anti-corruption agenda is strikingly evident in recent AML developments. For example, at the 2016 Anti-Corruption Summit, the then-UK Prime Minister called for a global movement to tackle illicit financial outflows, in his words the problem of ‘people stealing from poor countries and hiding that wealth in rich ones’.¹⁹ He specifically identified the property market as a problematic sector, saying that the UK should ‘clean up our property market and show that there is no home for the corrupt in Britain’.²⁰ His comments followed claims that at least £100 billion is laundered through the UK every year,²¹ and that corrupt capital is widely used to buy property in the UK.²² The same year, the Home Affairs Select Committee on the *Proceeds of Crime* suggested that ‘supervision of the property market is totally inadequate, and that poor enforcement has laid out a welcome mat for money launderers’.²³

More recently, there have been notable legal and policy responses to address, *inter alia*, money laundering in the UK property market. These include the expansion of the ‘Flag It Up’ campaign to the property sector;²⁴ the enactment of unexplained wealth orders (UWOs);²⁵ the introduction of new Money Laundering Regulations (ML Regs);²⁶ a greater focus on professional enablers;²⁷ and updates to the People of Significant Control (PSC) Register.²⁸ Clearly, significant efforts are being undertaken to tackle

¹⁸ *ibid*, 17.

¹⁹ D. Cameron, Anti-Corruption Summit 2016: PM’s Closing Remarks (12 May 2016) at <https://www.gov.uk/government/speeches/anti-corruption-summit-2016-pms-closing-remarks> (last accessed 8 May 2020).

²⁰ *ibid*.

²¹ Home Affairs Select Committee, *Proceeds of Crime*, HC 25 (2016-17). This claim was based on figures suggested by Transparency International during oral evidence. However, it must be acknowledged that it is virtually impossible to identify precisely the extent of money laundering. See M. Levi, P. Reuter and T. Halliday, ‘Can the AML System Be Evaluated Without Better Data?’ (2018) 69 *Crime, Law and Social Change* 307.

²² Transparency International UK and Thomson Reuters, *London Property: A Top Destination for Money Launderers* (TI-UK, 2016).

²³ Home Affairs Select Committee, *Proceeds of Crime*, HC 25 (2016-17), para 61.

²⁴ Home Office, HM Revenue and Customs, and Ben Wallace MP, ‘Campaign to Prevent Properties Being Bought With Dirty Money’ (26 October 2018).

²⁵ Criminal Finances Act 2017, Part 1. For consideration of the first UWO, see *Hajiyeva v National Crime Agency* [2020] EWCA Civ 108.

²⁶ Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017; Money Laundering and Terrorist Financing (Amendment) Regulations 2019.

²⁷ See National Crime Agency, *Annual Plan 2018-19*, 12.

²⁸ Department for Business, Energy & Industrial Strategy, *Register of People with Significant Control: Guidance for Registered and Unregistered Companies, Societates Europaeae, Limited Liability Partnerships, and Eligible Scottish Partnerships* (Scottish Limited Partnerships and Scottish Qualifying Partnerships). Version 4 (June 2017).

money laundering in relation to the UK property market,²⁹ and similar efforts are being made in other jurisdictions (e.g. Australia, Canada, and the US).³⁰

The amount of money involved in property transactions and the inherent vulnerabilities of the real estate sector to money laundering have given rise to concerns that it is all too easy to launder money through property.³¹ In this sense, unsurprisingly the property market has been seen as a key area for AML regulation. This fact accords with the view that ‘the intersection of licit and illicit markets, and the dependence of illicit markets on the former, have invited regulatory intervention in furtherance of crime control’.³² Regulatory strategies cannot, however, be viewed in isolation: regulation ‘operates in a world where the law is imperfect, enforcement and compliance costly, resources limited, and the regulator has discretion’.³³ So, while the AML regime might have laudable objectives,³⁴ there are significant difficulties in its practical implementation. Furthermore, there has been criticism that the AML regime imposes onerous and uncertain obligations on private actors and that there is a lack of proper support for them by national agencies and institutions.³⁵ In the same sense, concerns have been expressed as to the fact that AML regulation has resulted in private actors engaging in de-risking (and de-banking) of customers.³⁶

Given this context, an extensive literature exists on AML, mainly focusing on the financial sector.³⁷ Moreover, as already recalled, international and national legislations have increasingly imposed obligations on different sectors and the actors involved in them, including lawyers, accountants and estate agents.³⁸ However, policymakers often overlook the practical difficulties in implementing AML regulation. Amidst concern as to the extent of and vulnerabilities to money laundering in the UK property market, this article focuses on the implementation of AML regulation in the UK real estate sector,

²⁹ See M. Harris, ‘Anti-Money Laundering and Property: The Government Has Upped the Ante’, *Estate Agent Today* (14 April 2018).

³⁰ See, for example, Austrac, *Strategic Analysis Brief: Money Laundering Through Real Estate* (Austrac, 2015); M. Maloney, T. Somerville, and B. Unger, *Combating Money Laundering in BC Real Estate* (Expert Panel on Money Laundering in BC Real Estate, 2019); Financial Crimes Enforcement Network, *News Release – FinCEN Reissues Real Estate Geographic Targeting Orders for 12 Metropolitan Areas* (15 May 2019).

³¹ Transparency International UK, *Faulty Towers: Understanding the Impact of Overseas Corruption on the London Property Market* (TI-UK, 2017).

³² P. Grabosky, ‘On the Interface of Criminal Justice and Regulation’ in H. Quirk, T. Seddon, and G. Smith (eds), *Regulation and Criminal Justice: Innovations in Policy and Research* (Cambridge: CUP, 2010) 83–84.

³³ C. Veljanovski, ‘Strategic Use of Regulation’ in R. Baldwin, M. Cave, and M. Lodge (eds), *The Oxford Handbook of Regulation* (Oxford: OUP, 2010) 87.

³⁴ However, in practice there is confusion as to the purpose of AML: see J. Ferwerda, ‘The Effectiveness of Anti-Money Laundering Policy: A Cost-Benefit Perspective’ in C. King, C. Walker, and J. Gurulé (eds), *The Palgrave Handbook of Criminal and Terrorism Financing Law* (London: Palgrave Macmillan, 2018).

³⁵ M. Bergstrom, K. Svedberg Helgesson, and U. Morth, ‘A New Role for For-Profit Actors? The Case of Anti-Money Laundering and Risk Management’ (2011) 49 *Journal of Common Market Studies* 1043.

³⁶ V. Ramachandran, M. Collin, and M. Juden, ‘De-Risking: An Unintended Negative Consequence of AML/CFT Regulation’ in C. King, C. Walker, and J. Gurulé (eds), *The Palgrave Handbook of Criminal and Terrorism Financing Law* (London: Palgrave Macmillan, 2018).

³⁷ See n 2 above.

³⁸ For instance, see K. Benson, *Lawyers and the Proceeds of Crime: The Facilitation of Money Laundering and its Control* (Oxon: Routledge, 2020); B. Unger and J. Ferwerda, *Money Laundering in the Real Estate Sector: Suspicious Properties* (Cheltenham: Edward Elgar, 2011).

examining the obligations imposed upon estate agents and their implementation in practice.

Methods

There is an extensive literature on regulation and compliance, traditionally looking at the perspective of regulators (and how they might ensure compliance³⁹) and regulatory failures.⁴⁰ A less investigated aspect is the conceptual ‘flipside’ of traditional regulatory studies,⁴¹ namely ‘how individuals within organizations who enact compliance day-to-day actually interpret and respond to regulation’.⁴² However, there is increased realisation of the learning value gained from the experiences of private actors in the implementation of regulation in practice, considering the pressing issues affecting compliance. Indeed, compliance is ‘fundamentally linked with the social and structural contexts of individual compliance agents’.⁴³ In the context of AML, an example of this is Iafolla’s research on how bank employees exercise discretion in deciding whether a particular transaction is ‘risky’.⁴⁴ With this research, she demonstrates how personally-held ideas can influence the decision of whether to report a transaction to the compliance department.⁴⁵ Similarly, in analysing the views of money laundering compliance officers, Verhage shows how compliance ‘remains a battle between commercial interests on the one hand, and rule observance on the other’,⁴⁶ and it does not necessarily aim at preventing money laundering risks.⁴⁷

By focusing on the UK real estate sector, this article offers new insights into the operation of AML. There are advantages to looking at AML compliance from the perspective of the regulated. Indeed, EAs can offer practical insights and suggestions for improving the AML regime. However, it should be recognised that the narratives presented here must be approached critically. Indeed, there is a widely portrayed view of EAs as self-interested actors who will do anything for their own benefit and who must be

³⁹ A classic example is the regulatory pyramid: I. Ayres and J. Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (New York: OUP, 1992). See also H.E. Jackson, ‘Variation in the Intensity of Financial Regulation: Preliminary Evidence and Potential Implications’ (2007) 24 *Yale Journal on Regulation* 253.

⁴⁰ See, for example, S.L. Schwarz, ‘Protecting Financial Markets: Lessons from the Subprime Mortgage Meltdown’ (2008) 93 *Minnesota Law Review* 373.

⁴¹ Though there are notable exceptions such as C. Parker and V. Lehmann Nielson, ‘Do Businesses Take Compliance Systems Seriously – An Empirical Study of the Implementation of Trade Practices Compliance Systems in Australia’ (2006) 30 *Melbourne University Law Review* 441.

⁴² G.C. Gray and S.S. Silbey, ‘The Other Side of the Compliance Relationship’ in C. Parker and V. Lehmann Nielsen (eds), *Explaining Compliance: Business Responses to Regulation* (Cheltenham: Edward Elgar, 2011) 123.

⁴³ *ibid.*, 127.

⁴⁴ V. Iafolla, ‘The Production of Suspicion in Retail Banking: An Examination of Unusual Transaction Reporting’ in C. King, C. Walker, and J. Gurulé (eds), *The Palgrave Handbook of Criminal and Terrorism Financing Law* (London: Palgrave Macmillan, 2018).

⁴⁵ *ibid.* For consideration of profiling and SARs in the context of counter-terrorism finance, see N. Ryder and U. Turksen, ‘Banks in defence of the homeland: Nexus of ethics and suspicious activity reporting’ (2013) 12 *Contemporary Issues in Law* 311.

⁴⁶ n 2 above, 68.

⁴⁷ *ibid.*

held accountable.⁴⁸ Almost invariably, such reports reinforce views that there are weaknesses in regulation, such as the AML regime, and that more needs to be done. Nonetheless, it is essential to consider grievances expressed by EAs (and other private actors) as to the practical difficulties involved in AML compliance. Indeed, ‘Ignoring an individual’s grievances or concerns is unlikely to foster a sense that the authority has used procedural justice’.⁴⁹ Moreover, private actors are more likely to comply where they feel that they are treated fairly in the operation of the AML regime.⁵⁰

This article employs a mixed methodology that includes doctrinal and empirical research. In particular, the article presents an analysis of the existing UK AML legislation and relevant policies alongside a critical examination of qualitative data. In this regard, seventeen semi-structured interviews were conducted with EAs and compliance officials.⁵¹ To ensure diverse perspectives, we contacted a range of potential participants, from large, multi-office agencies to smaller local agencies, including both buying and selling agents. We recognise that seventeen interviews are not generalisable to the entire industry, however, alongside the caveats mentioned below, this number did enable us to gain some practical insight into the operation of AML obligations by private actors who are seen as ‘the first line of defence’.⁵² The interviews lasted an average of one hour. Twelve interviews were audio-recorded and transcribed, while for the other five interviews, the interviewer took detailed notes. The interviews’ content was subsequently analysed using NVIVO, focusing on both specific aspects peculiar to each interview and shared key themes that emerged from the whole sample of interviews.⁵³

We deliberately decided not to interview law enforcement officials or regulators for this project,⁵⁴ as the focus was on the perspectives of those subject to regulation and how they apply AML rules. Two further caveats must be acknowledged: access and bias/validity.⁵⁵ First, it was not entirely straightforward to gain access to potential interviewees. While contact details of estate agencies are available online, the topic of

⁴⁸ For recent media reports related to money laundering, see BBC News, ‘Countrywide Fined £215,000 Over Money-Laundering Failings’ (4 March 2019); J. Evans, ‘UK Estate Agents Hit by Crackdown on Money Laundering’, *Financial Times* (9 March 2019).

⁴⁹ K. Murphy, ‘Procedural Justice and Its Role in Promoting Voluntary Compliance’ in P. Drahos (ed), *Regulatory Theory: Foundations and Applications* (Acton: ANU Press, 2017) 47.

⁵⁰ T.R. Tyler, ‘Procedural Justice, Legitimacy, and the Effective Rule of Law’ (2003) 30 *Crime & Justice* 283.

⁵¹ Ethical approval was granted by the University of Sussex (reference: ER/CK298/3).

⁵² Home Office and HM Treasury, *Action Plan for Anti-Money Laundering and Counter-Terrorist Finance* (April 2016) 12.

⁵³ A number of themes arose in this analysis, including money laundering red flags; awareness and understanding of AML obligations; implementation and compliance; specific activities of real estate professionals; opinions on the AML regime; views of, and engagement with, regulators and law enforcement; and emerging issues (e.g. Brexit; cryptocurrencies). For discussion of some of these themes not covered in this article, see I. Zavoli and C. King, ‘Preventive AML in the UK property market: inside views from the sector’ in P. van Duyne et al (eds), *Criminal defiance in Europe and beyond: From organised crime to crime-terror nexus* (Eleven International Publishing, 2020); I. Zavoli, ‘The use of cryptocurrency in the UK real estate market: An assessment of money laundering risks’ in K. Benson et al (eds), *Assets, Crime and the State: Innovations in 21st Century Legal Responses* (Oxon: Routledge, 2020).

⁵⁴ However, these backgrounds are represented on our Advisory Board. The Advisory Board consisted of an investigator in the National Crime Agency; a financial intelligence officer in the Metropolitan Police; a barrister; an official in an NGO; and a senior (international) academic.

⁵⁵ For wider discussion, see N. Golafshani, ‘Understanding Reliability and Validity in Qualitative Research’ (2003) 8 *The Qualitative Report* 597.

AML-research tends to arouse suspicion. Some agencies that we contacted did not respond to our emails, while others responded but declined to take part.⁵⁶ Second, the fact that a particular agent did/did not participate in this study does not imply that they are/are not compliant with AML obligations. In this regard, it must be recognised that where a particular individual is knowingly involved in ML, then that person would be unlikely to be willing to participate in this study.

Regulation of estate agents and the UK anti-money laundering framework

There are many reasons why regulation in a particular sector or profession might be desirable.⁵⁷ For example, where a situation calls for skill or expertise in dealing with a task, then insistence upon a certain standard of skill might be necessary. The medical profession is an obvious example: it makes sense to regulate the profession to ensure high standards and quality of care for patients. On the other hand, there are also reasons not to require regulation, such as, for instance, entry restrictions into a sector or increased costs. Debates as to the regulation of EAs⁵⁸ (or ‘estate agency work’, which is the term used in the Estate Agents Act 1979) have been ongoing for quite some time, and they have demonstrated motivations of regulatory capture, public interest, and/or asymmetric information.⁵⁹ Nowadays, EAs are subject to a myriad of regulations⁶⁰ (although some still describe this sector as a ‘Wild West’ habited by ‘rogues’⁶¹).

One aspect of regulation that is particularly relevant for the work of EAs is AML. As noted earlier, there is a significant focus on the property market as a destination for

⁵⁶ For example, a typical reply would come from a PA saying: ‘I have spoken with XXX regarding your request and regretfully he is unable to participate at this time but thanks you for your interest in our company.’ Others replied directly to say, for example, ‘Thank you for contacting me but unfortunately I do not have the time to commit to this interview.’; or ‘Over the years I have spent many hours participating in government surveys and my experience has been that they listen politely but do not take any notice whatsoever. As a consequence, I have stopped participating - Sorry’.

⁵⁷ For consideration of what ‘regulation’ is, see J. Black, ‘Critical Reflections on Regulation’ (2002) 27 *Australian Journal of Legal Philosophy* 1; B. Orbach, ‘What is Regulation?’ (2012) 30 *Yale Journal on Regulation Online* 1.

⁵⁸ For recent review, see Regulation of Property Agents Working Group, *Final Report* (July 2019) 11. Chair: Lord Best.

⁵⁹ For consideration of historical efforts, see M. Latham, ‘“A Fraud, a Drunkard, and a Worthless Scamp”: Estate Agents, Regulation, and Realtors in the Interwar Period’ (2017) 59 *Business History* 690; P. Shears, ‘Hang Your Shingle and Carry On: Estate Agents – The Unlicensed UK Profession’ (2009) 27 *Property Management* 191. For wider consideration of motivation and regulation, see M. Law and S. Kim, ‘Specialization and Regulation: The Rise of Professionals and the Emergence of Occupational Licensing Regulation’ (2005) 65 *Journal of Economic History* 723.

⁶⁰ See, for example, Estate Agents Act 1979; there is also other legislation not specific to estate agents, but which is applicable, such as the Consumer Protection from Unfair Trading Regulations 2008. A further avenue of regulation is industry self-regulation, for example through the various representative bodies (such as NAEA Propertymark (the National Association of Estate Agents)), though ‘it is not clear that there is an effective self-regulatory system for the sector as a whole’. Regulation of Property Agents Working Group, *Final Report* (July 2019) 11. Chair: Lord Best.

⁶¹ BBC News, ‘Government to Crack Down on ‘Rogue’ Estate Agents’ (8 April 2018); M. Hunt, ‘Got an Issue with Your Rogue Estate Agent or Letting Agent? Here’s How You Can Claim compensation’, *The Telegraph* (20 November 2019).

laundering criminal proceeds.⁶² Here, public interest aspects of regulation are strikingly evident. For example, it can be argued that EAs are at the front line and are well-positioned to contribute to AML efforts; EAs are under a moral obligation to do so; and the importance of AML justifies the imposition of legal obligations. Such arguments are prevalent and indeed are also extended to other sectors.⁶³ This article thus considers the perspective from the other side,⁶⁴ to examine practical obstacles to the implementation of AML in practice. Before considering the empirical findings of this study, it is important to recall some aspects of the applicable AML regime that will also be critical for the analysis of our data.

The UK AML regime encompasses both a repressive (i.e. criminal law) and a preventive approach.⁶⁵ The key criminal law legislation today is the Proceeds of Crime Act 2002 (POCA).⁶⁶ The principal money laundering offences are: concealing, disguising, converting, transferring or removing from the jurisdiction criminal property;⁶⁷ entering into or becoming concerned in an arrangement which she knows or suspects facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person;⁶⁸ and acquiring, using, or having possession of criminal property.⁶⁹ In addition, there are secondary offences concerned with ‘failing to disclose’ and ‘tipping off’.⁷⁰ Alongside POCA, another important piece of legislation is the ML Regs 2017.⁷¹ These Regulations contain key provisions concerning the AML regime, including: identifying the ‘relevant persons’ that the Regulations apply to;⁷² specifying risk assessment steps and policies, controls and procedures that must be taken or put in place by ‘relevant persons’;⁷³ providing for training requirements;⁷⁴ requiring customer due diligence (CDD) measures;⁷⁵ and providing for reliance on third-party CDD checks⁷⁶ as well as for maintaining records.⁷⁷ There are also specific provisions concerning supervision and registration;⁷⁸ information gathering and investigatory powers;⁷⁹ and enforcement.⁸⁰

⁶² See n 21 above.

⁶³ S. Hufnagel and C. King, ‘Anti-Money Laundering Regulation and the Art Market’ (2020) 40 *Legal Studies* 131.

⁶⁴ See n 41 above.

⁶⁵ G. Stessens, *Money Laundering: A New International Law Enforcement Model* (Cambridge: CUP, 2000) 108.

⁶⁶ Earlier legislation also dealt with money laundering. For example, the Criminal Justice Act 1988, Part VI. On the historical development, see *R v Montila* [2004] UKHL 50.

⁶⁷ POCA, s 327. S 340 defines ‘criminal property’.

⁶⁸ POCA, s 328.

⁶⁹ POCA, s 329.

⁷⁰ POCA, ss 330-333.

⁷¹ Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017. The ‘relevant persons’ subject to the Regulations are set out in Reg 8. The supervisory authority for estate agency businesses is HM Revenue and Customs (HMRC).

⁷² ML Regs, Part 2. Estate agents are specifically identified in Regs.8(2)(f) and 13.

⁷³ ML Regs, Regs 18-21.

⁷⁴ ML Regs, Reg 24.

⁷⁵ ML Regs, Part 3.

⁷⁶ ML Regs, Reg 39.

⁷⁷ ML Regs, Reg 40.

⁷⁸ ML Regs, Part 6.

⁷⁹ ML Regs, Part 8.

⁸⁰ ML Regs, Part 9.

As previously indicated, the objective of this article is to examine how the AML regime operates in practice, informed by experiences of estate agents and compliance officials. This focus is deliberate: in recent years, there has been significant policy discourse emphasising the role of professional enablers or gatekeepers in facilitating money laundering. For example, the 2017 UK National Risk Assessment (NRA) noted the threat of money launderers ‘exploiting UK and overseas financial and professional services industries’.⁸¹ Specifically, in relation to EAs, the NRA identified key risks such as being used to help buy and sell property to launder criminal funds; complicit agents helping criminals buy or sell property; perceived low understanding of risks in the sector, and low compliance with the ML Regs.⁸² The FATF expressed similar sentiments in its 2018 Evaluation: ‘Estate agent businesses do not have a significant understanding of their risks or how to effectively mitigate them’,⁸³ although it did also note that compliance standards have improved.⁸⁴

When examining the UK AML framework, a key aspect that emerges is the role of and the function attributed to private actors. Indeed, alongside other private actors, estate agents have been enlisted in ‘policing’ activities (specifically ‘following-the-money’ strategies to tackle crime).⁸⁵ This is particularly evident in the AML context, where private actors are expected to conduct checks on their clients and to report suspicions to law enforcement agencies.⁸⁶ For many, AML requirements are seen as a form of government outsourcing of regulatory responsibility,⁸⁷ or, as the UK AML/CTF Action Plan puts it, the private sector is ‘the first line of defence’.⁸⁸ Thus, the rest of this article examines how this ‘first line of defence’ operates in practice, from the perspective of those doing AML.

Customer Due Diligence

Doing CDD

The role of private actors is starkly evidenced in obligations to conduct CDD checks and to report any suspicions (concerning customers or specific transactions) to the authorities.

⁸¹ HM Treasury and Home Office, *National Risk Assessment of Money Laundering and Terrorist Financing* 2017 (October 2017) 19.

⁸² *ibid.*, 54.

⁸³ FATF, *Anti-Money Laundering and Counter-Terrorist Financing Measures - United Kingdom, Mutual Evaluation Report* (December 2018) para 288.

⁸⁴ *ibid.*, para 312.

⁸⁵ On such responsabilisation of private actors, see P. O'Malley and D. Palmer, ‘Post-Keynesian Policing’ (1996) 25 *Economy and Society* 137; D. Garland, *The Culture of Control: Crime and Social Order in Contemporary Society* (Oxford: OUP, 2001) 126; G.C. Gray, ‘The Responsibilization Strategy of Health and Safety: Neo-liberalism and the Reconfiguration of Individual Responsibility for Risk’ (2009) 49 *British Journal of Criminology* 326.

⁸⁶ See M. Egan, ‘The Role of the Regulated Sector in the UK Anti-Money Laundering Framework: Pushing the Boundaries of the Private Police’ (2010) 6 *Journal of Contemporary European Research* 272, 285 who contends that ‘the implementation of AML measures by the regulated sector increases the amount of intelligence available to policing agencies and thereby assists the public police in making appropriate operational choices’.

⁸⁷ See n 2 above, 79-80.

⁸⁸ Home Office and HM Treasury, *Action Plan for Anti-Money Laundering and Counter-Terrorist Finance* (April 2016) 12.

For example, where a relevant person is required to conduct CDD checks,⁸⁹ the obligations are to:

- (a) identify the customer unless the identity of that customer is known to, and has been verified by, the relevant person;
- (b) verify the customer's identity unless the customer's identity has already been verified by the relevant person; and
- (c) assess, and where appropriate obtain information on, the purpose and intended nature of the business relationship or occasional transaction.⁹⁰

In addition, the relevant person must conduct ongoing monitoring of a business relationship, including scrutiny of transactions and undertaking reviews of records and keeping documentation up-to-date.⁹¹ Thus, this level of scrutiny can change the relationship between the company and its clients, with a shift from 'trust' to 'suspicion'⁹² and with potential client alienation.⁹³

As a consequence, it is unsurprising that CDD requirements impact EAs' practice and their business. Our data shows that there was some disquiet among EAs about asking for relevant documentation from people that they know well, sometimes for many years.⁹⁴ To avoid jeopardising their business, some interviewees referred to methods they adopted to balance the need for checks with the maintenance of a trustworthy relationship with their clients. For instance, one EA spoke of exercising discretion to use a more light-touch approach (or simplified due diligence) where, for example, 'the lady is 92 and we've got evidence of the fact she's lived in that house for 42 years'.⁹⁵ Another interviewee stated that they still go through relevant checks with someone that they have known, personally or professionally, for many years, but that this person would be 'in a different category' and would not set off alarm bells.⁹⁶ Moreover, even when EAs require more details on a customer, alternative approaches are used. For instance, some interviewees spoke about the use of internet searches and LinkedIn (and even Facebook) to find further information.⁹⁷ Thus, EAs appear to adopt a pragmatic, indeed flexible, approach depending on the circumstances of particular situations.

Nonetheless, it was stressed that CDD must still be done,⁹⁸ and that legitimate buyers would usually do their utmost to provide all requested information.⁹⁹ In this regard, some EAs mentioned the fact that the prevalence of CDD checks nowadays means that most people understand that AML checks are being carried out and that some clients (e.g. those who work in financial services) might consider it peculiar if they were not asked

⁸⁹ As provided for by ML Regs, Reg 27(1).

⁹⁰ ML Regs, Reg 28(2).

⁹¹ ML Regs, Reg 28(11).

⁹² n 34 above, 1050.

⁹³ M. Gill and G. Taylor, 'Preventing Money Laundering or Obstructing Business? Financial Companies' Perspectives on "Know Your Customer" Procedures' (2004) 44 *British Journal of Criminology* 582, 587.

⁹⁴ eg Interview 14.

⁹⁵ Interview 1.

⁹⁶ Interview 2.

⁹⁷ eg Interviews 3; 12.

⁹⁸ eg Interview 2.

⁹⁹ eg Interview 3.

for relevant documentation.¹⁰⁰ However, difficulties might arise in doing CDD checks, especially with specific categories of customers, like foreign buyers. Indeed, some interviewees mentioned difficulties with doing CDD checks on foreign buyers, for example, because there might be no face-to-face contact.¹⁰¹ A related difficulty is where documentation might be fake: 'It is absurd to put the obligation on estate agents to check whether a passport is fake. What if it is Russian and it is in Cyrillic'.¹⁰² Therefore, EAs seem to be placed in a position of vulnerability¹⁰³ because they are required to conduct CDD checks but are confronted with significant practical obstacles to compliance. Practical obstacles were a recurring theme in this research; while many participants expressed positive support for the AML regime, such support is impacted by its operation in practice, and the expectations imposed on private actors. Not only do practical obstacles make it more challenging to comply with legal obligations, there are additional costs, and also opportunity costs, for businesses (as will be discussed in later sections).

One particular difficulty relates not necessarily to a person's identity or proof of funds, but rather to the source of funds.¹⁰⁴ By definition, a money launderer would have money available to launder. Thus, it will often require a judgement call by EAs:

Often they'll see a bank statement which has got a couple million quid in it, but of course there's no evidence to suggest where that money came from. It may have gone in 5 minutes before you saw it, it might go out 5 minutes afterwards. It's really building up a picture, carrying out a risk assessment as to whether this person you're dealing with, you think they are likely to have 2 million legitimate pounds in their pocket and that of course is a judgment call.¹⁰⁵

This focus on making judgement calls aligns with previous research conducted by Gill and Taylor. They state that regulated companies have to assess the evidence available to them and to make 'a very difficult judgment' (especially in the context of financially excluded individuals).¹⁰⁶ Moreover, as Gelemerova notes, judgement calls are inherently subjective and often involve considerations of striking a balance, as part of a risk assessment/ risk management approach.¹⁰⁷ Furthermore, the judgement can be influenced by broader considerations, like the perception of a person as 'out of place' in a particular transaction.¹⁰⁸ This multifaceted sway is particularly important in the context of risk-management, given the potential for false positives (i.e. wrongly identifying a risk and acting upon that) and false negatives (i.e. failing to identify a risk and failing to take

¹⁰⁰ eg Interviews 8; 14.

¹⁰¹ eg Interview 1.

¹⁰² Interview 6.

¹⁰³ See M. Albertson Fineman, 'The Vulnerable Subject and the Responsive State' (2010) 60 *Emory Law Journal* 251.

¹⁰⁴ eg Interviews 3; 9.

¹⁰⁵ Interview 3.

¹⁰⁶ n 92 above, 588.

¹⁰⁷ L. Gelemerova, 'On the frontline against money-laundering: the regulatory minefield' (2008) 52 *Crime, Law and Social Change* 33, 47.

¹⁰⁸ M. Levi, 'Money for Crime and Money From Crime: Financing Crime and Laundering Crime Proceeds' (2015) 21 *European Journal on Criminal Policy and Research* 275.

appropriate action).¹⁰⁹ Moreover, the costs of a wrong judgment call can be significant: losing commission on, say, a £2 million transaction (as alluded to in the above quote) in the case of a false positive, or being caught up in a money laundering investigation and/or media scandal in the case of a false negative.

Finally, amongst our interviewees a significant criticism of how CDD operates concerns the doubling- or tripling-up of checks - for example, CDD being done by a bank, a solicitor, and an EA,¹¹⁰ costing time and money every time. As suggested by some interviewees, if there were a central place (or process) for AML checks, that would reduce the cost for clients.¹¹¹ However, there are practical difficulties with such a suggestion, for example, in relation to privacy and security concerns.

CDD in practice: Politically Exposed Persons

A PEP is an individual who is (or has been) entrusted with a prominent public function.¹¹² Given this status, there is the possibility of abuse of position. Indeed, there are many situations where government officials, or their families and associates, have engaged in corruption. Notable examples include the Marcos family in the Philippines and the Abacha family in Nigeria.¹¹³ In many instances, PEPs (whether foreign or domestic) will try to launder their corrupt proceeds.¹¹⁴ Thus, AML requirements are regarded as playing an important role to tackle these criminal activities, and the operation of such obligations, such as CDD checks, offers interesting insights into practical realities.

Of course, the mere fact that a person is a PEP does not necessarily mean that that person is engaged in criminal activities, nor should it automatically arouse suspicion. As a precaution, however, the AML regime provides for specific guidelines and principles that apply when EAs enter into a business relationship with PEPs. As the FATF Guidance points out,

When considering whether to establish or continue a business relationship with a PEP, the focus should be on the level of ML/TF risk associated with the particular PEP, and whether the financial institution or DNFBP has adequate controls in place to mitigate that ML/TF risk so as to avoid the institution from being abused for illicit purposes should the PEP be involved in criminal activity.¹¹⁵

Under the UK ML Regs 2017, a ‘relevant person’ must apply enhanced CDD checks and enhanced ongoing monitoring when dealing with PEPs (or family or known close associates).¹¹⁶ For example, Regulation 35(3) requires an assessment of ‘(a) the level of risk associated with that customer, and (b) the extent of the enhanced customer due diligence measures to be applied in relation to that customer’.

¹⁰⁹ R. Ericson, ‘Ten Uncertainties of Risk-Management Approaches to Security’ (2006) 48 *Canadian Journal of Criminology and Criminal Justice* 345, 348.

¹¹⁰ eg Interviews 4; 11; 12; 13.

¹¹¹ eg Interview 9.

¹¹² FATF, *FATF Guidance: Politically Exposed Persons (Recommendations 12 and 22)* (June 2013) 3.

¹¹³ For discussion of kleptocracy, see n 16 above.

¹¹⁴ For wider consideration, see FATF, *Laundering the Proceeds of Corruption* (July 2011).

¹¹⁵ n 111 above, 7.

¹¹⁶ See ML Regs, Regs 33 and 35.

An obvious point in this regard is whether a PEP is identified as such by private actors.¹¹⁷ In our study, difficulties in identifying someone as a PEP were noted. For example, it was suggested that a person involved in bribery or corruption in a developing country is unlikely to be forthcoming with their role as, say, a judge or senior civil servant.¹¹⁸ Indeed, there was scorn for the oft-asserted view (for example in training courses) that the best way to identify a PEP is to ask them: ‘Well, if I’m a dodgy PEP who’s using bribery from my Russian foreign deal, am I really gonna say, “Yeah, I’m a PEP”’.¹¹⁹ Given the requirements of enhanced CDD and monitoring of PEPs, it is essential that EAs can identify such a person. Difficulties in this area were aptly summed up by one interviewee when discussing a lack of AML compliance:

I don’t think it’s from much around customer due diligence, it’s around that understanding of the PEPs and the financial sanctions, and I think it’s a case of if you went in and started a talk to a negotiator on the front desk and said to them, “Explain to me what a PEP is. Explain to me when you look at financial sanctions”. I don’t know whether they could really, fully, go into those details as to what they’re looking for. I think they all have a really, really good understanding of, “I need to confirm somebody’s identity and where they live”, I think it’s the other ancillary bits to the money laundering regulations.¹²⁰

Similarly, another interviewee stated: ‘PEP is something that the majority of the industry don’t understand and don’t know how to deal with’.¹²¹ The issue here relates not to the legislation itself, but to its operation in practice. If regulated actors are unable to identify those individuals where enhanced checks ought to be conducted, then – irrespective of what is specified in legislation – there will be a lacuna in practice.

To mitigate the risks associated with a transaction involving a PEP, some EAs have adopted the approach of automatically conducting enhanced checks where they think that someone is involved in politics (whether in the UK or abroad).¹²² Risk management is thus evident; however, such a blanket approach is an example of regulatory over-compliance. In other words, when faced with uncertainty, regulated actors are going beyond the requirements of the AML regime to manage the risks involved.¹²³ This then runs counter to the risk-based approach and is reminiscent of a rules-based approach whereby secondary risk management strategies are adopted as additional protection by regulated actors.¹²⁴ Some interviewees mentioned certain nationalities and how their behaviour can be confusing, but then stated that that might simply be ‘a cultural thing’.¹²⁵ A difficulty in practice, though, is that individual

¹¹⁷ On the challenges of identification, see Z. Miltina et al, ‘Model for Identification of Politically Exposed Persons’ in B. Johansson et al (eds), *Perspectives in Business Informatics Research* (Cham: Springer, 2017).

¹¹⁸ eg Interview 1.

¹¹⁹ Interview 9.

¹²⁰ Interview 13.

¹²¹ Interview 9.

¹²² eg Interview 1.

¹²³ For similar argument in the context of financial institutions, see E. Tsingou, ‘New Governors on the Block: The Rise of Anti-Money Laundering Professionals’ (2018) 69 *Crime, Law and Social Change* 191.

¹²⁴ M. Power, ‘The Risk Management of Everything’ (2004) 5 *Journal of Risk Finance* 58.

¹²⁵ Interview 14.

(mis)conceptions as to what is *normal* or *unusual* can influence how AML rules are applied in practice. As Iafolla points out in the context of the banking sector, ‘clients who do not conform to preconceived social roles may be viewed with increased suspicion and subject to further risk analysis and scrutiny, whether or not their transactions are legitimate’.¹²⁶

In contrast to efforts where PEPs themselves are involved in a transaction, some interviewees expressed disquiet about doing AML checks on PEP family members,¹²⁷ even though such reluctance runs counter to perceptions of vulnerability to ML.¹²⁸ This is a significant finding given that perceptions of legitimacy can influence compliance; as Valerie Braithwaite points out in her research on tax compliance, ‘compliance may be thought of as framing the analysis of how authorities might go about eliciting public cooperation within a regulatory field. Legitimacy is broader, framing the analysis of whether or not the existence of the regulatory field is justified’.¹²⁹ Given the emphasis on PEP family members and associates being involved in laundering proceeds of corruption,¹³⁰ the lack of *commitment*¹³¹ in relation to an apparent vulnerability for money laundering demonstrates that the legitimacy of the particular rules is questioned.

A further aspect of the operation of AML rules in the PEP context is third-party checks. Some EAs rely on outside companies (such as Experian and Smart Search) for AML checks against PEPs.¹³² The 2017 Regulations do permit reliance on third-party CDD checks, but they explicitly provide that: ‘notwithstanding the relevant person’s reliance on the third party, the relevant person remains liable for any failure to apply such measures’.¹³³ Curiously, some interviewees suggested that reliance on outside companies might absolve them of liability if anything goes wrong: ‘they take on the responsibility. So, if something slips through it’s on them not on us’¹³⁴ (reliance on third-party checks is discussed further in the next section).

From the data above, it seems that the operation of AML rules in practice is haphazard given a lack of clarity - not so much as to *what* is required (i.e. checking identity and address), but rather *when* the rules apply and *how* best to apply them. Given this context, then, it is unsurprising that - in their survey of MLROs - Gill and Taylor concluded that ‘A very clear majority of respondents felt that KYC procedures would not prevent money laundering by PEPs, either in the UK or abroad’.¹³⁵

¹²⁶ n 43 above, 101.

¹²⁷ eg Interview 13.

¹²⁸ See n 92 above, 589.

¹²⁹ V. Braithwaite, ‘Resistant and Dismissive Defiance Towards Tax Authorities’ in A. Crawford and A. Hucklesby (eds), *Legitimacy and Compliance in Criminal Justice* (New York and London: Routledge, 2012) 93.

¹³⁰ See FATF, *Laundering the Proceeds of Corruption* (July 2011).

¹³¹ As Braithwaite notes, commitment ‘conveys a belief that the regulatory purpose is sound and that the regulatory system should be valued and supported by everyone’. V. Braithwaite, ‘Resistant and Dismissive Defiance Towards Tax Authorities’ in A. Crawford and A. Hucklesby (eds), *Legitimacy and Compliance in Criminal Justice* (New York and London: Routledge, 2012) 97.

¹³² eg Interview 8.

¹³³ ML Regs, Reg 39(1).

¹³⁴ Interview 8.

¹³⁵ n 92 above, 589.

Reliance on third-party checks

A recurring issue in our interviews was whether EAs could rely on CDD checks by a third-party.¹³⁶ As already noted above, such third-party reliance is permitted under the Money Laundering Regulations.¹³⁷ Our empirical findings concerning this issue can be grouped into three approaches: 1. those that actively embrace the option and collaborate with trusted colleagues; 2. those that rely upon checks done by others as a means of absolving themselves; and 3. those that do not rely upon checks done by others out of an abundance of caution.

With the first approach above, some interviewees noted that they are relying upon checks done by others and that a group of different agencies have come together to set up a best practice forum.¹³⁸ It was said that they are willing to rely upon checks done by each other, but not information received from other agencies.¹³⁹ This fact lends support to the idea of a ‘club’ spirit, where competition is put aside, and a common approach is adopted against dirty money.¹⁴⁰ In other instances – the second approach - it emerged that some EAs attempt to rely upon checks by others as a way of relieving themselves of responsibility under the Money Laundering Regulations. One interviewee described a particular EA who has a standard form with a section for the conveyancer to complete to say that AML checks have been completed: ‘So, they were automatically trying to pass the buck without any dialogue at all, no knowledge of whether that conveyancer was solid themselves, anything like that’.¹⁴¹ This approach seems to confirm the idea that ‘much compliance is multifaceted’¹⁴² and, therefore, various (sometimes very different) reasons can drive compliance and the obliged subjects’ approaches to AML.¹⁴³ Thus, this second approach represents a middle-ground position between acting and non-acting, trust and suspect, where EAs’ compliance is driven by a formal fulfilment of their obligations rather than a direct commitment.¹⁴⁴ Other interviewees spoke about being careful to comply with AML rules, and that they have not yet had any concerns that prompted the filing of a SAR. One person argued that the reason for this is that she already knows many of her clients. If she did not know the person, and it involved ‘a top-end purchase’ then, she said, she would ‘ask them to be qualified by their lawyer or by their bank’.¹⁴⁵ She continued: ‘So, we sort of don’t really have a need to be concerned, ‘cause you sort of know who they are. And, you can Google them, and you can check them up on, you know, the internet, these days, so...’.¹⁴⁶ What is evident from this approach is a sense of self-

¹³⁶ To rely on checks by a third-party, that third-party must fall within the requirements specified in ML Regs, Reg 39(3).

¹³⁷ ML Regs, Reg 39.

¹³⁸ eg Interview 11.

¹³⁹ eg Interview 11.

¹⁴⁰ G. Favarel-Garrigues, T. Godefroy, and P. Lascoumes, ‘Reluctant Partners? Banks in the Fight Against Money Laundering and Terrorism Financing in France’ (2011) 42 *Security Dialogue* 179, 189.

¹⁴¹ Interview 9.

¹⁴² A. Bottoms, ‘Understanding Compliance with Laws and Regulations: A Mechanism-Based Approach’ in M. Krambia-Kapardis (ed), *Financial Compliance: Issues, Concerns and Future Directions* (Cham: Palgrave MacMillan, 2019) 32.

¹⁴³ *ibid.*

¹⁴⁴ On this ambivalence, see A. Verhage, ‘Between the Hammer and the Anvil? The Anti-Money Laundering-Complex and Its Interactions With the Compliance Industry’ (2009) 52 *Crime, Law and Social Change* 9, 23.

¹⁴⁵ Interview 12.

¹⁴⁶ Interview 12.

justification, particularly where there is ambiguity about the correct way to behave: ‘The greater the ambiguity of the situation, the more people will feel confident in their own ethicality’.¹⁴⁷ Finally, under the third approach, some interviewees noted that although the Regulations permit the use of third-party CDD checks, EAs remain liable if something goes wrong.¹⁴⁸ Therefore, they will not rely upon CDD checks by others on that basis.¹⁴⁹ In this regard, once again, we see evidence of regulatory over-compliance, whereby – to minimise risk – regulated actors are cautious in application of AML rules, instead preferring to strictly comply so as to maintain control and certainty.

Impact on business

Where regulation impacts upon businesses/individuals, it is unsurprising that regulatees might reflect upon how are impacted. In this study, interviewees reflected upon how AML obligations affect them. When discussing the implementation of CDD checks, for example, there was criticism of how AML can impact upon the sale process. Indeed, CDD checks can impact both customers and EAs negatively. For example, if an EA experiences a delay when doing AML checks upon a potential buyer, that impacts upon the transaction. So, the client is inconvenienced. Moreover, such delays might open up the possibility of another agent coming along with a different buyer and thus causing the initial agent to lose a sale.¹⁵⁰ In this sense, concerns were expressed that a firm that complies with AML requirements might be regarded as ‘kind of a pain for people to buy through’ simply because they do AML checks, thus putting those firms at a disadvantage compared to others that are not doing the same checks.¹⁵¹ Thus, there can potentially be a disincentive to compliance. Some sales EAs have tried to manage the risk of losing a transaction by doing AML checks at an early stage (before putting an offer to their client, the vendor).¹⁵² In other words, they pre-emptively conduct CDD checks to ensure that everything is in order so that, if the transaction does proceed, it reduces the risk of it collapsing at a later stage due to AML discrepancies.

It was noted that if an EA asks too many questions, then a person trying to launder money through that agency can simply withdraw with no consequences, by merely saying that they have changed their mind and no longer want to purchase the particular property.¹⁵³ Thus, the very act of asking questions and seeking to comply with AML obligations could impact an EA’s business, potentially making them less likely to comply. Indeed, an EA might well develop an unfavourable, or defiant, attitude towards AML obligations where those obligations impact their business, even where they are generally supportive of the aims of the AML regime.¹⁵⁴ That said, the risk management strategy noted earlier, namely conducting CDD checks at an early stage, allows for such instances

¹⁴⁷ Y. Feldman, *The Law of Good People: Challenging States’ Ability to Regulate Human Behavior* (Cambridge: CUP, 2018) 195. We thank Liz David-Barrett for this point on behavioural ethics.

¹⁴⁸ eg Interview 10: ‘whether you rely upon somebody else to do the CDD and then provide it to you, you still remain liable under the current regulations’. See ML Regs, Reg 39(1).

¹⁴⁹ eg Interview 8.

¹⁵⁰ eg Interview 12.

¹⁵¹ Interview 8. For wider consideration, see S. Shapiro and R. Rabinowitz, ‘Punishment Versus Cooperation in Regulatory Enforcement: A Case Study of OSHA’ (1997) 49 *Administrative Law Review* 713.

¹⁵² eg Interview 8.

¹⁵³ eg Interview 9.

¹⁵⁴ For wider discussion on defiance, see n 128 above.

to be weeded out. Such a strategy will not always work, however. For example, in previous studies, concerns have been expressed about the negative impact of AML requirements on one-off or time-sensitive products (e.g. stocks and shares).¹⁵⁵ In our research, similar misgivings were evident for some EAs. For example, there can be difficulties where there is pressure to exchange contracts quickly; in such instances, it might not be possible to conclude full AML checks before completion.¹⁵⁶ The EA is thus faced with a conundrum: comply and potentially lose a commission, or do not comply and risk prosecution.

Reporting suspicion

Process

The concept of ‘suspicion’ has been described as the ‘keystone’ of the AML regime, and it underpins the suspicious activity reports (SARs) process.¹⁵⁷ The obligation to report arises under POCA, which provides for ‘required disclosures’¹⁵⁸ and ‘authorised disclosures’.¹⁵⁹ In both instances, a failure to report can result in criminal prosecution. Authorised disclosures have an additional role in that they provide intelligence to law enforcement authorities. According to Donald Toon of the National Crime Agency (NCA), ‘the financial intelligence contained within SARs and UKFIU international requests enhances the intelligence picture against money laundering and all serious and organised crime threats’.¹⁶⁰ Such intelligence, however, stems from EAs doing ‘spying and detective work’¹⁶¹ or ‘being asked to be the eyes and ears of the State’.¹⁶² Some interviewees suggested that they do not have the skill nor expertise to carry out such a role. For example, it was said that checking identification documentation is fine, but investigating the source of funds involving overseas trusts might be beyond the understanding of EAs.¹⁶³ Moreover, obligations to report may undermine relationships of trust and confidentiality with a client.¹⁶⁴

From the foregoing, an important question arises as to how EAs approach decisions to file a report. Some interviewees spoke of different methods that they adopt, such as the ‘smell test’: if something appears ‘a little bit odd’ you should take a step back and ask whether that should be reported to the MLRO.¹⁶⁵ A traffic-lights system was also

¹⁵⁵ See n 92 above, 590.

¹⁵⁶ eg Interview 11.

¹⁵⁷ Law Commission, *Anti-Money Laundering: The SARs Regime* (HC 2098, June 2019), para 5.2. For consideration of suspicion, see *R v Da Silva* [2006] EWCA Crim 1654, paras 16-17.

¹⁵⁸ POCA, ss 330-332.

¹⁵⁹ POCA, ss 327-329.

¹⁶⁰ NCA, *Suspicious Activity Reports (SARs) Annual Report 2018*, ‘Statement by the Chair of the SARs Regime Committee’. See A. Verhage, ‘Great Expectations but Little Evidence: Policing Money Laundering’ (2017) 37 *International Journal of Sociology and Social Policy* 477, 480 where the AML reporting system is described as ‘a coalition of public and private partners involved in all-inclusive surveillance’.

¹⁶¹ Interview 12.

¹⁶² Interview 3.

¹⁶³ eg Interview 7.

¹⁶⁴ J. Ayling and P. Grabosky, ‘Policing by Command: Enhancing Law Enforcement Capacity through Coercion’ (2006) 28 *Law and Policy* 417, 426-427.

¹⁶⁵ eg Interview 1.

suggested: if everything is right, then it is green; if there is something wrong, but not a criminal offence (e.g. a form has not been completed correctly), then it is amber; and if something is a 'fail' under the ML Regs, then it is a red.¹⁶⁶ Filing SARs becomes, therefore, an activity which relies upon individual perceptions and choices, and there is no common approach. Not only does this result in a scattered and (possibly) inconsistent approach to potential suspicious activities, but it also emphasises different levels of experience and, therefore, capacity to detect and 'smell' such activities.

There is extensive literature that suggests that process-based regulation significantly influences people's reactions to their experiences with authorities.¹⁶⁷ It is useful, then, to consider EAs attitudes towards the SARs filing process. SARs are reported to the UK Financial Intelligence Unit (UKFIU), which is based within the NCA. Theoretically, filing a SAR ought to be relatively straightforward,¹⁶⁸ but our data suggests that this is not always the case. One criticism mounted against the SAR system concerned its design: it is a system designed for the banking sector, and it does not fit well into other sectors.¹⁶⁹ As one person succinctly puts it: 'It is cumbersome'.¹⁷⁰ Others suggested that even if there is some suspicion, it might not be possible to file a SAR as there is not enough information for that system to accept the SAR.¹⁷¹ There was also disapproval for the registration process and its complexity. Indeed, an EA has an HMRC 'gateway', but if they want to file a SAR, they must do that through the NCA portal, which is not linked to the HMRC gateway. As one interviewee puts it, 'it's more complicated than it need be. ... If I want to tip off the State, that I think something's dodgy going on, why not make it easy for me to do so?'.¹⁷² It was also suggested that it should be possible to submit SARs anonymously: 'If I think one of my competitors is up to no good, I might prefer to anonymously tip off the state ..., because I might not trust the state reassurances that I would receive anonymity anyway'.¹⁷³

Given the value attached to the quality of interpersonal treatment by authorities,¹⁷⁴ it is significant that there was a perception of not being supported by AML authorities when engaging with the SAR process. Concerning the support from the State, one participant stated: 'It wasn't terribly responsive. ... They didn't give me any advice. It was more like I'd ticked the box, that was the experience'.¹⁷⁵ Research in the banking sector demonstrates the importance of positive rapport and informal partnerships/

¹⁶⁶ eg Interview 1.

¹⁶⁷ See J. Braithwaite and T. Makkai, 'Trust and Compliance' (1994) 4 *Policing and Society* 1.

¹⁶⁸ A. Campbell and E. Campbell, 'Solicitors and Complying with the Anti-Money Laundering Framework: Reporting Suspicions, Applying for Consent and Tipping-Off' in N. Ryder, U. Turksen, and S. Hassler (eds), *Fighting Financial Crime in the Global Economic Crisis* (Oxon: Routledge, 2015). See also National Crime Agency, *Obtaining consent from the NCA under Part 7 of the Proceeds of Crime Act (POCA) 2002 or under Part 3 of the Terrorism Act (TACT) 2000* (October 2013).

¹⁶⁹ eg Interview 1.

¹⁷⁰ Interview 1.

¹⁷¹ eg Interview 4.

¹⁷² Interview 15.

¹⁷³ Interview 15.

¹⁷⁴ T.R. Tyler, 'Procedural Justice, Legitimacy, and the Effective Rule of Law' (2003) 30 *Crime & Justice* 283, 298.

¹⁷⁵ Interview 6.

engagement between (AML) regulated actors and law enforcement.¹⁷⁶ While the relationship between (major) banks and financial institutions in the UK might be more engaging (perhaps unsurprising given the percentage of SARs that they submit¹⁷⁷), other sectors do not necessarily experience the same support and engagement. In that regard, enhancing the process (and engagement therewith) may positively promote compliance.¹⁷⁸

Linked to the lack of support is the lack of feedback: there is (generally) a unidirectional flow of information. Such a lack of two-way engagement can affect how the process operates because, for example, private actors do not develop knowledge as to what works or what is useful.¹⁷⁹ A recurring issue in this study was whether EAs should receive any update on SARs submitted. As one interviewee stated: ‘It’s a bottomless pit and you never get anything out’.¹⁸⁰ That person went on to say that ‘it would be helpful to have feedback, to have pointers as to what to look for, because we are very much in the dark. We can’t even talk to anyone else about it because of tipping off concerns’.¹⁸¹ Others, however, thought that once a SAR is submitted, that is the end of the matter and there is no need to hear any more (unless the NCA asks for clarification).¹⁸²

Feedback loops can be important in ensuring proper functioning of regulation, though there can be obstacles in practice. For instance, in the AML context, providing general, anonymised feedback on all the SARs submitted in a particular year by a large bank - that submits a substantial number of SARs - might well be unproblematic (albeit time-consuming for law enforcement), given the volume of SARs involved. In contrast, where a firm (whether estate agent or otherwise) submits a small number of SARs in a given year, it is almost impossible to fully maintain anonymity. Moreover, there are further considerations where an AML investigation is still ongoing. Nonetheless, there are benefits where regulated actors are able to see the benefits or outcomes of their particular contribution (in this instance, the filing of a SAR) to an investigation. This can take the form of direct communication from law enforcement or even seeing the outcome in the news;¹⁸³ indeed, seeing media reports of AML enforcement relating to the estate agent sector was positively commented upon by some interviewees, even if that was not related to their own actions.¹⁸⁴

Interestingly, some noted the difficulties in maintaining confidentiality when filing a report. Whereas the only people who ought to know are the individual EA (who reports suspicion to the money laundering reporting officer (MLRO)) and the MLRO; the reality is otherwise. As one interviewee stated: this type of business

¹⁷⁶ C. Eren, ‘Cops, Firefighters, and Scapegoats: Anti-Money Laundering (AML) Professionals in an Era of Regulatory Bulimia’ (2020) *Journal of White Collar and Corporate Crime*. Advance Access Online. DOI: [10.1177/2631309X20922153](https://doi.org/10.1177/2631309X20922153)

¹⁷⁷ For a breakdown by sector, see NCA, *UK Financial Intelligence Unit Suspicious Activity Reports Annual Report* 2020, 9.

¹⁷⁸ M. Rorie et al, ‘Examining Procedural Justice and Legitimacy in Corporate Offending and Beyond-Compliance Behavior: The Efficacy of Direct and Indirect Regulatory Interactions’ (2018) 40 *Law & Policy* 172.

¹⁷⁹ A. Verhage, ‘Great Expectations but Little Evidence: Policing Money Laundering’ (2017) 37 *International Journal of Sociology and Social Policy* 477, 482.

¹⁸⁰ Interview 11.

¹⁸¹ Interview 11. Separately, there was considerable disquiet about the tipping off offence: eg Interview 5.

¹⁸² eg Interview 15.

¹⁸³ n 175 above.

¹⁸⁴ eg Interviews 1; 2; 4; 9.

mainly works in open plan offices as a team and therefore the whole team is going to know about the situation, particularly in the market now where we're fairly low volume of transactions so everybody is going to know, and therefore the risk of something getting out is far greater than it perhaps would be indicated by the regulations.¹⁸⁵

This person went on to say that the ML Regs 'weren't written by someone who operates in the front-line of estate agents'.¹⁸⁶ This comment suggests a disconnection between the creation of AML rules on paper and their implementation into practice, with a criticism towards law-making and policy-making processes that do not align the theoretical expectations of the legislator with the reality on the frontline. This regulatory 'detachment' emerges both in relation to AML general principles and obligations, and their imposition on EAs, and the theoretical understanding of the practice of EAs and how they can implement AML regulation in their daily practice. This is a common thread that has emerged from our interviews and raises the question of the need to have a better understanding of the practices of different sectors when creating AML regulation.

Self-protection

A recurring theme in AML (particularly as regards CDD and reporting suspicions) is self-protection, which in many instances leads to a box-ticking approach. This theme arises from an AML regime that is 'designed in a way that inevitably provokes fear of penalties and reputational damage'.¹⁸⁷ Thus, there is an evident preference for a more rules-based approach on the part of private actors, or a 'desire for a totally automatic detection system that would obviate the need for individual decision making'.¹⁸⁸ Yet, such an approach goes against the rationale underlying the risk-based approach in the AML regime. The rules-based approach accords, however, with the adoption of secondary risk management strategies to avoid potential blame should something go wrong.¹⁸⁹ Again here, EAs felt to be placed in a position of vulnerability.¹⁹⁰ In this regard, a key concern for private actors is to 'do whatever they can to protect themselves rather than do what they are expected to do'.¹⁹¹ As a consequence, EAs do not act as a filter for suspicious activities;

¹⁸⁵ Interview 3.

¹⁸⁶ Interview 3.

¹⁸⁷ n 106 above, 48.

¹⁸⁸ G. Favarel-Garrigues, T. Godefroy, and P. Lascoumes, 'Sentinels in the Banking Industry: Private Actors and the Fight against Money Laundering in France' (2008) 48 *British Journal of Criminology* 1, 11.

¹⁸⁹ See M. Power, 'The Risk Management of Everything' (2004) 5 *Journal of Risk Finance* 58, 63. For consideration of rules- and risk- based approaches in the context of AML, see G. Sinha, 'Risk-Based Approach: Is it the Answer to Effective Anti-Money Laundering Compliance?' in K. Benson, C. King, and C. Walker (eds), *Assets, Crimes and the State: Innovation in 21st Century Legal Responses* (Oxon: Routledge, 2020).

¹⁹⁰ For wider discussion, see A. Grear, 'Vulnerability, Advanced Global Capitalism and Co-symptomatic Injustice: Locating the Vulnerable Subject' in M. Albertson Fineman and A. Grear (eds), *Vulnerability: Reflections on a New Ethical Foundation for Law and Politics* (Farnham: Ashgate, 2013). For consideration in other contexts, see E. Oakley and S. Vaughan, 'In Dependence: The Paradox of Professional Independence and Taking Seriously the Vulnerabilities of Lawyers in Large Corporate Law Firms' (2019) 46 *Journal of Law and Society* 83.

¹⁹¹ A. Bello, *Improving Anti-Money Laundering Compliance: Self-Protecting Theory and Money Laundering Reporting Officers* (Cham: Palgrave Macmillan, 2016) 48.

instead, often the approach adopted is that it is better to be safe than sorry and to report anything out of the ordinary. This emphasis, however, runs counter to the intentions of the risk-based approach, which was introduced to enhance the quality of reports from the private sector. Thus, the result has been legal uncertainty for those subject to the AML regime,¹⁹² whose focus is (usually) primarily on compliance with the law.¹⁹³

In this study, such considerations were evident for many interviewees. Some spoke about doing the minimum that is required to be compliant,¹⁹⁴ and conducting checks simply ‘to tick a box’¹⁹⁵ because EAs often ‘want to be on the safe side’.¹⁹⁶ To this end, some interviewees spoke about having processes in place ‘to cover their own backsides’.¹⁹⁷ Others have policies in place whereby if a person is still ‘live’ on their system (i.e. they are still dealing with that person), they will run AML checks on an annual basis.¹⁹⁸ Moreover, some interviewees put significant focus on covering themselves against future action:

My main concern is to get the SAR in, to have it documented so that if it ever does go off I can then sit back and say, “We made a SAR on that date. That’s not our problem, we’ve done what we are required to do in law, with a SAR. What you do with it, is up to you”.¹⁹⁹

Another stated that once a SAR is filed and received by the NCA,

then it’s not the agent’s problem then if something happens. They’ve done their bit, it’s up to the authorities then - whether that’s the tax authorities, the police - to do their bit. The agent has flagged it. If the agent doesn’t flag it, then obviously there’s the risk that somebody could come back to the agent and say, “You should’ve spotted this”.²⁰⁰

A recurring theme was that EAs err on the safe side and submit a report if there is any suspicion,²⁰¹ in order to satisfy (and be protected from) regulators.²⁰² Inevitably, defensive reporting becomes an embedded approach ‘understandably so, with a few hours spent submitting a SAR being infinitely preferable to the prospect of more than a few

¹⁹² V. Mitsilegas and N. Vavoula, ‘The Evolving EU Anti-Money Laundering Regime: Challenges for Fundamental Rights and the Rule of Law’ (2016) 23 *Maastricht Journal of European and Comparative Law* 261, 274; cf A. Bello and J. Harvey, ‘From a Risk-Based to an Uncertainty Based Approach to Anti-Money Laundering Compliance’ (2017) 30 *Security Journal* 24.

¹⁹³ B. Coombs-Goodfellow and M. Eshwar Lokanan, ‘Anti-Money Laundering and Moral Intensity in Suspicious Activity Reporting: An Application of Jones’ Issue Contingent Model’ (2018) 21 *Journal of Money Laundering Control* 520; A. Verhage, ‘Great Expectations but Little Evidence: Policing Money Laundering’ (2017) 37 *International Journal of Sociology and Social Policy* 477.

¹⁹⁴ eg Interview 14.

¹⁹⁵ Interview 9. Also Interview 14.

¹⁹⁶ Interview 10.

¹⁹⁷ Interview 3.

¹⁹⁸ eg Interview 8.

¹⁹⁹ Interview 1.

²⁰⁰ Interview 3.

²⁰¹ eg Interview 13.

²⁰² A. Amicelle, ‘Towards a “New” Political Anatomy of Financial Surveillance’ (2011) 42 *Security Dialogue* 161, 168.

years' incarceration for a substantive laundering or failure to disclose offence'.²⁰³ Our findings fit with a broader emphasis on precaution and security, or in some instances 'even being cautious about how one is being cautious'.²⁰⁴ Therefore, the focus on 'box-ticking' places significant emphasis on the 'norm of compliance'.²⁰⁵ As Svedberg Helgesson and Morth state,

seemingly technical procedures entail more complexity when they are to be handled in practice. Private actors need to make decisions that the legislator has not regulated, or foreseen, when the procedures are to be translated into practice. We argue that the room for manoeuvre for private actors to make decisions and policies is to a large extent dependent on how the balance between box-ticking and human judgement is designed in the legislation.²⁰⁶

For most interviewees in this study, the inclination was to focus on box-ticking rather than to exercise their judgement on a case-by-case basis. This approach was motivated by an abundance of caution; however, it does run counter to the risk-based approach. Notwithstanding that finding, however, not all interviewees adopted such an approach. A small number of interviewees highlighted that they only submit a SAR where there is a genuine concern.²⁰⁷ Indeed, there was some scepticism as to whether EAs do simply file SARs just to be safe. If that were the case, it was suggested, then there would be a lot more SARs from the sector.²⁰⁸

Impact on Business

Our interviews reveal that the decision whether or not to report a potential client or potential customer is a significant one. Moreover, there is a cost of doing so, even if only with the time involved.²⁰⁹ A further potentially problematic issue is that if there is a suspicion on the part of the EA, and they file a SAR, then the EA cannot proceed with that transaction without consent from the NCA (or until the expiration of the relevant time period²¹⁰), nor can they inform their client about the reason for the delay. If the EA proceeds with the transaction, they are exposed to potential criminal liability; if they explain the reason for the delay to their client, again they are subject to potential criminal liability.²¹¹ The conundrum with filing a report is summed up by one interviewee as follows:

²⁰³ S. Kebbell, 'The Law Commission: Anti Money-Laundering and Counter-Terrorism Financing – Reform of the Suspicious Activity Reporting Regimes' [2018] *Criminal Law Review* 880, 890.

²⁰⁴ n 108 above, 353.

²⁰⁵ K. Svedberg Helgesson and U. Morth, 'Involuntary Public Policy-making by For-Profit Professionals: European Lawyers on Anti-Money Laundering and Terrorism Financing' (2016) 54 *Journal of Common Market Studies* 1216, 1220.

²⁰⁶ *ibid.*

²⁰⁷ eg Interview 8.

²⁰⁸ eg Interview 10.

²⁰⁹ Interview 3, who suggested that 'it's probably a couple of hour process to actually make a report. And, time is money'.

²¹⁰ POCA, ss 335-336.

²¹¹ For consideration of practical scenarios where such difficulties can arise, see A. Campbell and E. Campbell, 'Solicitors and Complying With the Anti-Money Laundering Framework: Reporting Suspicious, Applying for Consent and Tipping-Off' in N. Ryder, U. Turksen, and S. Hassler (eds), *Fighting Financial Crime in the Global Economic Crisis* (Oxon: Routledge, 2015).

We are told, once you report it, you can't deal with him until he's been cleared. So, you've lost the impetus of any sale you might be doing because by the time they've come back and cleared him, he's long gone.²¹²

It was stressed that this problem conflicts with the role of EAs: 'Your job as the agent is to get the deal through'.²¹³ This concern for EAs' incentives is heightened given the nature of the sector, often working on a no-sale-no-fee basis, which might discourage EAs from making reports. As one EA stated, 'They should do it absolutely correctly, but in some instances I'm thinking, "Well if the fee's large enough, I might not look so carefully at the CDD because I have bills to pay"'.²¹⁴ Thus, willingness to comply can be distorted by the nature, or reality, of business. Similar considerations are evident in other areas of regulation, where regulatees 'struggled to disentangle normative from instrumental motivations, and wrestled with the temptation to backslide when legally mandated improvements proved very expensive'.²¹⁵ For instance, it was noted that some EAs do not consider filing a SAR when a transaction falls through which runs counter to what the AML rules provide. While some did understand this requirement,²¹⁶ not all EAs do. Economic factors appear to be an influence here: as one interviewee (who did draw attention to this requirement) noted, the issue for many EAs is that:

If you don't exchange contracts, you don't get paid. So, if your client pulls out because they think you've rumbled them, well, why would you spend time now submitting a SAR when the evil that you're involved in has stopped and you're not going to get paid for that work?²¹⁷

Monetary considerations, unsurprisingly, affect decisions as to whether or not to fully comply with AML regulations; this is significant given that probability of detection influences the likelihood of compliance.²¹⁸ Significantly, then, HMRC appears to have increased enforcement action against estate agents.²¹⁹ A further point here is that – given monetary considerations do play a part in compliance – questions arise as to whether there is a 'sham' of commitment to AML.²²⁰ It was suggested that given this aspect of the role of EAs, 'we're expecting the wrong people to be the gatekeepers'.²²¹ However, if HMRC's increased enforcement action is sustained, and there is a likelihood of publicity

²¹² Interview 12.

²¹³ Interview 12.

²¹⁴ Interview 10.

²¹⁵ N. Gunningham, 'Enforcement and Compliance Strategies' in R. Baldwin, M. Cave, and M. Lodge (eds), *The Oxford Handbook of Regulation* (Oxford: OUP, 2010) 123.

²¹⁶ eg Interview 9.

²¹⁷ Interview 9.

²¹⁸ D. Nagin, 'Deterrence in the Twenty-First Century' (2013) 42 *Crime and Justice* 199.

²¹⁹ J. Evans, 'UK Estate Agents Hit by Crackdown on Money Laundering', *Financial Times* (9 March 2019).

²²⁰ n 187 above, 15.

²²¹ Interview 9.

and reputational damage,²²² then a ‘normative climate’ towards compliance might develop.²²³

Designing future AML initiatives in the UK real estate market: key insights from the sector

The data analysed in our study reveals some relevant aspects that should be considered in future initiatives and policies involving the real estate sector and the fight against money laundering. First, the quasi-policing role of private actors and their expanding involvement in AML strategies as fundamental gatekeepers²²⁴ has resulted in an evident sense of duty amongst those regulatees towards AML. In other words, the new regulation implemented in the UK has helped to create a community of regulatees that is, at least from a real estate perspective, informed and aware of its responsibilities within the AML regime. Therefore, the expansion of the list of subjects obliged under the ML Regs and the imposition of new obligations has strengthened the sense of belonging of EAs to a set of rules that cannot be disregarded or bypassed. This was an unexpected finding; indeed, at the outset of this study, we hypothesised that there would be resistance to AML compliance.

This view held by EAs towards the AML regime, however, does not indicate the absence or the overcoming of issues emerging in AML compliance. In this regard, a recurring complaint in our interviews related to the *burden* of compliance: as one interviewee stated, ‘it’s a huge cost to the business, you know, absolutely huge’.²²⁵ As previously recalled, the financial, logistical, and administrative costs associated with AML compliance are seen to impact the business of EAs and their approach to AML heavily, with potentially disruptive effects for the entire regulatory regime. This finding is in line with the idea that ‘The costs of compliance seem to outweigh the risks’²²⁶ and, in the long term, there is a real danger of losing the support of gatekeepers. This is not a problem confined to the real estate sector; it has also been observed in other sectors (e.g. banking) where financial and reputational interests have influenced AML compliance.²²⁷

Another finding of our study is that the AML regime is perceived by EAs as being flawed by what can be described as a lack of commitment by national authorities towards regulatees. Indeed, as emerges from various interviews, there is a general frustration amongst EAs for the lack or inconsistency of guidelines provided by HMRC and NCA regarding fundamental aspects of their AML obligations, such as CDD checks and SARs.²²⁸ It is evident that there is a need for better guidance and information for EAs. While there is, admittedly, some sector-specific guidance,²²⁹ the terminology used is often

²²² For example, D. Byers, ‘Purplebricks fined after money-laundering breach’ *The Times* (18 August 2020); BBC News, ‘Countrywide Fined £215,000 Over Money-Laundering Failings’ (4 March 2019).

²²³ n 141 above, 17.

²²⁴ On responsabilisation, see n 84.

²²⁵ Interview 9.

²²⁶ A. Veng Mei Leong, *The Disruption of International Organised Crime: An Analysis of Legal and Non-Legal Strategies* (Oxon: Routledge, 2007) 134.

²²⁷ n 143 above.

²²⁸ In its 2019 review of SARs, the Law Commission recognised the reality of fragmented and conflicting guidance: Law Commission, *Anti-Money Laundering: The SARs Regime* (HC 2098, June 2019) 52 *et seq.*

²²⁹ HMRC, *Anti-Money Laundering Supervision: Estate Agency Businesses* (June 2017). While this article was being finalised, updated guidance was issued. However, it remains to be seen whether this addresses

vague, and there is a tendency to adopt a broad-brush approach that can be applied to different sectors. This might be a reasonable method to promote general consistency *across* regulated sectors, but EAs criticise the lack of detail or sector-tailored policies and provisions which they would need to cope with specific issues encountered *within* the real estate market. Some interviewees particularly lament the ‘one-size-fits-all’ approach in relation to SARs.²³⁰

From the foregoing, it emerges that, despite the good disposition of many in the sector, EAs denounce the limits of the governance imposed on them, and they struggle to reconcile their new responsibilities with the limited engagement from national authorities. As an interviewee told us, ‘I think the guidance which HMRC issued is okay, but if you ever go to them to say, “What would we do in this situation?” Their advice is always, “It’s up to you, it’s your business, you need to make your own decision”. [...] They’re very non-committal on helping firms. I think it’s always a case of “Read the guidance, it’s there”’.²³¹ This discrepancy in the authorities’ approach risks widening the gap between EAs and governing bodies, rather than reducing it, and it resembles the findings of studies carried out on other AML regulated sectors.²³² Indeed, the lack of support and guidance for EAs affects the relationship between regulators and regulatees negatively. Furthermore, once EAs are subject to the AML regime, and the associated obligations, so too are there expectations on their part – and these expectations of support and guidance are not being met.

The misalignment between obligations and support has contributed to the spread of a ‘do-it-yourself’ approach among EAs, which now applies to various obligations, including CDD checks and SARs. From the analysis of our interviews, it is clear that EAs have tried to fill in the gaps themselves by adopting flexible methods of compliance and finding alternative solutions to problems emerging in their daily practice. For instance, the need to take into account well-known customers or the variety of clients involved in property transactions has pushed EAs to implement diverse compliance strategies that are not provided by national authorities. This phenomenon is not necessarily a negative outcome per se. On the contrary, it can be a positive development for the real estate sector, and the AML regime as a whole, because it reinforces the idea of a ‘community’ of subjects that works to achieve AML purposes. Moreover, the direct initiatives of EAs show the risk-based approach in action, and they demonstrate the effects of an independent undertaking by private actors. This finding is in line with research by Tsingou on compliance officials, where it is said that ‘professionalization has led to an extension of governance functions, from implementation, to active interpretation of rules, to shaping the content of governance through regulatory creep’.²³³

The multiple compliance methods and approaches adopted by EAs, however, can also be detrimental to the AML regime. This is particularly true if we look at the justifications given by EAs for their compliance strategies and the outcomes of these choices. As already recalled, EAs quite often seem to rely on self-justification and self-protection when coping with challenges in implementing their AML obligations. In so

concerns that guidance is not sufficiently tailored for the sector. See HMRC, *Estate agency business guidance for money laundering supervision* (Updated October 2020).

²³⁰ eg Interview 1 when saying that ‘the SAR system is not really a good system because it’s designed really for SARs in the banking sector’.

²³¹ Interview 13.

²³² See, for instance, n 2 above, 94-95 in relation to the banking sector.

²³³ n 122 above, 192.

doing, EAs choose to apply ‘passively’ AML provisions without exercising the necessary level of critical assessment required by the risk-based approach. In other words, they do not always evaluate actively the risks associated with a transaction, but they prefer to count on subsequent evaluation made by national authorities, such as the NCA. This approach frustrates the objectives of the multilevel AML regime, and it might also overload the system, most evidently with overly defensive reporting. The result is ‘a burdensome bureaucracy for the innocent, whilst providing scant deterrent for the launderer’.²³⁴ Moreover, by adopting an ‘automated’ response to ML risks or suspicious transactions, EAs can create risks of false positives or false negatives that impact the regulatory regime negatively.²³⁵ Indeed, if regulatees do not implement AML regulation with a correct judgement,²³⁶ the filtering obligations imposed on them would have no effect, and the AML system would be undermined. This is particularly evident when looking at EAs’ views on identification checks and how they deal with PEPs.

The consequences of poor implementation of AML regulation by EAs are not limited to the discovery of ‘bad practices’ and practical issues. They are also linked to the question as to whether EAs can conduct their business and pursue transactions without being affected negatively or unduly influenced by AML compliance. As recalled previously, some EAs argue that the nature of their business and the negative impact on their relationship with customers play a crucial role in the extent of their compliance with AML obligations. From the analysis of our interviews, it might be said that in various cases, the first victims of compliance are compliant EAs. In this sense, two important aspects must be considered when designing AML regulation. The first is to avoid possible disadvantages for those private actors who are compliant with AML. In other words, there is a need to provide clear, consistent guidance to whole sectors and to facilitate compliance responses, for instance, when filing SARs or conducting CDD checks. The second aspect pertains the need for the legislator to recognise the potential impact of compliance on the business of EAs. Indeed, some commentators suggest that there may be a need for the State to incentivise compliance.²³⁷

Having discussed the meaning and relevance of the findings obtained in this study, it is possible to make some final considerations on the value of this contribution and possible future research on the topic.

Alongside the extension of the AML regime to encompass non-financial businesses and professions as additional gatekeepers, a vast, critical literature has emerged. Notwithstanding the global evaluations undertaken by the FATF,²³⁸ which

²³⁴ M. Killick and D. Parody, ‘Implementing AML/CFT Measures That Address the Risks and Not Tick Boxes’ (2007) 15 *Journal of Financial Regulation and Compliance* 210, 210. See also G. Sinha, ‘To Suspect or Not To Suspect: Analysing the Pressure on Banks to Be ‘Policemen’’ (2014) 15 *Journal of Banking Regulation* 75, 79.

²³⁵ n 108 above, 348.

²³⁶ n 43 above.

²³⁷ N. Tilley, ‘Privatizing Crime Control’ (2018) 679 *The Annals of the American Academy of Political and Social Science* 55. For a discussion of how ‘material considerations’ influence decision-making, see S. Simpson and M. Rorie, ‘Motivating Compliance: Economic and Material Motives for Compliance’ in C. Parker and V. Lehmann Nielsen (eds), *Explaining Compliance: Business Responses to Regulation* (Cheltenham: Edward Elgar, 2011).

²³⁸ See, for instance, FATF, *Anti-Money Laundering and Counter-Terrorist Financing Measures - United Kingdom, Mutual Evaluation Report* (December 2018). For critical comment of the FATF MER process, see P van Duyne, J Harvey and L Gelemerova, ‘A “risky” risk approach: proportionality in ML/TF

purport to measure the ‘effectiveness’ of AML in different jurisdictions, it is not possible to say whether AML works or not. Notwithstanding various anecdotes, ‘there is still very little scientific knowledge about the effectiveness and efficiency of the countermeasures adopted to combat the phenomenon’.²³⁹ Indeed, ‘a huge amount of money (we do not know how much) is now being spent on a global surveillance and reporting system, and we do not know whether and to what extent the system works or not’.²⁴⁰ Moreover, the AML regime ‘exhibits many deficiencies and imposes extensive costs on the private and public sectors, and harms upon the public’.²⁴¹

Thus, rather than expansion of the AML regime (which continues unabated – as evident in recent Money Laundering Directives;²⁴² various FATF efforts;²⁴³ and domestic legislative amendments²⁴⁴), it is timely to reflect upon operation in practice. To put it bluntly, the extant AML regime is problematic and does not work well in practice because, as Henry Ford once said, ‘if you always do what you’ve always done, you’ll always get what you’ve always got’. Thus, this article has aimed to reflect upon the experiences of EAs tasked with implementation of AML in practice.

First of all, our research reinforces concerns as to the operation of ‘suspicion’. While the broad-brush approach in POCA requires a report to be made where a person knows or suspects, or has reasonable grounds for knowing or suspecting, that another person is engaged in money laundering,²⁴⁵ this has proved problematic in practice. Moreover, as the Law Commission highlighted in its 2019 review, ‘there is currently no means of ensuring that the burden of reporting is proportionate to the gravity of the offence, the value of the criminal property and the benefit to law enforcement agencies of this intelligence’.²⁴⁶ Thus, the burden of compliance is often ignored in policy development, whereas - as our study shows - considerations of burden (and opportunity lost) significantly influence compliance. Further, the risk-based approach is undermined by the desire for self-protection and, consequently, anything remotely suspicious being reported, which overwhelms law enforcement capacity to analyse SARs.

Second, our study focuses on the operation of AML within one sector. A recurring complaint was the differences inherent in that sector and the need for sector-specific guidance. The Law Commission has acknowledged the need for a sector-tailored approach, but it has also stressed that ‘There remains a strong argument for having a single, accessible, interpretation of universal legal concepts common to all sectors’.²⁴⁷

regulation’ in C. King, C. Walker, and J. Gurulé (eds), *The Palgrave Handbook of Criminal and Terrorism Financing Law* (London: Palgrave Macmillan, 2018).

²³⁹ B. Vettori, ‘Evaluating the Anti-Money Laundering Policies: Where Are We?’ in B. Unger and D. van der Linde (eds), *Research Handbook on Money Laundering* (Cheltenham: Edward Elgar, 2013) 474.

²⁴⁰ P. Alldridge, *What Went Wrong With Money Laundering Law?* (London: Palgrave Macmillan, 2016) 3.

²⁴¹ T. Halliday, M. Levi, and P. Reuter, ‘Anti-Money Laundering: An Inquiry into a Disciplinary Transnational Legal Order’ (2019) 4 *UC Irvine Journal of International, Transnational, and Comparative Law*, Art.3, 3.

²⁴² Directive (EU) 2018/843; Directive (EU) 2018/1673.

²⁴³ For example, the FATF Standards are regularly updated, most recently in October 2020; FATF itself is undertaking a ‘strategic review’ which ‘aims to strengthen the efficiency and effectiveness of the FATF and make the assessment and monitoring processes more timely, effective and risk-based’: FATF, *Outcomes FATF Plenary, 19-21 February 2020* (FATF, 21 February 2020).

²⁴⁴ See the ML Regs 2017 and 2019.

²⁴⁵ See, for instance, POCA, s 330(2).

²⁴⁶ Law Commission, *Anti-Money Laundering: The SARs Regime* (HC 2098, June 2019) para 1.55.

²⁴⁷ *ibid.*, para 3.13.

Such a stand-alone document encompassing the various legal concepts (such as ‘suspicion’) would be valuable but should be accompanied by supervisor-approved guidance for individual sectors. This combination would result in greater clarity and consistency for EAs (and other regulatees). It remains to be seen whether updated guidance issued in October 2020 will address practical concerns in the sector.²⁴⁸

Third, the burden of compliance is compounded by ambiguity. While the legislation itself is relatively straightforward, practice evidences many instances where regulatees determined to comply are confronted with uncertainty. Given the absence of clear, sector-tailored guidance, the tendency is, again, to report as a means of self-protection. The lack of engagement from enforcement agencies when such uncertainty arises reinforces the sense of vulnerability amongst EAs and can result in poor-quality reports. Further, the process of reporting is hindered (and burden of compliance increased) as a result of difficulties with the SARs reporting system and the lack of a joined-up gateway/portal for both HMRC and the NCA, which adds unnecessary complexity.

Fourth, AML compliance impacts upon the business of regulatees, most obviously in terms of costs and time, but it can also affect the relationship with clients. Moreover, compliance can unduly delay transactions. Inevitably, those EAs that seek to ensure that they comply are adversely affected, with concerns that those who are laxer with their obligations would be advantaged. In this sense, any system of regulation that results in compliant regulatees losing out risks inherently undermining itself.

Finally, our study demonstrates a relevant finding concerning support for the AML regime, at least in principle. Contrary to our initial expectations, there was significant support for AML obligations and the role of EAs as important gatekeepers. Many interviewees felt that they had an important role to play as part of ‘the first line of defence’.²⁴⁹ Thus, criticism of the AML regime related more to practical hurdles and/or burdens, rather than the issue of whether EAs have a role to play in AML. Notably, the one-size-fits-all approach was criticised, and a recurring theme was that obligations imposed upon EAs do not adequately take account of the lived realities of how estate agency business operates. This final quote aptly sums up the feeling of many: ‘it’s a drag, it’s horrible, it’s aggravation, but I get it and we do it - we have to do it’.²⁵⁰

Future research on the topic of AML implementation, and associated challenges, in the UK real estate market could focus on two aspects that are not within the scope of this article, but that could be investigated as independent streams of research. First, the question of self-regulation of EAs (and indeed other sectors) persists. It would be especially interesting to evaluate the role of self-regulation for compliance purposes and to what extent this might have an impact on the implementation of AML regulation by private actors. Indeed, as demonstrated in our study, EAs are often left to decide the best approach to fulfil their AML obligations, and this creates a quite scattered picture with many variations in the sector and initiatives adopted independently from legislative requirements. Second, attention could be given to the existence of possible differences among EAs in relation to reputational incentives based on their role as buying, selling, or letting agents. In this sense, future research might analyse if and how AML compliance varies when different types of EAs are involved in a property transaction, especially

²⁴⁸ See n 228.

²⁴⁹ n 51 above, 12. Though there was also discontent by others, with AML requirements described by one interviewee as ‘an absolutely pointless exercise’: Interview 12.

²⁵⁰ Interview 3.

looking at the effects that the fulfilment of AML obligations might have on the relationship with customers. However, this type of research would require a large data set with many interviews and opinions gathered from the sector. Indeed, only with an extensive amount of data would it be possible to identify significant findings and make relevant considerations as to the topic.

Appendix 4

RCMP “E” Division – Money Laundering in the Real Estate
Sector: Media Reference which Cites “Secret Police Study” –
March 14, 2019



E DIVISION MONEY LAUNDERING REVIEW: PART II

Prepared for: A/COMM KA (Kevin) HACKETT

Date: 2019-03-14

**MONEY LAUNDERING IN THE REAL ESTATE SECTOR:
MEDIA REFERENCE WHICH CITES "SECRET POLICE STUDY"**

On 2019-03-07, E Division Criminal Operations, Federal, Investigative Services & Organized Crime (CROPS FISOC) and senior managers from Federal Policing and the Combined Forces Special Enforcement Unit – BC (CFSEU-BC) met with Dr. Peter GERMAN, Mr. Adam ROSS and Mr. Raheel HUMAYUN to provide an explanation of the possible origin and authenticity of the report referenced in the media as a secret police study of Vancouver-area property transactions which exceed \$1B and linked to the money laundering efforts of transnational organized crime.

A copy of media article is appended for your reference.

Following the media report, it was believed, at the time, the police report referenced had been identified. Written in November 2017, the methodology consisted of obtaining data from the Real Estate Board of Greater Vancouver (REBGV) which listed residential properties purchased in the calendar years 2015 and 2016 valued at a threshold exceeding \$3M. Approximately 1200 lines of data were reviewed. The property addresses were then queried through the BC Online Land Titles data base to identify property owners. These owner names were then checked using the PRIME-BC database to determine potential criminality / criminal involvement.

The initial findings revealed that about 10% of the owners who purchased properties during that time frame were linked to some level of criminality, including suspicious currency transactions, drug importation / production / trafficking, gaming intelligence, fraud, extortion and proceeds of crime. A wide range of other criminal offences related to assault, child pornography, immigration, weapons, and others were also identified.

It is imperative to note initial findings were, in no manner, definitive or conclusive. The study did not conduct further or complete analysis, cross-referencing or validation against historical or current investigations, intelligence or other opened or closed data sources. Contrary to its description in media reporting, it does not assert crime networks could have laundered over \$1B through Vancouver homes in 2016, or that 95% of the 10% of transactions are believed to be linked to "Chinese" organized crime,

These discrepancies led to further examination and assessment of the descriptions and referencing to determine whether another BC RCMP report(s) containing sensitive police information could have been the subject of the media reporting.

Nine (9) additional BC RCMP reports were located. It has taken some time to review and compare these in an effort to identify the source of information in the public domain. The first-noted discrepancies as well as additional factors and details in media reports are not contained in or consistent with the other BC RCMP reports. Furthermore, the media cites the use of other agency reports, documents, legal filings and unspecified police intelligence to derive information for the article.

Therefore, the origin and authenticity of the confidential police report cited in the media has not been identified with absolute certainty. Although it bears a close resemblance to that described in the media report, it also presents the study's findings in a manner which is sufficiently misinterpreted and speculative to cause reservation.

/Prepared by: C/M Kelly C. RAINBOW, 2019-03-14

Fentanyl: Making a Killing

Secret police study finds crime networks could have laundered over \$1B through Vancouver homes in 2016

By Sam Cooper, Stewart Bell and Andrew Russell
November 26th, 2018

The stately \$17-million mansion owned by a suspected fentanyl importer is at the end of a gated driveway on one of the priciest streets in Shaughnessy, Vancouver's most exclusive neighbourhood.

A block away is a \$22-million gabled manor that police have linked to a high-stakes gambler and property developer with suspected ties to the Chinese police services.

MORE: Read the full Fentanyl investigation

Both mansions appear on a list of more than \$1-billion worth of Vancouver-area property transactions in 2016 that a confidential police intelligence study has linked to Chinese organized crime.

The study of more than 1,200 luxury real estate purchases in B.C.'s Lower Mainland in 2016 found that more than 10 per cent were tied to buyers with criminal records. And 95 per cent of those transactions were believed by police intelligence to be linked to Chinese crime networks.

The study findings, obtained by Global News, are a startling look at what police believe to be the massive money laundering occurring in the Vancouver-area real estate market.

WATCH: How organized crime groups launder suspected drug money in B.C. real estate

They are also an indication of how — according to police intelligence sources — Canada's narcotics are hiding the huge amounts of cash they are amassing from the fentanyl crisis, which resulted in the deaths of thousands of Canadians last year.

“You know that Netflix show *Ozark*, about laundering drug cartel money?” said an expert, who could not be identified because of ongoing investigations in B.C. “I always think that if those characters came up to Vancouver, they could launder all their cash in just one day.”

While the study only looked at property purchases in 2016, an analysis by Global News suggests the same extended crime network may have laundered about \$5-billion in Vancouver-area homes since 2012.

At the centre of the money laundering ring is a powerful China-based gang called the Big Circle Boys. Its top level “kingspins” are the international drug traffickers who are profiting most from Canada's deadly fentanyl crisis.

The crime network, according to police intelligence sources, is a fluid coalition of hundreds of wealthy criminals in Metro Vancouver, including gangsters, industrialists, financial fugitives and corrupt officials from China.

WATCH: Police investigation links dirty cash to luxury real estate. John Hua reports.

They are involved in drug import and production schemes, casino money laundering, real estate money laundering, prostitution, and financial crimes, the sources said.

The common link among them is an underground banking scheme in which Chinese VIP gamblers and gangster associates secretly transfer money between China and Richmond, B.C., in order to fund fentanyl imports and trafficking in Canada.

B.C. Lottery casinos are an important conduit in the underground transactions. But the money laundered through gambling is miniscule compared to the sums flowing through real estate.

WATCH: How does fentanyl get into Canada? Global News reveals the nefarious route the opioid takes.

One expert said Canadians would be stunned to learn how many of Vancouver's homes have been built on drug money since the 1990s, when heroin from Hong Kong and China started flooding into Vancouver and Toronto.

The police intelligence study, completed this year, examined real estate purchases valued between \$3 million and \$35 million. The researchers suspected significant money laundering in the \$1- to \$3-million range — including suspicious condo flipping transactions — but didn't have the time or resources to study the over 20,000 transactions.

Against the sample of about 1,200 high-end sales in 2016, researchers cross-referenced property documents with databases of criminal records and confidential police intelligence regarding ongoing investigations and networks of suspected criminals.

Many of the suspected criminal homes in the sample

cost more than \$10 million. And in an indication of how drug cash can move land prices dramatically higher in some Vancouver neighbourhoods, property records show some of the suspected fentanyl kingpins paid well above recent sale prices for homes in the study.

A \$22-million home in Shaughnessy was connected by police intelligence in the study to a Macau gambler who took out tens of millions in real estate loans from suspected organized crime lenders operating out of Metro Vancouver casinos, according to allegations in Lottery Corp. documents and legal filings.

Property documents indicate the alleged VIP bought the Shaughnessy home for just \$7.5 million in 2011. But when a ring of private lenders attempted to enforce real estate loans, documents show, the home was sold in 2016 for an astounding \$14-million price gain, at \$22-million.

Since 2012, the alleged VIP has sold a number of Metro Vancouver homes worth about \$50 million in total, property documents show. And the gambler has made 28 suspicious transactions in B.C. Lottery casinos, according to Lottery Corp. investigation documents.

But in 2018, 51-year-old Paul King Jin — a former Richmond massage parlour owner who, according to Lottery Corp. documents, is targeted by the RCMP in probes of suspected transnational drug trafficking — sued the Macau gambler for \$8 million.

Jin claims in 2016 he discharged a mortgage on the \$22-million home so the Macau gambler could sell the property and repay creditors. But Jin hasn't been paid, he claims, because other lenders rank above him.

The home is no longer owned by suspects named in the police intelligence study.

WATCH: A look at exactly how profitable the opioid is for criminals in Canada.

Jin's filings said the Macau gambler described himself as "a man of great wealth" involved in real estate development in Canada and China. But in a legal response, the gambler's lawyer said he had already sold three homes and paid \$35 million to a group of "private lenders." And these lenders took advantage of the gambler's addiction with loans that "may at worst be criminal," the Macau gambler claimed.

The gambler has returned to Macau, legal filings say, and Global News has not been able to reach him for comment.

Jin has not responded to questions from Global News about police allegations. Some of Jin's associates have been charged in a drug trafficking and money laundering investigation, but it is not known if Jin has been charged.

In another 2016 sale, a suspected fentanyl kingpin and casino loan shark bought a \$3.6-million home in West Vancouver. And one alleged criminal bought two adjacent Vancouver homes, worth over \$3 million each, on the same day.

Another alleged kingpin bought a \$15-million Shaughnessy mansion in 2016, as well as a tear-down \$3.5-million bungalow on a south Vancouver block that is zoned for condo building.

One of the 2016 study homes, a \$17-million mansion in Shaughnessy, is owned by a Chinese industrialist and Vancouver real estate developer, documents show.

But according to police intelligence, the owner is allegedly involved in narcotics imports and exports. Property and lending documents show the owner's family holds at least nine Vancouver-area homes worth over \$60 million, in addition to assembling hundreds of acres of residential land in Metro Vancouver since 2014 and also proposing to develop a Vancouver luxury condo tower.

Global News has not been able to reach the Shaughnessy mansion owner for comment on police suspicions.

The owner is also tied through corporate records to an alleged illegal casino in Richmond that Lottery Corp. investigators believe is run by Big Circle Boys. And the owner's family holds positions in the Chinese People's Political Consultative Conference, corporate records from China indicate.

WATCH: How Chinese gangs are laundering drug money through Vancouver real estate

A few hundred metres away in central Shaughnessy, is yet another \$17-million abode with alleged links to the Big Circle Boys.

This second mansion made Vancouver headlines in 2007, when its owner — a Big Circle Boys kingpin described as one of Canada's top priority crime targets — was gunned down outside his front gates.



A scenic view of Vancouver's downtown. A study of more than 1,200 luxury real estate purchases in B.C.'s Lower Mainland in 2016 found that more than 10 per cent were tied to buyers with criminal records

THE CANADIAN PRESS IMAGES/Bayne Stanley

The mansion is now owned by a Richmond real estate agent, court records show. Police intelligence sources say the realtor is intimately related to a B.C. Lottery Corp. gambler and Metro Vancouver real estate developer who is accused in a \$500-million corruption case in China. Global News could not reach the realtor for comment, and the alleged VIP gambler has denied financial corruption allegations reported in China.

Other study findings suggested criminals in China anonymously bought B.C. real estate with Bitcoin, the crypto-currency used by drug traffickers. One Beijing Craigslist advertisement offered an eight-bedroom mansion in the hills of Coquitlam for 1,075 bitcoins, the equivalent of \$3.3 million.

The findings come amid Metro Vancouver's housing affordability crisis, in which middle-class families have been priced out of the city. Many of these properties were left empty, and bought on paper by the spouses and children of suspected criminals. Investigators were surprised that some convicted drug trafficking criminals didn't even conceal their property purchases.

Even so, the RCMP just doesn't have the resources to tackle so many suspected money laundering transactions in Vancouver, a source said.

Meanwhile, home prices in Vancouver have tripled since 2005.

Across the Lower Mainland, prices began to sky rocket in late 2012. Some analysts believe a flood of money from China in recent years forced Metro Vancouver home prices to disconnect from the region's median household wage of \$72,000, which ranks among the lowest for Canadian cities, and 50th in North America.

Urban planning expert Andy Yan, director of the City Program at Simon Fraser University, said the real estate money laundering data "begins to explain what is happening in Vancouver."

"This is financial fentanyl for our real estate," Yan said. "You have found \$1 billion. But it is probably magnified in the banking system, with all of the black money, gray money, and legitimate money cascading through local institutions, to make a toxic sausage. So this is a national security issue. And also a national financial issue."

Government documents obtained by Global News show that the government believes that in 2012, loan sharks connected to gangs in China and associated Chinese VIP gamblers ramped up a flood of suspected drug cash transactions in Vancouver-area casinos.

READ MORE: Opioid crisis may be lowering Canadians' life expectancy, report says

There were \$64-million worth of suspicious cash transactions in these casinos in 2012, \$119 million in 2016, and \$66 million in 2017. But suspicious cash transactions in B.C. Lottery casinos surged to \$176 million in 2015 — including \$136 million in \$20 bills.

Meanwhile, in a mirror image of what is suspected to be a record year for B.C. casino money laundering, Lower Mainland home prices sky rocketed by over 30 per cent in 2015.

A fentanyl-trafficking investigation expert said Chinese crime methods for laundering cash in Vancouver real estate have followed a consistent pattern since the 1990s, when the current kingpins of fentanyl started to dominate Canada's heroin markets.

"It has always been the same people involved, and unfortunately the longer they do it, the more legitimate they look," the expert said. "What they do is buy these tear-downs, and they do renovations and build mansions. I know one case, (a Chinese heroin kingpin) laundered eight of these homes in Vancouver himself."

At the same time, police and confidential sources in Vancouver have believed that for about 20 years the Big Circle Boys and associates used B.C. casinos, mostly in Richmond, for drug dealing.

They "liked to conduct money exchanges in casinos," according to a record filed in B.C. Supreme Court. "The drug trafficker could then have the casino as an explanation for the money, if stopped by the police."

Police say that almost every drug seizure they now make in Vancouver turns up some form of synthetic opioid produced at factories in China. Cocaine is still the drug Vancouver police seize most. But one expert predicted that by the end of 2018, fentanyl would become the most common drug on Vancouver streets.

As the drug kingpins of Vancouver have raked in profits and the city's real estate prices have surged, the fentanyl crisis has spread from its epicentre among addicts in Vancouver's impoverished Downtown Eastside to communities across the country, leaving behind a devastating body count.

"It's a neat circle. Welfare-Wednesday spending ultimately enriches those fueling the affordability crisis," one law enforcement source said. "And that creates the need for Welfare-Wednesday."

Last year, nearly 4,000 Canadians died from an opioid-related overdose, according to figures from Health Canada, with the vast majority of deaths

involving fentanyl.

Government figures released in September showed that more than 1,000 Canadians lost their lives to apparent opioid overdoses in the first three months of 2018 – or more than 11 people per day.

Senator Vernon White, a former police chief who has advocated for measures to block the fentanyl supply from China, called the deaths and the related housing affordability crisis among the greatest threats facing Canada.

“I have been in policing 33 years and I have never seen anything with the profitability that fentanyl has,” White said. “This is a security threat. If terrorists were killing 5-6,000 people per year, we would do something about it.”

A 2017 B.C. Supreme Court sentencing ruling stated that drug traffickers can turn one kilogram of heroin worth \$70,000 — blended with \$12,500 worth of fentanyl powder — into 100 kilograms of counterfeit heroin, worth about \$7 million on the street.

But it is the blending of various drugs with fentanyl, which is 50 to 100 times more toxic than morphine, that has caused fatal overdoses to surge, the ruling says.

And yet, about 10 years before fentanyl started to flood Vancouver, Canadian courts had already found that Big Circle Boys were the dominant Chinese crime syndicate in Canada causing opioid overdose deaths.

One convicted Toronto-based Big Circle Boys kingpin acknowledged that he was likely responsible for causing heroin drug overdose deaths in Vancouver and southern Ontario, a 2003 federal court ruling says. The man also admitted he sent massive drug cash proceeds back to China, to buy businesses, including a coal mine.

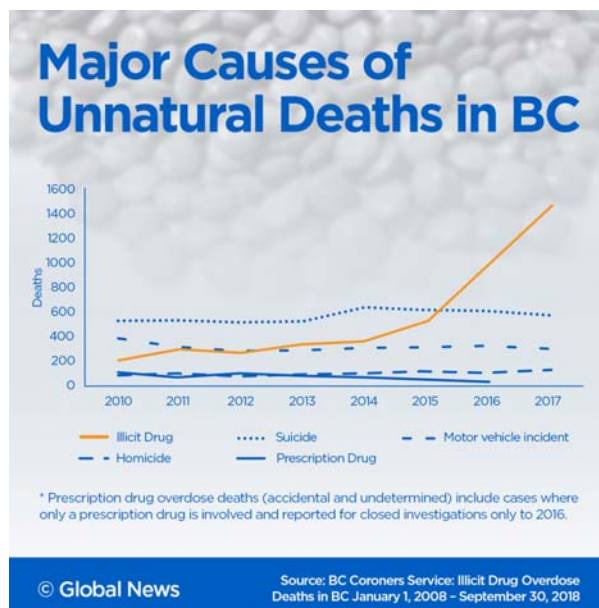
© 2018 Global News, a division of Corus Entertainment Inc.

PREVIOUS CHAPTER

An introduction to Fentanyl: Making a Killing

2 OF 2

SHARE THIS ARTICLE



Neil Sagani / Global News

Appendix 5

FINTRAC's Update on the Real Estate Sector: Meeting with the
Canadian Real Estate Association, Presentation – August 7, 2019



FINTRAC's Update on the Real Estate Sector

**Meeting with the Canadian Real Estate Association
August 7, 2019**

Presented by:

Annie Bédard - Manager, Compliance Sector, FINTRAC

Guillaume Giguère, Team Leader, Compliance Sector, FINTRAC



Presentation Overview

- ▣ SNAPSHOT OF 2018-19 EVENTS & ACTIONS
- ▣ FINTRAC's COMPLIANCE FRAMEWORK
- ▣ FINTRAC's ASSESSMENT APPROACH
- ▣ 2018-19 COMPLIANCE EXAMINATION FINDINGS
- ▣ GOING FORWARD



Snapshot of 2018-19 Events and Actions

- Extensive media coverage of the vulnerabilities of the real estate sector to money laundering:
 - “Money Laundering funded 5.3B in BC Real estate purchases in 2018” *CBC – May 8, 2019*
 - “Toronto’s real-estate market risky for money laundering, with \$28B in opaque investments: report” *Global News – March 21, 2019*
 - “Millions in real estate linked to B.C. money-laundering investigations is 'owned' by nominees” *Vancouver Sun – April 30, 2019*
- British Columbia Government implemented new measures and commissioned three studies focused on money laundering to identify gaps and potential solutions;
- Government of Canada and B.C. Government created an Ad Hoc Working Group on Real Estate to further identify gaps and find ways to strengthen the AML/ATF Regime; and
- Funding was allocated to FINTRAC in the Federal Budget 2019 to increase the number of examinations and outreach in the real estate and casino sectors, with a focus on British Columbia.



FINTRAC's Engagement with the Real Estate Sector

■ Reporting Entities and Industry Associations

- Bilateral meetings with associations such as CREA and some real estate boards;
- Speaking at AML/ATF conferences and symposiums;
- Co-chairing the Guidance & Policy Interpretation Working Group where all reporting entity sectors are represented;
- Three STR guidance documents were published in January 2019 that explain how to identify and report suspicious financial transactions, as well as provide sector-specific ML/TF indicators.

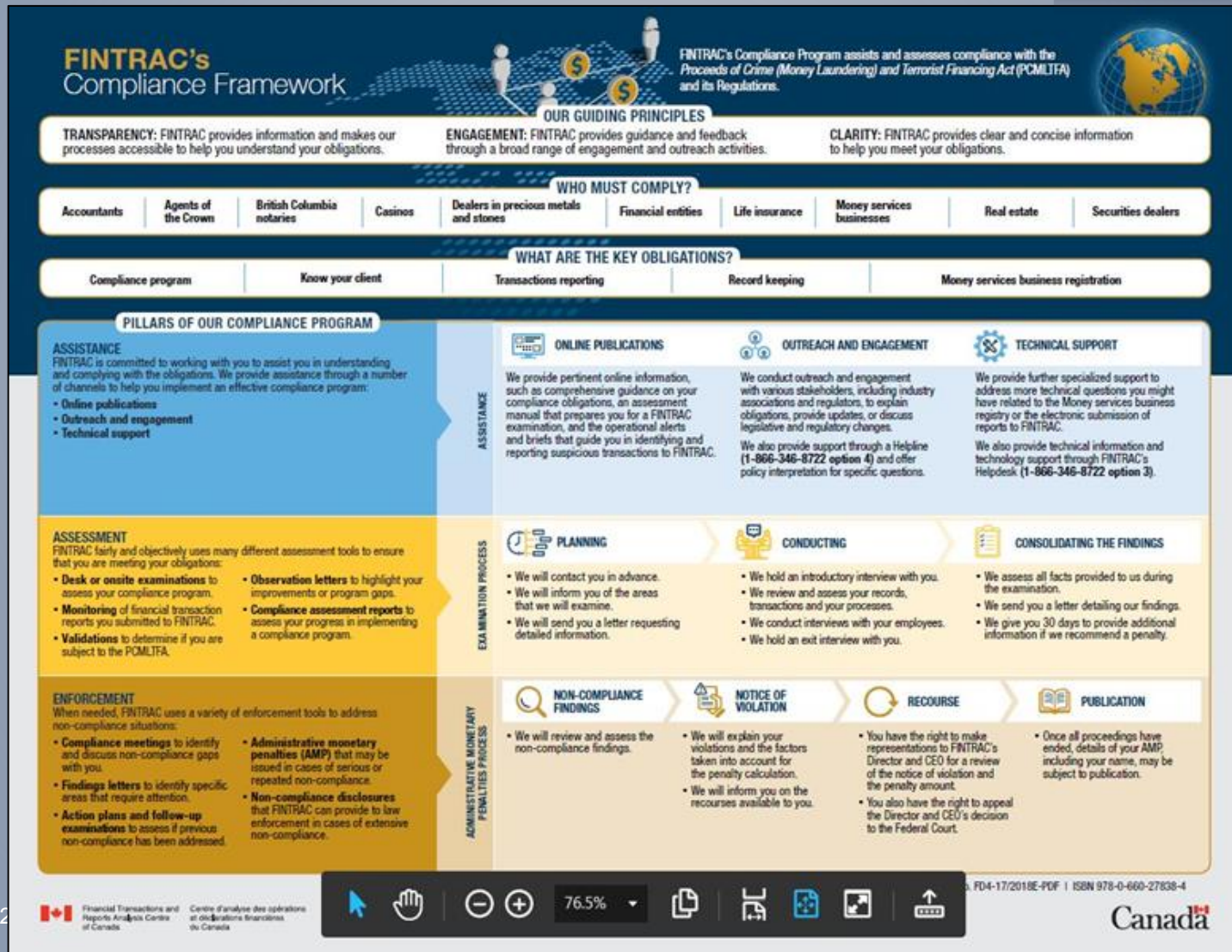
■ Other Regulators

- Regular meetings with provincial real estate regulators and assisting them in the development of training; and
- FINTRAC signed a new MOU with the Real Estate Council of BC in March 2019.



FINTRAC's Compliance Framework

FRAMEWORK





FINTRAC's Transparency Initiative

▣ **FINTRAC Assessment Manual**

- ▣ Prepares REs for a FINTRAC examination, providing an understanding of the examination process and methods, including how FINTRAC utilizes its assessment approach in assessing the effectiveness of their compliance programs.

▣ **Revised AMP Policy**

- ▣ Serves to ensure that REs understand how FINTRAC calculates penalties, while taking into account the concept of “harm done”.

▣ **Voluntary Self-Declaration of Non-Compliance (VSDONC) Public Notice**

- ▣ Encourages REs to comply by coming forward with self-identified non-compliance, while having certainty on FINTRAC's approach and response.



FINTRAC's Evolution to an Assessment Approach

Why the shift?

- ▣ Natural starting point of the regime was on technical compliance, where compliance was assessed on individual requirements.
- ▣ As the program matured there has been a progressive and natural shift to an assessment approach.
- ▣ Under this approach, all deficiencies identified are cited, however, findings are presented holistically, identifies the root cause and reflects harm associated with the non-compliance.



FINTRAC's Evolution to an Assessment Approach (cont'd)

What is the assessment approach?





Administrative Monetary Penalties (AMP) Program

Revised AMPs Policy

- ▣ FINTRAC undertook a comprehensive review of its Administrative monetary penalties program to address decisions of the Federal Courts in 2016.

Revisions to the AMP Program, include:

- ▣ Ensuring that it considers the unique factors in each case to determine the penalty amount, based on the harm caused by the violations committed;
- ▣ Ensuring that the factors that lead to the penalty calculation are clearly outlined; and
- ▣ Publishing its enhanced Administrative monetary penalties policy for greater transparency.

Public Naming Changes

- ▣ As of June 21, 2019, FINTRAC will make public all AMPs imposed.



2018-19 COMPLIANCE EXAMINATIONS FINDINGS

- ▣ 190 compliance examinations in the real estate sector
 - 72 onsite examinations
 - 118 desk examinations

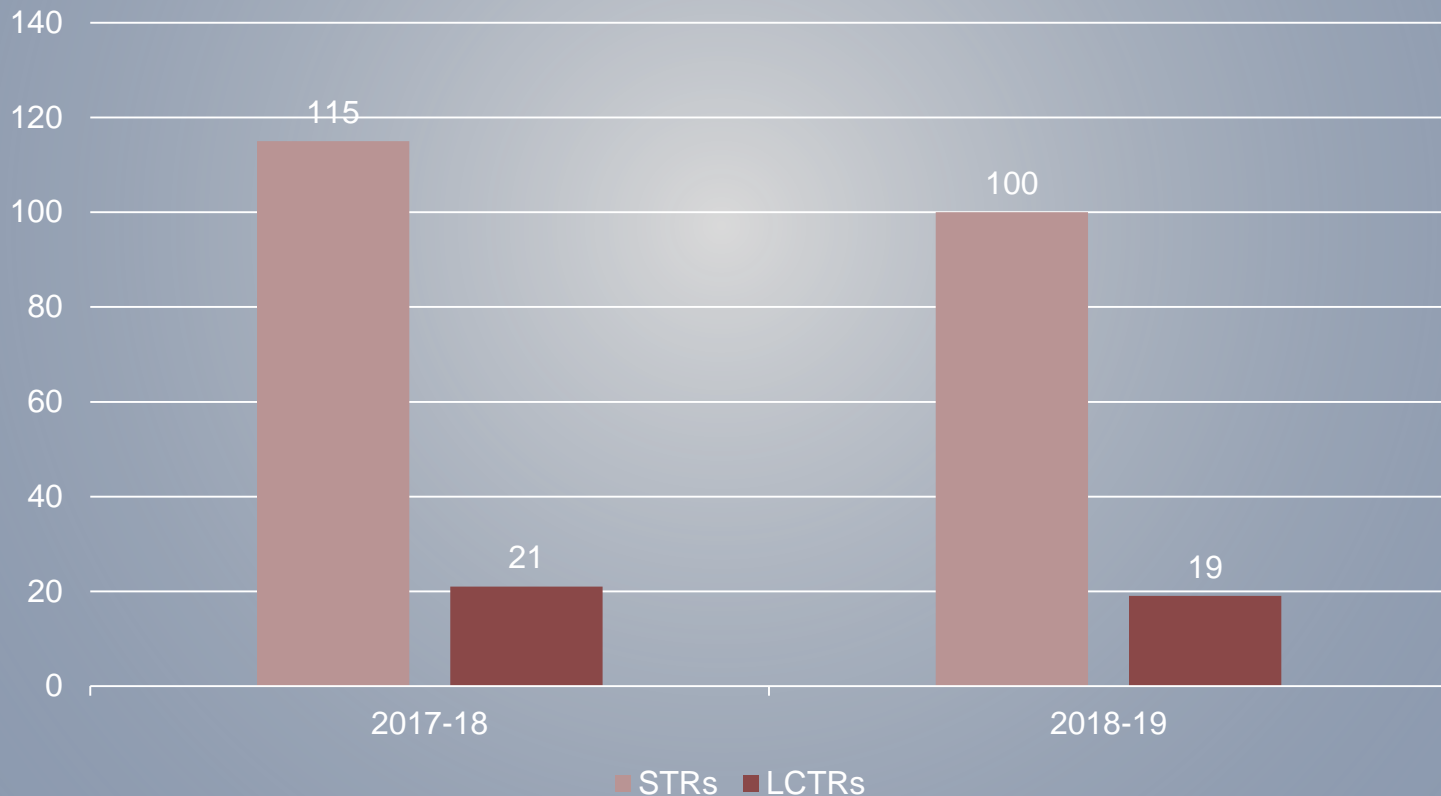
- ▣ In regards to their obligations, reporting entities in the sector performed well in the following areas (*Note: below is the % of exams where the element was scoped in and found to be fully compliant*):
 - Compliance Officer (94% compliant)
 - Third Party determination (94% compliant)
 - Ascertaining ID (74% compliant)

- ▣ Areas in the sector where we identified the highest level of non-compliance were in the following areas (*Note: below is the % of exams where the element was scoped in and found to be partially or fully non-compliant*):
 - Risk assessment (95% were deficient)
 - Policies and procedures (75% were deficient)
 - Record Keeping (73% were deficient)



Reporting Volume for the Real Estate Sector

Number of Reports Submitted by the Sector
in 2017-18 and 2018-19



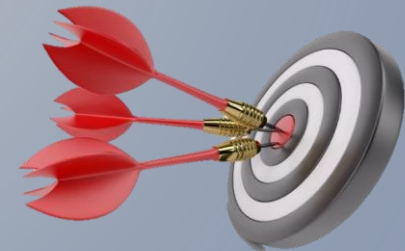


GOING FORWARD



Going Forward

- ▣ Publication of Harm Done Guides in the fall;
- ▣ Implement an enhanced examination methodology with an educational component;
- ▣ Increase number of examinations in British Columbia;
- ▣ Implementation of recent regulatory amendments;
- ▣ Continue to engage with industry associations, reporting entities and regulators; and
- ▣ Develop new communications products.



The background of the slide features a network diagram with white human figures connected by lines, overlaid with various currency symbols (Dollar, Euro, Pound, Bitcoin, Yen) on a blue dotted grid. At the bottom, a globe shows North America in orange.

Feedback and Questions

Appendix 6

A Guide for Developing a Notary Practice Risk Assessment
Program – July 2018

A Guide for Developing a Notary Practice Risk Assessment Program

Prepared For:
The Society of Notaries Public of BC



July 2018

Developed By:
About Business Crime Solutions Inc.
Merrickville, Ontario

Table of Contents

Page

1.0	Introduction	3
2.0	Some Background.....	4
2.1	BC Notaries and Risk Assessment Programs	4
2.2	Structure of the Risk Assessment Program	4
3.0	Practice-Based Risk Assessment	5
3.1	Step One: Defining Your Practice	5
3.2	Step Two: Defining and Measuring Risk	9
3.3	Step Three: Arriving At Your Practice Risk Rating	12
3.4	Step Four: Calculating the Practice Risk Level	22
4.0	Clients and Business Relationships	22
4.1	Business Relationships	22
4.2	Obligations Once a BR is Created	24
4.3	Linking the BR to Your RAP	24
4.4	Step One: Defining Client Risks	25
4.5	Relationship-Based Risk Assessment Overview	26
4.6	Step Two: Client Risk Assessment Questionnaire	27
4.7	Step Three: Mitigating Client Relationship Risk	30
4.8	A Final Few Words on Business Relationships	31
5.0	Structuring the Risk Assessment Program Manual	32

1.0 INTRODUCTION

In 2008, the Government of Canada introduced amendments to the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and its Regulations to enhance the Canadian anti-money laundering and anti-terrorism financing (AML/ATF) programs required of the various reporting sectors subject to the legislation. As part of these amendments, the Risk-Based Approach (RBA), which requires reporting entities to conduct assessments of their exposure to money laundering and terrorism financing risk using a number of prescribed criteria, was introduced.

Subsequent to these amendments FINTRAC has developed three separate documents that provide both general and notary-specific information when it comes to preparing and managing a notary practice Risk Assessment Program (RAP). For ease of reference the links to these three documents are listed here:

- **Compliance Program Requirements:**

- <http://www.fintrac.gc.ca/guidance-directives/compliance-conformite/Guide4/4-eng.asp>

- **Risk-Based Approach Guide:**

- <http://www.fintrac.gc.ca/guidance-directives/compliance-conformite/rba/rba-eng.asp>

- **Risk-Based Approach Workbook for British Columbia Notaries:**

- <http://www.fintrac.gc.ca/guidance-directives/compliance-conformite/rba/rba-bc-eng.asp>

Taken collectively the three documents provide the necessary background, risk management theory and generic models that can be used by a notary to develop and prepare a RAP that applies to the operational aspects of their specific notary practice.

The Risk Assessment Program is one of the five pillars to a reporting entities AML/ATF Compliance Program. Specifically, the RAP must be designed:

- To assess and document those risks associated with money laundering and terrorist financing that can impact on a notaries practice in BC; and
- To document and implement mitigation measures designed to deal with the identified risks.

The resultant RAP must be specific to the notaries practice and be sufficiently dynamic that it can be updated, expanded and modified to manage the changes in the practice itself; the changes brought on by legislative enhancements and amendments; and new trends and products impacting the delivery of services to the practices clients.

The RAP must work with the differences in the application of standardized services found in each notary practice. It must work with the various nuances found in the standardized services delivered by the individuals working within the practice. The RAP must address the regulatory requirements that apply to the design and delivery of risk management within the practice. And foremost, the RAP must include common sense controls and effectiveness measures that enable those notaries responsible for the practice to monitor and rely on its comprehensiveness, efficacy, outcomes and intended impacts.

A Risk Assessment Program should always be viewed as a ‘work in progress’ and not simply a

manual of things to do. Clients change, services change, the law changes, regulatory requirements change and money laundering practices/trends change --- so must the RAP keep pace with these changes.

Designing a focused Risk Assessment Program that: meets the legislative expectations; is representative of a notaries practice; is clear, comprehensive and accurate in its content; and, can be applied, enhanced, measured and remediated when necessary is the goal of this Guide supported by the descriptive content and examples used to help clarify the detail and its application.

2.0 SOME BACKGROUND

2.1 BC Notaries and the Requirement to Develop a Risk Assessment Program

BC Notaries have been designated as a reporting sector under Section 33(1) of Canada's Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations. You have specific regulatory requirements when engaged in any of the following activities on behalf of any individual or entity:

- receiving or paying funds (other than those received or paid for professional fees, disbursements, expenses or bail);
- real property or business assets or entities; or
- Transferring funds or securities by any means.

Common services related to these activities include: real estate conveyances; and, assistance with mortgage preparation and registration. Assessing, documenting, managing and mitigating the risks for possible money laundering and terrorist financing associated with these activities and services is the foundation for the risk assessment program.

2.2 Structure of the Risk Assessment Program

A notary practice risk assessment program looks at risk at two distinct levels:

A. Your Practice

This includes looking at those services provided through your practice; the various ways you deliver those services to your clients; the locations where your practice operates; and other relevant factors that impact on the practice and give rise to potential risks.

B. Your Clients and the Business Relationships You Have With Them

This includes the services your clients use and the methods they use to access those services; the locations where your clients live and do business; and their activities, transaction patterns, and other relevant factors specific to the way you both do business together.

Both levels require you to ask a variety of questions, using the answers to those questions to identify three specific things:

1. The factors that best describe what your practice is all about;
2. The types of clients who use your services; and
3. The relationship that exists between your practice and your client-base.

Let's walk through the various steps associated with each level and by doing this, your Risk Assessment Program will take shape.

3.0 PRACTICE-BASED RISK ASSESSMENT

3.1 STEP ONE – Defining Your Practice

The easiest way to get the true picture of your practice is to ask yourself a variety of descriptor questions. The answers to which will provide an overview on the size, scope and diversity with which your business operates. Each element of that overview must then be assessed as to the degree of risk it brings; how that risk can be controlled; and whether you are willing to accept any risk that remains after those controls are applied.

- **Type of Practice:**

What kind of practice do you operate?

- Sole Practitioner Yes ____ No ____
 - Partner or Association with other Notaries Yes ____ No ____
 - Practice is part of a multi-service¹ group of practitioners Yes ____ No ____
 - Do you have a different model? Yes ____ No ____
 - If yes, briefly describe it _____
-

How long have you been practicing as a notary?

- New to 2 years Yes ____ No ____
-

¹ Immigration consultants, accountants, lawyers, realtors, mortgage brokers and/or others.

- 2 to 5 years Yes _____ No _____
- 5 to 10 years Yes _____ No _____
- 10 to 20 years Yes _____ No _____
- More than 20 years Yes _____ No _____

How many individuals work in your practice? _____

- How many are full time employees? _____
- How many are part time/occasional employees? _____

What is your employee turnover rate?

None _____ Low _____ Moderate _____ High _____

• **Location of Your Practice:**

How many locations does your practice have? 1 ____ 2 ____ 3 ____ 4 or more (specify) _____

Is/are your office location(s) in BC only? Yes ____ No ____

List the community or communities where your practice has office locations:

Do you have any affiliate locations outside of BC²? Yes ____ No ____

- If yes, where?

Is your office location in or near a port? Yes ____ No ____

Is your office location near an International Border? Yes ____ No ____

• **Define Your Client-base:**

Is your client-base restricted to the community where your office(s) is/are located? Yes ____ No ____

If your clients come to you from different parts of BC, list those locations:

² For example, you use referral agencies in other countries to send you clients. Or, you firm is a member of an international network of notary practitioners? Or, you have partnered with real estate finder agencies in other countries who refer clients interested in buying or selling property in BC.

Do all your clients reside in British Columbia? Yes ____ No ____

Do you have clients who live in other parts of Canada? Yes ____ No ____

Do you have clients who live in other countries³? Yes ____ No ____ if yes, list countries:

What percentage of your clients have used your services once only? _____%

What percentage of your clients are repeat clients? _____%

What percentage of your clients are related to you? _____%

What percentage of your clients are related to other of your clients? _____%

What percentage of your clients are walk-ins⁴? _____%

What percentage of your clients are referrals from other real estate professionals⁵?
_____%

What percentage of your clients are referrals from other clients? _____%

What percentage of your clients come to you as a result of advertising or marketing?
_____%

Have you ever turned a potential client away? Yes ____ No ____

- If yes, identify the reason(s)

• **AML-Regulated Services Provided through Your Practice:**

Which of the following AML-Regulated services does your practice provide?

- Residential property transfers (including float homes and manufactured homes) ____
- Commercial property transfers ____
- Transferring funds related to real estate ____
- Small Business transfers ____

³ For example: USA, China, Japan, Philippines, Russia, others.

⁴ Clients who seek out a notaries services through their own efforts. (i.e. not a referral)

⁵ For example: Realtors, mortgage brokers, lawyers, title insurance companies, property surveyors

- Transferring funds at request of a client⁶ _____
- Regulated FI mortgage refinancing _____
- Mortgage lending through private funds _____

What is the percentage of transactions undertaken in each of the above checked off services within a 12-month period? (Total should be 100%)

- Residential property transfers _____
- Commercial property transfers _____
- Small Business transfers _____
- Transferring funds at request of a client⁷ _____
- Mortgage lending through private funds _____
- Regulated FI mortgage refinancing _____

Do you have plans to expand the AML-regulated services in the near future? Yes _____ No _____

If yes, which services?

Will your new services be offered locally only _____; BC-wide _____; across Canada _____; or internationally _____? (Check all that apply)

Having generated the answers to these questions, you have now created content essential for two things.

- **A comprehensive summary of your practice.** This summary sets out briefly the various parameters of your working world, specifically: where you work; who, if any, do you work with; the size of your practice; how long you have been in practice; origin of your client base; and how far the reach of your practice is. The summary should be placed in the opening part of the RAP so that any reader will get a clear snapshot of the structure and client-base that comprises your practice. The summary will provide any regulatory examiner or your biennial review consultant, tasked with auditing your AML/ATF Compliance Program, some sense of the scope of risks your RAP will need to address at both your operations and client levels. A word of caution about the summary, ensure that you keep it current. The RAP is a dynamic document, and like everything else in life, as your practice grows and changes so should the summary. Examiners and auditors focus on what your practice is all about at the time of their visit. They then compare your Compliance Program, as you have set it down on paper, with what they observe --- limitations, if they exist, will very quickly emerge and you, or your practices compliance officer, will be asked to explain and possibly cited for the short comings.

⁶ For the purchase of high end goods; estate payments; and the like.

⁷ For the purchase of high end goods; estate payments; and the like.

- **The beginnings of your practice-based risk assessment.** As indicated earlier your businesses RAP must address the AML/ATF risks associated with your practice in general plus those generated by your clients and the business relationships you have with them. The practice-focused risks are those associated with the services offered; locations where you do business; methods you use to provide your services; and other associated factors⁸ that come with risks that need control. The next segment of this Guide will address practice-based risks; but first we will take a closer look at defining risk --- inherent, residual and acceptable; measuring the degree of risk associated with each factor; and subsequently putting in place the necessary controls and risk-mitigation measures that manage risk acceptable to your business-model.

3.2 STEP TWO – Defining and Measuring the Risks

A generic **definition of risk** can read something like this:

Risk can be seen as a combination of the chance that something may happen and the degree of damage or loss that may result if it does occur. The definition includes two components:

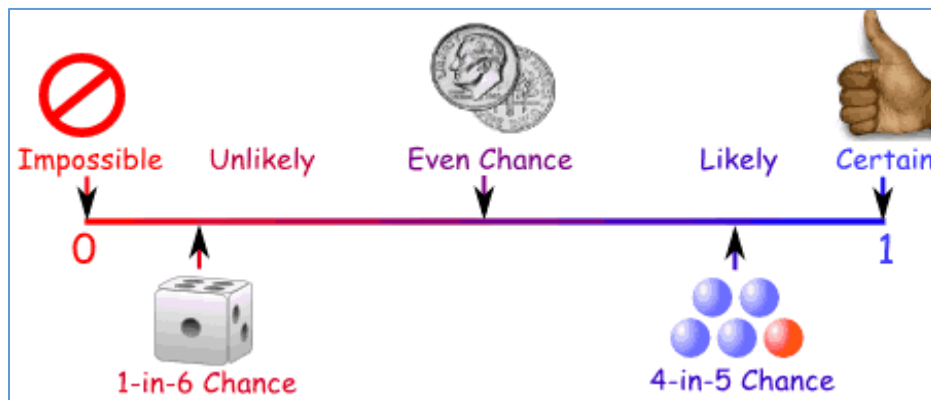
- (a) The **probability** (likelihood) that a harmful event will occur; and
- (b) The **amount of loss** (cost) that will result from the event.

For example, if you find yourself driving your car in a snow storm, there is a risk that you could slide off the road and hit a tree (the harmful events) and damage your car (the loss). The amount of risk from this dilemma can be determined by estimating the likelihood that you could slide off the road and hit a tree and the amount it would cost you to repair your car.

- Now consider the **probability component**, what does that entail? **Probability** is the measure of the likelihood that a certain event will occur. In other words, what are the chances something will occur?

Money laundering or terrorist financing can't be predicted with total certainty. The image below gives you a picture of what this means.

⁸ These factors can include such things as: regulatory demands; market trends; data-base controls; and, competition pressures.



Take a look at the following example:

If you put a million dollars in a bank vault but leave the vault door and the bank door wide open, turn off the video cameras, and send all the employees, including the security guards, home for the weekend, there is almost a 100% 'Probability' that when you arrive at the bank on Monday the 'Cost' will be the loss of one million dollars.

Now, think about probability if you factored in any of the following to this scenario:

- What would be the Likelihood if you had left the video camera on over the weekend?
- What if you just locked the front door but left the door to the vault wide open?
- What if you locked all the doors, turned on the detection equipment, and had security guards periodically inspect the premises?
- Would the Probability be finally zero? **No.**

Why is that?

No controls are perfect. Guards can be bribed. Locks can be broken. There will always be a possibility, no matter how remote, someone will find a way to steal the money. Unless you decide to shut down the bank and get out of the business, there will always be a residual risk that a criminal will want to manipulate to find a way to subvert the controls. The best we can say is how likely a risk will happen and subsequently, identify what methods you can put in place to mitigate, or lessen the risk to the point that it can be tolerated and controlled.

- **Categories of Risk**

For the purposes of your RAP development, you will need to focus on two categories of risk --- **Inherent and Residual**. **Inherent risks** are those risks that come with the services, delivery methods, locations, clients and other relevant factors that make up your practice. They are the risks you must try to control through mitigating practices, resulting in what we refer to as the outcome, or **residual risk**.

You must then decide whether you can live with the residual risk or not --- in other words will you be able to tolerate the risk? If not then you should not allow that as part of your practice. If you can, then the issue becomes how good you can keep it under control. On a macro-level your controls will define what customers you will do business with; where you will do business; what services your practice will offer; and how your services will be delivered to your clients.

- **Developing a Risk Measurement Scale**

We have been talking about the probability of some factor or activity associated with your notary practice putting you and your practice at risk for money laundering and/or terrorist financing taking place. But before we look at these, these risks need to be assessed or measured in terms of the **likelihood** that they will occur.

You start by developing a **likelihood scale**. It refers to the potential of a ML/TF risk occurring in your business for the particular risk being assessed. You can define as many levels of likelihood as you believe are necessary for your particular practice, but keeping the levels to small number will prevent you from reading too much into the amount of risk a factor carries with it. In other words, too many shades of grey will only serve to complicate your RAP and increase the risk that a regulator will find fault with your management of the risks.

That being said, it is proposed that you use a four-level scale: **Low, Medium, High and Not Applicable (NA)**. Putting these levels into a Table, what you will have looks like this:

TABLE 1: RISK LEVEL DESCRIPTIONS

RATING	DESCRIPTION/LIKLIHOOD OF A ML/TF RISK
Not Applicable	The risk rating is not relevant to your practices inherent risk rating matrix
Low	The risk is very unlikely to occur in your practice
Medium	The risk may occur in your practice but can be mitigated with controls
High	The risk will most likely occur and requires strong controls to be acceptable to your practice or will be viewed as unacceptable

Having set your risk tolerance scale, it will be important to arrive at an overall risk rating for your practice. This overall rating will be a summation of the individual risks associated with each element and activity that occurs in your practice. The simplest and most practical approach to scoring risk is to assign a number to each rating and the total of all those numbers will give you a score that corresponds to one of your risk ratings.

Keeping with the rating Table above, the associated scores can be assigned as follows:

TABLE 2: RISK LEVEL SCORES

RISK-LEVEL	ASSIGNED SCORE
------------	----------------

Not Applicable	0
Low	1
Medium	2
High	3

Now, having set the mechanics of what levels of risk to use and what value to assign to each level, the next step is to create a Table, which identifies those elements and activities that make up your practice; identifies the inherent risk level of possible money laundering and/or terrorist financing that is present; give the reason(s) behind the assigned level; identify what controls will mediate the risk; assign the residual risk remaining given the controls; assign a score to the residual risk level; and then specify whether you will tolerate that risk or not.

3.3 STEP THREE – Arriving at your Practice Risk Rating

Time to revisit the responses and detail you have generated from the various questions you posed about your practice, examples of which were listed earlier in Section Two of this Guide. The first step will be to assign the various factors/activities to those categories specified by FINTRAC as being part of your risk assessment, specifically: services provided; delivery methods for those services; the geographic factors associated with your practice; your client-base; and finally, other factors that can play an impact on your overall risk.

TABLE 3: CATEGORIES OF FACTORS/ACTIVITIES ASSOCIATED WITH YOUR PRACTICE

SERVICES	DELIVERY METHODS	GEOGRAPHIC FACTORS	CLIENTS	OTHER
-Residential Conveyance	- In-person only	-1 office location	-Local residents only	-Regulatory requirements
-Commercial Conveyance	-By phone only	-2+ office locations in BC	-Across the province	-Part of a multi-service practice
-Transferring funds related to real estate	-Combination method	-Locations in other provinces	-Other provinces & Territories	-Affiliation with international associations
-Small Business transfers	-Agent or mandatary	-Located in a port	-Foreign Nationals	-Use software to manage client files
-Transferring funds at request of a client ⁹	-Web-Based Only	-Located near an international border	-Referral clients <ul style="list-style-type: none"> • Family/Friends • Other clients 	-Staff turnover
-Regulated FI mortgage refinancing			-Walk-in clients	-Marketing strategies
-Mortgage lending through private funds			-Repeat clients	

⁹ For the purchase of high end goods; estate payments; and the like.

The various factors in each category are now transferred to a Table that provides an assessment of each factor with respect to: its application to your practice; the chosen inherent risk rating; the rationale supporting that inherent rating; whether you will simply accept or need to mitigate that risk; what mitigation measures you have put in place; the subsequent residual risk level associated with the risk; will you tolerate the risk; and finally a value placed on the residual risk.

The residual risk value assigned to each factor will equal one of the assigned scores found in Table 2 above. Those scores will be subsequently totaled and the number will fall into one of the assigned risk level ranges. That risk rating represents your *Practice Risk Score* and could change or remain the same at your next scheduled risk assessment review period.

Remember, your RAP is a dynamic process and as you add, change, or delete various factors applicable to your practice the risk level could change dependent on the score resulting from your review.

Table 4, provides an example of how to risk assess the various factors relevant to your practice. The list of factors by category set out in Table 3 have been used and the risk score subsequently calculated to determine your *Practice Risk Score*.

- **A Few Important Risk Rating Facts Associated With BC Notaries**

Before starting the risk rating process it is important to take note of a number of risk ratings currently established for your sector and the primary services you provide in your practice. In 2015 the Federal Department of Finance released an *Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada*. This document gave *British Columbia Notaries* a **Medium-Vulnerability Rating** with respect to their inherent vulnerability to impacts from money laundering and/or terrorist financing. That same assessment ranked *real estate agents and developers*, the central figures in real estate deals, as having a **high vulnerability rating**; and, *domestic banks*, that provide the financing in many real estate deals, received a **very high vulnerability rating**. Taken together these ratings suggest that a notary practice without the appropriate mitigating measures in place would be viewed closer to the higher end of the risk scale.

Table 4, over the next several pages, provides a condensed summation of some of the categorical risks associated with a notary practice. The items are not meant to be all encompassing. Additional risk factors identified by the individual preparing the RAP should be included in the Table that reflects your specific practice.

TABLE 4: NOTARY PRACTICE RISK ASSESSMENT OVERVIEW TABLE

Source of Risk	Applies to Practice	Inherent Risk Rating	Rationale for Risk Rating	Accept/Mitigate/NA	Mitigation Measures	Residual Risk	Acceptable Risk Tolerance	Risk Score
	Y/N	L/M/H				L/M/H	Y/N	0 to 3
Services Provided								
1. Residential Conveyancing	Yes	High	Canada's 2015 National Risk Assessment gave a high vulnerability rating for ML/TF to the real estate sales and development sector. In addition, law enforcement in BC have found real estate sales closely aligned with the ML activities of organized crime groups and the movement of funds out of Pacific Rim countries by identified officials caught up in corruption.	Mitigate	<ul style="list-style-type: none">• Client Due Diligence is required on every residential transaction.• <i>ABC Notary Practice</i> uses the detailed KYC forms included as part of the conveyancing software provided by our supplier. Those forms include capturing client and any applicable 3rd-party information.• All clients with established Business Relationships (BR) are risk rated and ongoing monitoring period set. High risk BRs also undergo Enhanced Due Diligence (EDD) procedures.• Training of employees includes specific detail for managing client.• All conveyancing transactions are reviewed by compliance to confirm required details are present and meet regulatory requirements.	Medium	Yes	2
2. Commercial Conveyancing	Yes	High	Canada's 2015 National Risk Assessment gave a high vulnerability rating for ML/TF to the real estate sales and development sector. In addition, law enforcement in BC have found real estate sales closely aligned with the ML activities of organized crime groups and the movement of funds out of Pacific Rim countries by identified officials caught up in corruption.	Mitigate	<ul style="list-style-type: none">• Client Due Diligence is required on every commercial transaction.• <i>ABC Notary Practice</i> uses the detailed KYC forms included as part of the conveyancing software provided by our supplier. Those forms include capturing client and any applicable 3rd-party information.• All clients with established Business Relationships (BR) are risk rated and ongoing monitoring period set. High risk BRs also undergo Enhanced Due Diligence (EDD) procedures.• Training of employees includes specific detail for managing client.• All conveyancing transactions are reviewed by compliance to confirm required details are present and	Medium	Yes	2

3. Small Business Conveyancing	Yes	High	Cash intensive small businesses are recognized by the FATF and FINTRAC as the perfect opportunity to comingle dirty money with legitimate. Foreign nationals immigrating to Canada can invest in local small businesses to provide an income once they have moved. Organized crime groups according to the RCMP use small businesses as cover for selling their illegal products and comingling the illegal profits with those of the business and place them into the banking system.	Mitigate	<p>meet regulatory requirements.</p> <ul style="list-style-type: none"> Client Due Diligence is required on every commercial transaction. ABC Notary Practice uses the detailed KYC forms included as part of the conveyancing software provided by our supplier. Those forms include capturing client and any applicable 3rd-party information. All clients with established Business Relationships (BR) are risk rated and ongoing monitoring period set. High risk BRs also undergo Enhanced Due Diligence (EDD) procedures. Training of employees includes specific detail for managing client. All conveyancing transactions are reviewed by compliance to confirm required details are present and meet regulatory requirements. 	Medium	Yes	2
4. Mortgage Lending through Private Funds	No	Medium	Private lending can involve funds where their source is not known. For example, organized crime groups can use third parties as lenders who in turn place illegal funds as private mortgages. Clients who do not qualify for traditional mortgages are willing to borrow private money at higher interest rates to purchase property or a small business. BCs property market is very desirable and competitive at this time.	NA	<ul style="list-style-type: none"> Not willing to risk the possibility of being a source for money laundering. 	Medium	No	0
5. Regulated FI Refinancing	Yes	Medium	Funds are coming from a regulated Canadian FI with a compliance program that manages the risks, if any, associated with the funds at its disposal for financing purposes.	Accept	<ul style="list-style-type: none"> FI compliance practices and ABC Notary Practice CDD requirements provide controls for managing transaction risks. All clients with established Business Relationships (BR) are risk rated and ongoing monitoring period set. High risk BRs also undergo Enhanced Due Diligence (EDD) procedures. Training of employees includes specific detail for managing client. All conveyancing transactions are reviewed by compliance to confirm 	Medium	Yes	2

					required details are present and meet regulatory requirements.			
6. Transferring Funds for Client	Yes	Medium	Not necessarily clear what the sources of the funds are. Movement of large amounts of client funds without acceptable explanation. Beneficiary does not match purpose of funds or involved with groups/sectors known to be suspicious for ML/TF activities.	Mitigate	<ul style="list-style-type: none"> • Maintain CDD practices supported by Source of Funds declaration and relationship review of beneficiary. • Where possible undertake media search on client and beneficiary. • Monitor beneficiary against sanctions and OSFI lists if amounts are excessive and being sent overseas. 	Low	Yes	1
7. Transferring Funds Related to Real Estate	Yes	High	Growing evidence that real estate transactions can have direct links to organized crime activities or those who have used organized crime groups to fund their needs (e.g., gambling, illegal drug-use).	Mitigate	<ul style="list-style-type: none"> • Maintain CDD practices supported by Source of Funds declaration and relationship review of beneficiary. • Where possible undertake media search on client and beneficiary. • Monitor beneficiary against sanctions and OSFI lists if amounts are excessive and being sent overseas. 	Medium	No	2
DELIVERY METHODS								
1. Undertake Transactions in Person Only	Yes	Medium	Client always present for all transaction activities. Cooperative with all CDD, Source of funds, and other detail requests.	Mitigate	<ul style="list-style-type: none"> • Current Notary Practice compliance program readily identifies possible red flags associated with client and transaction itself. • Employees trained to watch for possible ML/TF red flags associated with client and transaction. • All conveyancing transactions are reviewed by compliance to confirm required details are present and meet regulatory requirements. 	Low	Yes	1
2. Undertake Transactions by Phone Only	No	High	Anonymity risk rises with client as does the risk for provided ID documentation to be fake.	NA	<ul style="list-style-type: none"> • <i>ABC Notary Practice</i> has a policy not to undertake transactions with clients solely using the telephone as the means for providing services. 	High	No	0
3. Undertake transactions using a combination of in-person and telephone communication	Yes	Medium	Some clients initially request services in person but live and work elsewhere resulting in some activities taking place over the phone. Phone activities will be limited to instructions from client and updating of activities. All	Mitigate	<ul style="list-style-type: none"> • Client Due Diligence is required on every transaction. • <i>ABC Notary Practice</i> uses the detailed KYC forms included as part of the conveyancing software provided by our supplier. • All clients with established 	Medium	Yes	2

s.			document signing must be done in person and all required ID information captured in person and confirmed with acceptable ID documents.		<p>Business Relationships (BR) are risk rated and ongoing monitoring period set. High risk BRs also undergo Enhanced Due Diligence (EDD) procedures.</p> <ul style="list-style-type: none"> • Training of employees includes specific detail for managing client. • All conveyancing transactions are reviewed by compliance to confirm required details are present and meet regulatory requirements. 			
4. Use of agents or mandataries to service client requirements.	Yes	High	Agents or mandataries increase risk of anonymity with clients and could fail to implement required compliance practices of <i>ABC Notary Practice</i> .	NA	<ul style="list-style-type: none"> • <i>ABC Notary Practice</i> currently does not rely on the services of agents or mandataries. 	High	No	0
5. Web-Based Transactions	No	High	Increased risk for client anonymity given the non-face-to-face transactions and activity associated with Internet driven transactions.	NA	<ul style="list-style-type: none"> • <i>ABC Notary Practice</i> currently does not undertake any web-based form of providing notary services. 	High	No	0
GEOGRAPHIC FACTORS								
1. Single Office in Community Location	Yes	Low	Maintaining a single office location in the community served enables <i>ABC Notary Practice</i> to control for non-compliance risks associated with multiple-offices or offices in other jurisdictions.	Accept	<ul style="list-style-type: none"> • All transactions run through this single location. 	Low	Yes	1
2. Office located in or close to ports and/or international borders	Yes	Medium	Risk increases for foreign clients crossing borders or stopping in the port to seek out notary to undertake transactions. Ports of entry are viewed as higher risk since there are no local links to established community businesses or service providers that can provide CDD controls.	Mitigate	<ul style="list-style-type: none"> • Client services limited to transactions involving low level dollar thresholds. • CDD is done in person and cross checked with references if needed. • Source of funds identified and confirmed if suspect. • Training of employees includes specific detail for managing non-resident clients. • Employees trained to watch for possible ML/TF red flags associated with client and transaction. 	Medium	Yes	2
3. Two or more locations in community or in other BC communities	Yes	Medium	The more locations services are offered the greater the risk for rogue employees to ignore compliance requirements. Required records can be incomplete if content and quality	Mitigate	<ul style="list-style-type: none"> • <i>ABC Notary Practice</i> employee turnover is very limited with those leaving to take on new jobs/attend school/ or move away. • Location managers review clients and transactions using the 	Low	Yes	1

			review procedures are not available and/or applied consistently.		<i>Practices</i> quality control Form, which are reviewed monthly by Compliance team.			
4. Practice location(s) is in identified high crime rate BC community	Yes	Medium	Higher crime rates increase the risk for known criminals to use the <i>Practice</i> services to clean the proceeds from their criminal activities.	Mitigate	<ul style="list-style-type: none"> Compliance monitors crime rates¹⁰ for the office(s) location(s) using law enforcement statistics, popular media stories, and similar methods. Strict compliance controls activated when a client has a known record for being involved with crime. Transactions which are suspected to be related to the use of proceeds of crime or for terrorist financing are reported using a STR. Client is placed on de-marketed client list so no further transactions will take place. 	Medium	Yes	2
5. Satellite Practice locations are set up outside of BC	Yes	High	Setting up practice offices outside of BC, and in particular, outside of Canada multiplies the risks for ML/TF given: criminal activity in those locations; local ML/TF regulatory requirements that must be followed; anonymity of clients; and the potential for local employees to be influenced by criminals wanting to use the services of your practice.	NA	<ul style="list-style-type: none"> <i>ABC Notary Practice</i> has no plans to expand its presence to communities outside of the Province of BC given the multitude of risks such a move would create. 	High	No	0
CLIENTS								
1. Local residents	Yes	Low	Clients are residents of the BC community in which the Practice is operating. Include individuals who are looking for a notary to assist with a transaction activity (walk-in); individuals who have been referred by someone familiar with the notary; or, a repeat client. Common through all groups is the familiarity with the environment in which they live and work.	Mitigate	<ul style="list-style-type: none"> All CDD requirements must be undertaken regardless of how familiar the client is to the notary. <i>ABC Notary Practice</i> uses the detailed KYC forms included as part of the conveyancing software provided by our supplier. All clients with established Business Relationships (BR) are risk rated and ongoing monitoring period set. High risk BRs also undergo Enhanced Due Diligence (EDD) procedures. Training of employees includes specific detail for managing client. 	Low	Yes	1

¹⁰ A list of links to various crime statistics resources has been included at Appendix A of this Guide.

					<ul style="list-style-type: none"> All conveyancing transactions are reviewed by compliance to confirm required details are present and meet regulatory requirements. 			
2. Clients located in other BC communities	Yes	Medium	Clients currently residing outside of the community where the notary practice is based bring with them the risk factors associated with their home community; the decision to not use a notary in their home community and the unknown rationale for doing this; and the increased anonymity risks associated with serving a client in other regions of the province.	Mitigate	<ul style="list-style-type: none"> All CDD requirements must be undertaken. <i>ABC Notary Practice</i> uses the detailed KYC forms included as part of the conveyancing software provided by our supplier. Training of employees includes specific detail for managing clients from other communities. All conveyancing transactions are reviewed by compliance to confirm required details are present and meet regulatory requirements. 	Low	Yes	1
3. Residents of Other parts of Canada	Yes	Medium	Clients currently residing in other parts of Canada bring with them the risk factors associated with their home community; the decision to use a notary in BC versus a lawyer in their home community and the unknown rationale for doing this; and the increased anonymity risks associated with serving a client resident in other regions of the Canada.	Mitigate	<ul style="list-style-type: none"> All CDD requirements must be undertaken. <i>ABC Notary Practice</i> uses the detailed KYC forms included as part of the conveyancing software provided by our supplier. Training of employees includes specific detail for managing clients from other communities. All conveyancing transactions are reviewed by compliance to confirm required details are present and meet regulatory requirements. 	Medium	Yes	2
4. Foreign Nationals	Yes	High	Foreign nationals bring with them many unknowns --- employment histories, possible criminal records, business background, possible links to corrupt government practices, sources of funds and income, purpose for the transaction and others. Notary access to information to clarify these unknowns is often difficult leaving questions unanswered; or if answered there could be questions about the source. Clients represented by third-parties increases the anonymity risks since no direct contact with the client is ever made.	Mitigate	<ul style="list-style-type: none"> <i>ABC Notary Practice</i> always applies EDD when it comes to foreign national clients. Compliance program requires detailed information about client background, sources of funds, purpose for transaction, and reliable sources confirming the acceptability of the client. Red flags for possible ML/TF activity associated with foreign national transactions are identified, understood and readily applied by practice employees. 	High	Yes	3
OTHER								
1. AML/ATF	Yes	High	The PCMLTFA is a criminal Act and	Mitigate	<ul style="list-style-type: none"> <i>ABC Notary Practice</i> has 	Medium	Yes	2

Regulatory Requirements			carries specific penalties for conviction of an offence under the Act. FINTRAC has the authority to apply Administrative Monetary Penalties (AMPs) if <i>ABC Notary Practice</i> fails to meet its application requirements to such a degree that an AMP is warranted. The risk level is also viewed as high given the dynamic nature of the legislation and the continual changes put into place and new requirements based on the ever changing practices and trends that occur with ML and TF.		implemented all required elements of a BC Notary AML/ATF Compliance Program applicable to its clients and services it provides. <ul style="list-style-type: none"> Both electronic and manual controls are in place to monitor all designated ID, record keeping, reporting and risk management is carried out. Annual assessment practices by compliance and Biennial Reviews are completed, with response plans implemented for identified limitations and deficiencies. 			
2. Association in a multi-service practice	Yes	High	A Notary practice operating in association with other real estate service providers such as Real Estate Brokerages, Mortgage Brokers, Non-Regulated Mortgage Providers, Land Surveyors, Building Inspection firms, and Title Insurance providers are open to client referrals from a business with no requirements under the PCMLTFA or limited commitment to meeting their requirements. Such associations are open to clients from foreign countries where one of the association businesses has referral agents.	Mitigate	<ul style="list-style-type: none"> <i>ABC Notary Practice</i> has implemented all required elements of a BC Notary AML/ATF Compliance Program applicable to its clients and services it provides. Both electronic and manual controls are in place to monitor all designated ID, record keeping, reporting and risk management is carried out. Annual assessment practices by compliance and Biennial Reviews are completed, with response plans implemented for identified limitations and deficiencies. Referral Agreements are in place with associated businesses outlining specific compliance requirements that must be provided with each referral. 	High	Yes	3
3. Software to assist with managing client files	Yes	Low	Compliance software, purchased or practice-developed, are intended to assist with compliance requirements (e.g., records, ID documentation, terrorist and sanction list monitoring) and as such provide control measures that assist with lowering risk and confirming requirements have been met. Risk arises when soft-ware fails to capture information or is under-performing in its control capabilities.	Mitigate	<ul style="list-style-type: none"> Annual testing of software practices will assist in isolating problems, which can be referred to the provider/developer for remediation. 	Low	Yes	1
4. High Level of Staff Turnover	N	Medium	Could be indicative that the practice is continually turning over staff	Mitigate	<ul style="list-style-type: none"> <i>ABC Notary Practice</i> at its inception was foremost a family 	Low	Yes	1

			given risks from employees not following established compliance practices.		<ul style="list-style-type: none"> run practice. As younger family members moved on to other careers, permanent and reliable employees have been hired to replace them and continue with their employment 			
5. Affiliation with International Notary Associations	Yes	Medium	If the affiliation results in the referral of clients from the foreign country, the associated risks cited for foreign national clients will kick in.	Mitigate	<ul style="list-style-type: none"> ABC Notary Practice always applies EDD when it comes to foreign national clients. Compliance program requires detailed information about client background, sources of funds, purpose for transaction, and reliable sources confirming the acceptability of the client. Red flags for possible ML/TF activity associated with foreign national transactions are identified, understood and readily applied by practice employees. Referral Agreements are in place with notary associations outlining specific compliance requirements that must be provided with each referral. 	Medium	Yes	2
6. Marketing Strategies	Yes	Medium	Marketing strategies that target potential foreign clients ¹¹ with potential links to money laundering activities either in their native land or in Canada and BC in particular.	Mitigate	<ul style="list-style-type: none"> Put in place Referral Agreements with agents or referral sources that set out specific compliance requirements that must be provided with each referral. Restrict notary services to residential or commercial property sales and small business conveyances. Refuse to enter into transactions where third parties are used and which involve potential clients from high risk countries who have little or no intention to live in property purchased in BC. 	Medium	Yes	2

¹¹ This includes countries where the media has reported on the movement of funds out of the country by corrupt officials or organized crime groups operating in BC.

3.4 STEP FOUR: Calculating Your Practice Risk Level

Remember, the various risk categories and risks described in Table 4 should be viewed as simply a sampling of those features that can bring a degree of risk to the operation of a notary practice. It is critical that any other features applicable to your practices operations and structure be added to your RAP and subsequently analyzed as demonstrated in this Guide. To help you identify other relevant risks, a quick look at FINTRAC-identified red flags that could surface when carrying out certain activities on behalf of your client may assist you. Such a list can be found on FINTRAC's website at the following link:

<http://www.fintrac.gc.ca/guidance-directives/transaction-operation/Guide2/2-eng.asp#s8-12>

Doing all this work now means that you can calculate your current Practice risk level. Simply total up the risk scores in column 8 of the Overview Table and then compare that total to the risk ranges set out here.

TABLE 5: RISK SCORE RANGES

RISK-LEVEL	SCORE RANGE
Low	0 to 27
Medium	28 to 54
High	55 to 81

Note that the upper end of the risk score range is dependent on the total number of elements included in your Risk Overview Table. With respect to TABLE 4 in this Guide we have 27 elements, which when multiplied by the high risk score of 3, gives a maximum total score for the practice of 81. Deciding on what range of total scores falls into each risk range, we kept it simple by assigning one-third of the total as the low risk range. Adding another one-third to give the medium risk range. And a final one-third to the total representing the high risk range.

4.0 CLIENTS AND BUSINESS RELATIONSHIPS

4.1 Business Relationships

Every BC Notary, as part of their practice Compliance Program, is required to undertake a risk rating of any client who has undertaken within a five year period at a minimum, two transactions where the client's ID documentation has to be shown; or has had two separate Suspicious Transaction Reports (STR), completed and/or attempted, filed on their transactions during the five year period. This pair of transactions, or STRs, have resulted in the creation of a **Business Relationship (BR)**.

The Business Relationship is ongoing until five consecutive years have passed from the most recent transaction where no further transactions having occurred between the client and the notary. At that point, a new BR could be created should the client return to the Notary and undertake two new qualifying transactions. The Business Relationship became a Compliance

Program requirement on February 1, 2014. Therefore, all of the transactions, or reports, that qualify for establishing a BR have to have occurred from that date forward.

So, what would constitute two transactions resulting in the creation of a BR? Quite straight forward actually:

Example One:

- *Client A engages ABC Notary Practice to assist with the sale of her home in Prince George during May 2014 --- ID from Client A is required as part of that sales process. Subsequently, Client A engages ABC Notary Practice to assist with the purchase of her new home in Prince George which closed in August 2014 --- ID from Client A is also required as part of that purchase process. **End result is a new Business Relationship.***

Example Two:

- *Client B engages XYZ Notary Practice to assist with the purchase of a small welding shop in Surrey in July 2017. Client B lives in China currently with plans to immigrate to Canada with his family as soon as they have been approved by the Canadian government. In December 2017, Client B requests the assistance of XYZ to help close the purchase of a home in Richmond, which will be lived in by his son and daughter currently enrolled at the University of British Columbia. **End result is a new Business Relationship.***

In both examples, we have two separate ID-qualifying transactions occurring within 5-years of each other involving the same client. However, if you take example two where Client B purchases the welding business but his son and daughter while studying at UBC decide to pool some of their trust funds to purchase the home in Richmond as an investment but also to live in while going to school, we have a situation whereby two separate client transactions have taken place and no BR will be created. Despite the fact that all parties are from the same immediate family.

Do you have to actually verify the client's ID documents in the second transaction ---as would be the case with Example One? FINTRAC's Business Relationship Guidance has been pretty clear on this and states the following:

"A business relationship is created when a client conducts a second monetary value transaction, *even if you apply the exception to not identify them a second time because you have no doubts about the information you used to identify them previously.*"

4.2 Obligations Once a Business Relationship is Created

Once the BR is created, a Notary is tasked with a series of requirements, those include:

- Keep a record of the *purpose and intended nature of the business relationship*
- Conduct *ongoing monitoring* of your business relationship with your client to:
 - detect any transactions that need to be reported as suspicious
 - keep client identification and beneficial ownership information, as well as, the purpose and intended nature records up-to-date
 - reassess your clients risk level based on their transactions and activities
 - determine if the transactions and activities are consistent with what you know about your client
- Keep *a record of the measures* you take to monitor your business relationships and the information you obtain as a result.

These activities are pretty straight forward, but sometimes compliance officers struggle a bit with defining what is meant by the purpose and intended nature of the business relationship (PIN). FINTRAC best describes it as “... a description of your business dealings with the client “. So when it comes to a notary practice, a PIN could read something like the following as determined by the business transactions that have created the BR:

- Purchasing or selling residential real estate
- Purchasing or selling business assets or entities
- Estate planning

It is important to note that the PIN of a business relationship will change over time if the business activities carried on with your client vary. For example, the sale and purchase of residential property may have been the original reasons for your client using your services; however, over time they may engage you to help with estate planning and/or the operation of their business. Consequently, the PIN needs to change to be more reflective of the overall business you do together. This fact further reinforces the reality that a BR is very much a dynamic, changing, process similar to your overall RAP.

4.3 Linking the BR to your Practice Risk Assessment Program

Now all this discussion about a BR in a Guide that focuses on designing a Practice Risk Assessment Program implies that maybe there is some kind of link between the two. Well there is! The RAP is all about identifying and managing risks with services provided to and the relationship with your clients. Those clients who have used your services on more than one occasion within a 5-year span now qualify as having a business relationship with your practice. Providing an ID-service only once can be viewed as simply a ‘one-off’ situation. But add a second ID required service, within a 5-year period, and the client has become a ‘repeat’ customer that results in the creation

of a BR. Consequently, the newly minted BR with that client has created ongoing risks that need to be managed through the regulated requirements set down by FINTRAC and listed in Section 4.2 above. Assessing the BR clients risk is an integral component of the second part of your practice's Risk Assessment Program --- *the relationship-based risk assessment (i.e. your clients)*. Specifically, Section 2 of FINTRAC's *Risk-Based Approach Workbook for British Columbia Notaries* states:

"If you have a business relationship, you need to make a risk assessment based on the inherent characteristics of your client."

Non-BR clients whose transactions keep them below the ID-threshold do not require you to make a risk assessment. Unless in the process of serving the client a trigger event¹² takes place that prompts you to assign the client a high risk rating. So what's next?

4.4 STEP ONE: Defining Your Client Risks

All BR-clients **plus** those clients outside of a BR-relationship who have been assigned a high-risk rating must be measured against your practice's *Relationship-Based Risk Assessment Overview*. The Relationship-Based Overview assesses client-specific risks using a comparable Table to the one used to look at your Practice Risk Assessment. *Section 4.5* provides an example of the various items such a Table might cover.

In addition, once a client has qualified for a Business Relationship he/she will need to be risk assessed using a tool such as a Customer Risk Assessment Questionnaire. An example of such a questionnaire has been included below in Section 4.6. The questionnaire should be reviewed on a scheduled basis to ensure its continued application to assessing risk level with your practice's clients. A copy of each client's questionnaire should be stored in either a hard-copy or electronic-format as part of their profile. The current-version of the questionnaire will be used again during the client's scheduled review period based on their assigned risk rating.

¹² Client undertakes a transaction that results in the notary filing an STR. The client is elevated to a position of influence in a government bureaucracy. Client has been found guilty for tax evasion.

4.5 Relationship-Based Risk Assessment Overview

TABLE 6: CLIENT-RELATIONSHIP RISK ASSESSMENT OVERVIEW TABLE

Source of Risk	Applies to Practice	Inherent Risk Rating	Rationale for Risk Rating	Accept/Mitigate/NA	Mitigation Measures	Residual Risk	Acceptable Risk Tolerance	Risk Score
	Y/N	L/M/H				L/M/H	Y/N	0 to 3
Non-BR Clients								
8. Occasional client - no ID-required transactions	Yes	Low	Limited or no risk for ML/TF transactions	NA	None	Low	Acceptable	1
9. Occasional client – 1 ID-required transaction	Yes	Medium	Clients who come in occasionally and undertake consistently low \$ transactions but have undertaken a transaction that requires formal ID documentation.	Mitigate	<ul style="list-style-type: none"> Full KYC undertaken and confirmed Source of funds required. 	Low	Acceptable	1
10. Repeat client using a variety of services but no BR	Yes	Low	Limited or no risk for ML/TF transactions	NA	None	Low	Acceptable	1
BR-Clients: Individuals								
1. Clients where BR is generated from real estate transactions alone	Yes	High	Real estate transactions are viewed as high risk transactions for ML/TF according to Canada's national risk assessment. BC-based real estate transactions are currently viewed as being used by organized criminal groups and individuals caught up in corruption practices to launder proceeds.	Mitigate	<ul style="list-style-type: none"> Full KYC undertaken and confirmed with each transaction Source of funds required BR monitoring in effect and EDD measures in place for clients rated as high risk. 	Medium	Acceptable	2
2. Regular/Repeat clients with BR activity from transactions other than real estate conveyances	Yes	Medium	Transactions could involve ML/TF if \$ value is high (\$25K or more) and frequency of occurrence is monthly or more. Transactions by foreign nationals always raises red flags as to source of funds, particularly if funds are from Pacific Rim nations.	Mitigate	<ul style="list-style-type: none"> Full KYC undertaken and confirmed with each transaction Source of funds requested BR monitoring in effect and EDD measures in place for clients rated as high risk. 	Medium	Acceptable	2
3. Clients where BR is established through STR/SATR	Yes	High	FINTRAC automatically requires clients where a STR/SATR has been filed to be rated as high risk.	Mitigate	<ul style="list-style-type: none"> Full KYC undertaken and confirmed with each transaction Source of funds required BR monitoring in effect and EDD measures in place for these high risk clients. 	High	Acceptable (Until De-marketed)	3

Source of Risk	Applies to Practice	Inherent Risk Rating	Rationale for Risk Rating	Accept/Mitigate/NA	Mitigation Measures	Residual Risk	Acceptable Risk Tolerance	Risk Score
	Y/N	L/M/H				L/M/H	Y/N	0 to 3
					<ul style="list-style-type: none"> Review period set at bi-annual to ensure transactions are assessed quickly. 			
BR-Clients: Business								
1. Clients where BR is generated from real estate transactions and/or small business conveyances alone	Yes	High	Real estate transactions are viewed as high risk transactions for ML/TF according to Canada's national risk assessment. BC-based real estate transactions are currently viewed as being used by organized criminal groups and individuals caught up in corruption practices to launder proceeds. Small-business purchases at risk for ML/TF especially if they are cash-based businesses. Purchase of local businesses by offshore businesses is risky given difficulty to confirm beneficial ownership and funds coming from safe-haven jurisdictions.	Mitigate	<ul style="list-style-type: none"> Full corporate KYC undertaken and confirmed with each transaction Beneficial ownership confirmed and EDD done on those individuals Source of funds required BR monitoring in effect and EDD measures in place for clients rated as high risk. 	High	Acceptable (Until De-marketed)	3
2. Regular/Repeat clients with BR activity from transactions other than real estate conveyances/sm all business purchases	Yes	Medium	Transactions could involve ML/TF if \$ value is high (\$25K or more) and frequency of occurrence is monthly or more. Transactions by foreign nationals always raises red flags as to source of funds, particularly if funds are from Pacific Rim nations.	Mitigate	<ul style="list-style-type: none"> Full corporate KYC undertaken and confirmed with each transaction Beneficial ownership confirmed and EDD done on those individuals Source of funds required BR monitoring in effect and EDD measures in place for clients rated as high risk. 	Medium	Acceptable	2
3. Clients where BR is established through STR/SATR	Yes	High	FINTRAC automatically requires business clients where a STR/SATR has been filed to be rated as high risk.	Mitigate	<ul style="list-style-type: none"> Full KYC undertaken and confirmed with each transaction Source of funds required BR monitoring in effect and EDD measures in place for these high risk clients. Review period set at bi-annual to ensure transactions are assessed quickly. 	High	Not Acceptable (De-marketed when STR/SATR filed)	0

4.6 STEP TWO: Develop and Apply a Client Risk Assessment Questionnaire

Risk rating clients who qualify for a BR-status need not be a complex process. An easy method is to use a questionnaire designed to provide a numeric score that corresponds with a set risk level. The questions in the questionnaire should be suited to a 'Yes' or 'No' response, with the final total of 'Yes' responses resulting in a specific risk level --- low, medium or high --- being assigned to your client. A sample of such a questionnaire has been inserted below for your reference.

Client Risk Assessment Questionnaire

Question	Yes	No
1. Client's knowledge of local AML laws, regulations and rules seems excessive.	X	
2. Client never undertakes a face-to-face transaction with practice employees.		X
3. Client only uses 3 rd parties to complete transactions with Notary practice.	X	
4. Client only uses a family member to make remittance payments (3 rd Party transactions), however remittances are ordered by phone by customer.		X
5. Client uses multiple forms to pay required funds for a transaction: cheque, cash, e-transfer or wire transfer.	X	
6. Client currently lives in a country identified as a high risk for money laundering.		X
7. Client lives outside of British Columbia.	X	
8. Client lives in high crime area in British Columbia.		X
9. Client currently lives in a port or border community within BC.		
9. Client changes BC residence every one to two years.		X
10. Photo identification provided is not current, valid and original.		X
12. Business relationship purpose and intended nature of activities raises red flags.	X	
14. A Suspicious Transaction Report (SAT or SATR) has been filed with FINTRAC.		X
15. Customer only pays for transactions in cash.		X
16. Customer pays for transaction with wires in a foreign currency.	X	
17. Value of customer's transactions are inconsistent with their stated occupation.		X
18. Customer is a politically exposed person - (\$100,000.00 EFT).	X	

Similar to determining your Practice risk level the upper end of the risk score range is dependent on the total number of questions included in your Questionnaire. The example questionnaire above includes 18 questions resulting in a maximum total score of 18 'Yes' responses. Using a similar risk-range distribution formula the client rating depending on the total number of 'Yes' responses could be as follows:

TABLE 7: CLIENT RISK SCORE RANGES

RISK-LEVEL	SCORE RANGE
Low	0 to 6
Medium	7 to 12
High	13 to 18

A rating of:

- **LOW:** means that money laundering is unlikely to occur
- **MEDIUM:** means that money laundering is reasonably probable to occur
- **HIGH:** means that money laundering is very probable to occur

In the case of our sample questionnaire, the risk score total of 'Yes' responses is 7; but because this client had Question 18 scored as a 'Yes' the client *automatically defaults* to High Risk. Remember that 'Yes' answers to both questions 14 and 18 are high risk default answers despite what the final total works out to be. Had question 18 not resulted in a 'Yes' response then this client would have fallen into the low-risk category.

The number of questions to include in your client questionnaire is truly up to you. If a risk factor would never occur in your practice, for example you would never provide a service to a foreign national, then it would make no sense to include a question that states the client is a foreign national. Use common sense when deciding on what questions to include and always make sure that each question could apply to your clients resulting in choosing the associated 'Yes' response. Furthermore, always ensure your questionnaire includes questions pertaining to a STR/SATR having been filed plus whether a client is a politically exposed person. I recommend that any PEP (Foreign or Domestic), HIO and family and close associates be ranked at the high level simply because corruption knows no geographic boundaries and for the ease with which defined mitigation measures can be imposed on the continuing business relationship with a PEP-determined client.

4.7 STEP THREE: Mitigating your Client Relationship Risk

Having risk rated your BR- or STR/SATR-client you now have to put in place the following requirements set out earlier in Section 4.2:

- Conduct *ongoing monitoring* of your business relationship with your client to:
 - detect any transactions that need to be reported as suspicious
 - keep client identification and beneficial ownership information, as well as, the purpose and intended nature records up-to-date
 - reassess your clients risk level based on their transactions and activities
 - determine if the transactions and activities are consistent with what you know about your client; and
- Keep *a record of the measures* you take to monitor your business relationships and the information you obtain as a result.

This activity and the supporting record of it is a scheduled requirement for all your client BRs. The frequency of that requirement is dependent on the current risk level assigned to the client. For example, the following schedule of review periods might be adopted by your practice:

TABLE 8: BR RISK LEVEL SCHEDULED MONITORING REVIEW PERIOD

Client Risk Level	Monitoring Review Period
LOW	Every Five Years
MEDIUM	Every Four Year
HIGH	Every Two Years

FINTRAC has established two scheduling parameters which govern review periods. They include:

- High risk client reviews need to be undertaken at minimum once every two years.
- Medium and low risk client reviews can then be staggered after the high risk period but neither must not exceed a five-year period.

Remember that at every monitoring review period you must also re-assess your clients risk level. That means undertaking the current version of your client risk questionnaire. Whatever score results then you need to make a record of that and identify any mitigating activities your risk assessment requires you to undertake at that level. Your client now starts the next cycle of their BR ending on the date associated with their risk level; at which point, you undertake the next monitoring review.

- **Watch Out for Trigger Events**

A trigger event is something that prompts you to spontaneously undertake a monitoring review outside of the scheduled review period for that client. For example, let us say a client is elected as an MLA for British Columbia during a recent provincial election campaign. Their election as an MLA automatically results in a trigger event since they are now a PEP-Domestic. And since we spoke earlier about having PEPs, foreign or domestic, defaulting automatically to a high risk rating then their election triggers the requirement for you to undertake a monitoring review even if their scheduled review would not take place for another 24-months. A similar trigger event would occur if you had to submit an STR or SATR on a client for the first time.

Less obvious trigger events can occur, for example, if a client starts to undertake services with you involving amounts of money that far exceeds what is their normal practice. If anything that should raise a red flag for you and prompt you to revisit the client's BR and determine if more information is required about your client and/or the transaction that prompted the red flag.

Business relationships are definitely dynamic and can change with the changes occurring in the services provided to your client or other non-services factors such as being elected to public office. Consequently, it is extremely important that you take your BR responsibilities seriously. Going forward, a future FINTRAC compliance examination could result in the examiner requesting to see a sample of your client BR records to look for:

- Required details set down in the record;
- Client current risk rating;
- Next scheduled monitoring review date; and,
- The records of all previous monitoring reviews.

Failure to have such records could result in a deficiency noted on your Examination Result's letter.

4.8 A Final Few Words on Business Relationships

A description of your practice BR-program must be set down in your overall Compliance Manual. You must not only describe how a client enters a BR with you but also set out the protocol you have in place to manage the BR. At minimum, you should create a BR record for each client (paper or data file) in which all the required information is captured including the next scheduled monitoring review date. Going forward, whenever the BR is reviewed, scheduled or trigger event, your activities and findings must be recorded, dated and signed off. This cycle repeats itself until the BR can be officially closed --- 5-years after the last transaction took place. Until then the BR is considered active and subject to review by FINTRAC or the consultant undertaking your biennial compliance review.

Including a discussion about your BR program as part of your RAP document is also a good idea since it will demonstrate that you understand the links between the BR and your Risk Assessment Program.

5.0 STRUCTURING THE RISK ASSESSMENT PROGRAM MANUAL

No Guide would be complete without a brief discussion of how to structure the document itself. Common sense with this Guide suggests the structure will follow the style in which the content herein has been presented to the reader. That being said here is a suggested outline to present your RAP narrative.

- 1. Title**
- 2. Table of Contents** [Reference all numbered Sections in your document.]
- 3. Background** [Here you should briefly discuss what a RAP is; the legislation governing its necessity; and its requirement for BC Notaries.]
- 4. Structure of RAP** [Briefly describe how your RAP is to be presented in the document i.e. steps and overall order of presentation.]

5. **Description of your Practice** [Using the information captured from your question and answer activity, set out in some detail a picture of your practice as it presents today.]
6. **Practice-Based Risk Assessment** [Describe your view on identifying risks; measuring those risks; and managing the residual risks using your various compliance practices and controls set out in your Compliance Manual. Be sure to close off this section of the document with the measured risk rating for your practice.]
7. **Client-Relationship Risk Assessment** [Describe the links between your BR program and the client risk assessment process. Prepare and discuss your Client-Risk Assessment Overview table. Discuss your client risk rating questionnaire and include a copy of the current questionnaire in an Appendix off the RAP for easy reference.]
8. **Client BR Management** [Discuss your protocol for managing client Business Relationships including your on-going monitoring activities, schedules and record keeping. Be sure to discuss when a BR ends so that any reviewer can get a clear understanding that you know when and why a BR file is closed.]
9. **Appendices** [Feel free to insert as many Appendices as you deem necessary to include examples and references to such things as questionnaires, risk mitigation protocols, etc.]
10. **Updating Record Table** [Remember the RAP is a dynamic document and changes based on many influences resulting in your having to update the content. Consequently, you will need to include on the last page of your RAP, or some other location that catches the reader's eye, a Table such as the one below.]

RECORD OF UPDATES

Date of Update	Changes Made and Location in RAP	Initials

Well there you have it! A Guide to developing your practice-specific document. Remember the RAP must represent your practice and simply cutting and pasting the different Tables found in this Guide may not be totally representative of your situation. You may even have to justify why you included certain factors as part of a review by your AML auditor or possibly even by an examiner. Consequently, ensure that all content is representative of your notary practice world. Be sure when you list the various things you use to mitigate your risks that those controls are in fact in place. A reviewer could ask to see how they work as part of your risk management program. And finally, although nothing is ever final with a RAP, ensure that you schedule annually to crack open the RAP to confirm everything you have said continues as you described it; and if changes have occurred then make those changes now, and not put off until later, and add what you have done to your *Record of Updates* Table.

Well that is it. Good luck with your efforts!!

Appendix 7

Public Consultations on Strengthening Corporate Beneficial
Ownership Transparency in Canada: What We Heard – April 6,
2021

[Canada.ca](#) > [Innovation, Science and Economic Development Canada](#) > [Public consultations](#)
> [Strengthening Corporate Beneficial Ownership Transparency in Canada](#)

Public consultations on strengthening corporate beneficial ownership transparency in Canada: What we heard

April 6, 2021

1) Executive summary

From February to May 2020, the Government of Canada undertook public consultations on the creation of one or more publicly accessible registries that identify the beneficial owners of Canadian corporations. Beneficial ownership refers to the natural persons who, through direct or indirect means, exercise ultimate ownership or control over a corporation, such as through an ownership interest or control over decision-making. This is distinct from legal ownership, which could involve other legal persons such as trusts or other corporations. Beneficial owners also refer to the natural persons behind nominee shareholders, who serve as a registered owner of shares in a corporation or assume a management position on behalf of a beneficial owner. The availability of timely and accurate data on the ultimate beneficial owners of companies is crucial for allowing law enforcement, tax and other competent authorities to identify the natural persons who may be implicated in suspicious activities.

This consultation examined the merits of beneficial ownership registries, features that would make them more effective, potential limitations on information disclosed, and other factors to be considered. Over the course of these consultations, the Government heard a clear message from a broad range of stakeholders — including law enforcement and tax agencies, industry associations, privacy commissioners, individual Canadians and civil society — that more must be done to reduce the risk of corporations being misused for illicit activities, such as money laundering and tax evasion.

To this end, nearly all parties agreed that there is a legitimate public policy rationale for housing beneficial ownership data within a central government repository. The registry (or registries, if undertaken at the provincial and territorial level) should contain accurate, verified and up-to-date data and use the latest in digital technologies. Measures should be taken to ensure the accuracy of beneficial ownership data and ease of use for individuals uploading their information to the registry, as well as those authorized to access it. Stakeholders called on the federal government to take a lead role in ensuring a seamless and standardized system interoperable with existing federal and provincial registries to reduce the need for multiple filings and facilitate compliance. Sanctions for not providing timely or accurate data to registries should be proportionate and flexible. Reasonable access fees for registry users could be considered to offset operating costs.

Public accessibility to the registry (or registries) was of significant interest to most stakeholders, who expressed divergent views. Many stakeholders advocated for full public access while others flagged significant privacy and security issues. Notwithstanding some support for public registries, public access was not considered by the majority of stakeholders as essential to achieving the policy objectives of combatting the misuse of corporations, considering the accompanying privacy and security risks. Furthermore, some parties expressed caution about the impact that public registries could have on investment,

particularly given Canada's proximity to the United States. At the time of the consultation, the United States was considering a registry only accessible to authorized government authorities, an approach that has now been adopted.

A strong majority of stakeholders agreed with the concept of tiered access, in which law enforcement, tax and other authorities could have unrestricted access to beneficial ownership information, with other classes of users (e.g., private sector companies with anti-money laundering obligations) restricted to a more limited dataset, based on need to know. A phased approach was also suggested, starting with granting access to competent authorities, and gradually expanding access to other parties only once a functional, verified registry (or registries) could be put in place.

2) Background

Although the vast majority of corporations contribute positively to society, certain features of companies can make them vulnerable to misuse for criminal activities, such as money laundering and tax evasion. When wrongdoers take advantage of the ability to create complex ownership structures and make use of nominee shareholders and directors, the identities of the natural persons or "beneficial owners" who own and control corporations can remain hidden from those who may need to know, such as law enforcement and tax authorities. The inability for competent authorities to obtain accurate and timely information on the ultimate beneficial owners of companies (whether from financial institutions, corporate registries, or from a corporation's own shareholder records) challenges their efforts to follow the money in financial investigations.

In Canada, responsibility for corporate law is shared between federal, provincial and territorial governments. Corporations Canada and its provincial and territorial counterparts maintain registries of all companies incorporated under the laws of their respective jurisdictions. Some of these registries are freely accessible by the

public, while others charge fees or subscriptions to access all or part of the data. Although maintaining basic information on the corporations (e.g., company name, registered address, names and addresses of directors), they do not explicitly require companies to identify their beneficial owners. Corporate registries do not generally investigate or verify the information provided by corporations.

In addition, financial entities operating in Canada (including banks, credit unions, insurance companies and money service businesses, referred to as "reporting entities") are required under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations*, where a client is acting on behalf of a corporation, to identify its beneficial owners. In fulfilling these obligations, reporting entities have noted the lack of a reliable, third-party source to corroborate beneficial ownership information provided by their clients and have consistently called for additional tools to help them fulfill their due diligence requirements.

Since 2016, the Government of Canada has been working with its provincial and territorial counterparts to increase the availability of beneficial ownership information for law enforcement and tax authorities. The December 2017 Agreement to Strengthen Beneficial Ownership Transparency reached by finance ministers committed jurisdictions to require corporations to keep records of their beneficial owners and address misuse of bearer shares. ¹ Through this agreement, ministers also agreed to continue existing work assessing potential mechanisms to enhance timely access by competent authorities to beneficial ownership information, such as through central registries.

Building on the 2017 commitment, federal, provincial and territorial ministers at the June 2019 special meeting of ministers responsible for anti-money laundering and beneficial ownership agreed to cooperate on initiating consultations to increase beneficial ownership transparency, in order to combat the misuse of corporations for money laundering, tax evasion and other financial crimes. To

implement this commitment the Government of Canada, in February 2020, initiated public consultations on the creation of a publicly accessible registry (or registries) of beneficial ownership for corporations. The consultation period closed on May 30. ² This report summarizes the results of the federal government's consultations, which included the participation of provincial and territorial officials.

3) Who we heard from

Over the course of the consultations, Innovation, Science and Economic Development (ISED) and Finance Canada officials met in person or by phone with 29 organizations across Canada, in the public, private and non-profit sectors, and received 50 written submissions. A broad spectrum of stakeholders provided input, including law enforcement and tax agencies, industry associations, privacy commissioners, individual Canadians and a coalition of civil society organizations. We would like to thank all stakeholders for meeting with us to share their views and for providing thoughtful submissions.

4) Aligning with international best practices

In recent years there has been heightened international attention to the use of corporations to conceal illicit activities, including money laundering, tax evasion and other financial crimes. Given the cross-border nature of many financial flows, governments around the world have a responsibility to prevent legal entities from being misused for criminal purposes. Under the global anti-money laundering and anti-terrorist financing standards set by the Financial Action Task Force (FATF), centralized registries of the beneficial owners of corporations are one of the tools that countries can use to ensure competent authorities have adequate, accurate and timely access to beneficial ownership information to support investigations.

Although the FATF standards do not mandate central registries of beneficial ownership, public or otherwise, many countries have implemented or are considering these to improve corporate transparency. The United Kingdom adopted the world's first free, open, publicly accessible registry of beneficial ownership for privately held corporations in 2016. Countries in the European Union, for their part, are at varying stages of implementing the European Fifth Anti-Money Laundering Directive adopted in 2018 ³. This Directive requires European Union members to each implement a central registry of beneficial ownership information that is accessible to competent authorities as well as parties, such as reporting entities, that can demonstrate a "legitimate interest". The Directive also requires that certain basic ⁴ information on beneficial owners accessible to the public.

Mechanisms for recording beneficial ownership information, select countries

A number of stakeholders expressed concerns that the lack of beneficial ownership reporting requirements in Canada's corporate law regime makes privately held companies vulnerable to abuse. A growing number of Canadian jurisdictions are requiring companies to keep records of their beneficial owners, but the process of performing these checks can be costly, may not always permit timely access, risks tipping off entities to an ongoing investigation, and rules out large-scale data analysis on trends and typologies.

In order to align with ambitious measures taken by other countries and support efforts to counter corruption worldwide, certain stakeholders called on Canada to adopt a publicly accessible registry along the lines of the United Kingdom. Others concurred with the merits of introducing a registry reporting requirement but expressed concerns about the ramifications of public access to this information and the effect it would have on enforcement and prevention outcomes.

Stakeholders have pointed to the evolving nature of beneficial ownership

transparency requirements as they are implemented in countries and jurisdictions worldwide. As countries implement measures to strengthen beneficial ownership transparency and align themselves with the FATF standards, there is a desire for Canadian governments to adopt international best practices and stay abreast of the challenges and lessons learned from embracing an increasingly transparent beneficial ownership regime. This includes understanding what measures are effective in encouraging compliance and detecting non-compliance, mechanisms to verify the accuracy of information reported to the registry, the degree to which beneficial ownership data should be made public and ensuring information remains current.

As noted in a recent FATF study ⁵, an ongoing reporting requirement for companies, the use of different verification means to ensure data accuracy, access by competent authorities as well as proportionate and dissuasive sanctions. are keys to an effective registry, which can supplement other means for obtaining beneficial ownership information.

Finally, several stakeholders recommended that the federal government engage in further consultations with authorities from other countries with and without public registries to better understand the efficacy and impact of beneficial ownership registries and lessons learned. Many of these stakeholders acknowledged the evolving nature of best practices influencing beneficial ownership transparency and the spectrum of options for implementation. In this context, it is important that Canada takes an evidence-based approach.

5) Implementing a central and seamless regime

Centralized access

Stakeholders agreed that Canada should do more to deter and detect the misuse of Canadian corporations, aligning itself with emerging international best practices related to beneficial ownership transparency, while minimizing the risk

of disparities arising as provinces put in place measures to collect beneficial ownership information. To this end, nearly all parties agreed that there was a legitimate public policy rationale for creating a central registry (or registries) to house beneficial ownership data. With respect to the current federal obligations on companies to obtain and record the identities of their beneficial owners, stakeholders cited the time and resource intensive nature of the tracing process. Stakeholders agreed that immediate data access for law enforcement, tax and other competent authorities could shorten the time required, giving investigators a clearer starting point to trace ownership without potentially tipping off the entity. Centralization could also permit large-scale data analysis for understanding trends and typologies on how corporations are being used.

Harmonization of requirements and interoperability

Several stakeholders emphasized that requirements on corporations to identify and report their beneficial owners to central registries should be harmonized across jurisdictions to the extent possible, with the enabling statutes consistent in their definitions and applications. Some parties pointed to discrepancies with the definitions of beneficial ownership within the various governing statutes and the threshold above which owners must report their holdings, such as the *Canada Business Corporations Act* (PCMLTFA) and equivalent provincial legislation, as well as the *Income Tax Act*. Some parties recommended mirroring the approach taken in Canadian securities laws, where provinces agree to adopt similar legislation but make carve-outs via regulations as needed. It was suggested that failure to ensure consistent requirements going forward could compound interoperability issues within Canada's beneficial ownership regime. Some stakeholders called for the 25% beneficial ownership threshold (used in Canadian legislation and other FATF member jurisdictions) to be lowered to 10%.

Similar views were expressed in relation to ensuring cross-jurisdictional

standardization of data requirements, file formats, technical interfaces and interoperability between federal and provincial registries. For maximum usability, stakeholders noted that such a registry should be searchable across a variety of relevant fields, including director, beneficial owner and company number.

Comprehensive coverage of other legal persons and arrangements

Stakeholders observed that requirements on corporations to report their beneficial ownership information to central registries ought to encompass trusts and partnerships, which fall under provincial jurisdiction. Recognizing that criminals can and will migrate to the least transparent vehicles, such a move would ensure consistent treatment and avoid creating further incongruence in the market.

Federal leadership

Stakeholders called on the federal government to take a lead role in ensuring a seamless and standardized model interoperable with existing federal and provincial registries to avoid multiple filings and creating a seamless interface and experience. Concerns regarding the potential lack of sufficient harmonization and corresponding impacts to the ease of doing business and investment led many stakeholders to advocate for a federally-coordinated beneficial ownership registry, which would either compile data across provincial and territorial registries, or provide a central portal for accessing provincial and territorial data concurrently.

6) Removing anonymity while protecting privacy

Public accessibility to a beneficial ownership registry was a subject of significant interest to most stakeholders. Although some stakeholders supported a public registry, others asserted that public access was not essential to achieving the policy objectives of combatting the misuse of corporations, and warned of the accompanying privacy and security risks. While stakeholders generally agreed

that the beneficial owners should not be able to remain anonymous from law enforcement and tax authorities, comparatively fewer believed that the full names or personal details of beneficial owners should be made public. In fact, nearly all acknowledged that there are valid risks to privacy and security harms arising from disclosure of identifying information and that once the information enters the public sphere, it would be difficult to retract or control its use for unintended purposes.

Stakeholders acknowledged that some jurisdictions already disclose the names and addresses of officers and directors, and that this level of disclosure should extend to beneficial owners. In their view, not all information about an individual should be considered personal information and the context in which the information appears is important in determining whether its disclosure infringes on reasonable expectations of privacy. These stakeholders argued that the benefits of disclosure of partial information could outweigh the risks, provided that privacy protections are explicitly spelled out in the enabling legislation underpinning the beneficial ownership regime.

Public access — safety and privacy

Certain groups of stakeholders cited safety concerns that could affect their members or their members' families if beneficial ownership data were publicly accessible, including extortion and kidnappings. Depending on the categories of personal information posted publicly, beneficial owners could be at high risk of fraud and identity theft, with small businesses being disproportionately vulnerable. Business stakeholders cautioned against indiscriminate public access, as it could allow ownership data to be scraped by third parties or otherwise misused for unintended commercial purposes. Public access could also lead to data being misinterpreted by observers to make unsubstantiated allegations about an individual's finances or business associates, harming their ability to make business dealings or access financial services in the future. While

many parties acknowledged the role of an exemption regime in alleviating safety concerns, where individuals could apply to have certain details withheld from public access, others were unconvinced of the efficacy or immutable nature of such a regime.

Concerns were similarly raised in relation to ensuring the privacy of beneficial ownership data for legitimate business reasons such as succession planning, competitive positioning and not tipping off competitors to mergers and acquisitions. Maintaining the security of data holdings on a public registry against unauthorized use was a significant concern, as a public-facing registry could be at higher risk of a data breach. These stakeholders believed that having a registry in itself would contribute to Canada's business confidence and confidence by foreign investors, though public access would not be necessary for these benefits to be enjoyed.

Phased-in approach

The majority of stakeholders agreed that access to the central registry (or registries) should be tiered, with law enforcement, tax and other competent authorities having access to the full spectrum of beneficial ownership information. Other classes of users, such as private sector "reporting entities", could receive access to a more limited dataset, accessible on a need to know basis or using a zero-knowledge proof method of access. To this end, several stakeholders recommended that the federal government proceed with caution on implementing a public registry in the short term, instead recommending a stepped or phased approach. In this way, access would be initially restricted to law enforcement, tax and other competent authorities, and gradually expanded to other entities and eventually the public only following careful planning, consultation, evaluation and implementation at each stage.

Supporters of a staged approach believed that it would afford government policymakers greater opportunity to consider a framework and governance

structure for an exemption regime inclusive of the types of exemptions that would be granted, the duration of such exemptions and the process for managing risks to personal security and security of data holdings. It would also afford time for developing and refining the core technology elements for ensuring that any registry solution is functional, verifiable and easy to use. Other stakeholders suggested that more targeted consultations related to the data elements to be held in the registry and those eligible to access them.

Exemption regime

Stakeholders generally agreed that if a public registry were established, beneficial owners who believe themselves or their families to be at personal risk should have the right to seek an exemption from disclosure of their personal information in the public registry. Stakeholders held a variety of views as to the stringency and rigour of an exemption regime, and whether exemptions from disclosure should be permanent versus time-limited. Some parties expressed caution about potential gaming of the exemption regime and the need for strict controls to confirm the threats claimed by the requesting parties. Stakeholders generally acknowledged that careful time and consideration would need to be given to establish an exemption regime and that such regime would not shield beneficial ownership information from review by law enforcement, tax and other competent authorities.

7) Ensuring Credible Registry Data

Stakeholders concurred that holding accurate, verified information was key to a credible and reliable registry, and for many this meant that government(s) responsible for the registries would need to take the lead in ensuring data integrity. With respect to ensuring accuracy of the data held in the registry, stakeholders held a range of views on potential verification methods, each with varying degrees of costs and complexity.

As an initial review mechanism, many parties suggested that governments could conduct basic due diligence on filings received, using technological solutions to identify problematic or suspicious filings that the registry can follow up for clarification. As examples of indicators that could be used to flag filings thought to be at risk of misuse, corporations with foreign or non-resident beneficial owners could be deemed higher risk and subject to greater scrutiny.

Respecting who should verify the beneficial ownership data, some stakeholders believed that the identities of beneficial owners could be validated through professional attestation (e.g., by a notary, accountant or lawyer). Others cautioned about the added costs and complexity of an attestation requirement for law-abiding businesses seeking to incorporate quickly and at a low cost, and the liabilities it would impose on attesters.

Several stakeholders saw the potential for cross-referencing data held by the registry or registries against that held by other government agencies (e.g., tax authorities), as well as allowing third parties to flag deficiencies in a certain corporation's information. In this regard, it was suggested that there could be a requirement for reporting entities to report any discrepancies between their client records and a client's registry filings, for follow-up by the registry. Many opposed this view, suggesting that the detection and investigation of inconsistencies should be left to the registrar.

Some stakeholders believed existing forms of government-issued identification such as drivers' licenses and passports were sufficient while others believed signed attestations from beneficial owners should suffice provided there were penalties for those that provide false information. Some stakeholders pointed to the verification methods set out in the PCMLTFA as guidance for acceptable methods. ⁶ As well, many considered that unique identifiers, linked to an individual's name, the month and year of birth, citizenship, country of principal residence, and address of correspondence could be used to identify a beneficial

owner with interests in multiple companies. Stakeholders expressed mixed views about the potential use of biometrics given the heightened privacy sensitivities around their use.

Some stakeholders believed that giving the public access to the registry would contribute to the verification and strengthen the quality of data in the registry. These parties were of the view that public scrutiny would lead to identification of information gaps, the identification of false or incomplete information, and detection of crime and corruption.

8) Minimizing the Cost and Compliance Burden to Corporations

Canada has a global reputation as a country that facilitates the ease of doing business. This includes making it easy for Canadians to start a business by ensuring that companies can be incorporated speedily and at a low cost. Many stakeholders expressed concerns that new reporting obligations could significantly add to the costs of running their business and compliance burden associated with new legislative and regulatory reporting obligations.

Updating and reporting obligations

To reduce the cost and compliance burden several stakeholders recommended adding beneficial ownership reporting obligations to companies' existing requirements to provide annual filings to the corporate registries. Others suggested using data collected through tax filings to populate the registry automatically as a straightforward and reliable means for ongoing data collection. Furthermore, there was general agreement that event-driven updates should be required following material changes to a company's individuals with significant control, complementing the baseline annual reporting. Many companies are only active for one year, after which they are dissolved. Event-driven updates could reduce the ability for illicit actors to circumvent the annual reporting obligation. Stakeholders suggested a range of timelines for making the necessary updates

(e.g., 14-30 days), with potential for alignment with the existing obligations in the *Canada Business Corporations Act* and equivalent provincial legislation. 7

Leveraging guidance and facilitating compliance

Many stakeholders argued that any new registry reporting requirement should be accompanied by an awareness campaign to make sure that corporations clearly comprehend their filing obligations, interpret their obligations consistently, and understand why compliance is important. Any filing system should be online and easy to use, minimizing paper-based processes to reduce administrative costs. Fillable forms, drop-down menus and similar features may be used to reduce the potential for errors in the data. Quarterly email updates could be used to prompt filers to report if there are changes to a company's beneficial owners, to encourage compliance.

Access costs

Stakeholders who advocated for a public registry generally also supported free access, arguing that a paywall would undermine the benefits of increasing corporate transparency. Others, however, saw user fees as a way to deter frivolous searches, and "data mining" by those who might seek to profit from or misuse the personal data of beneficial owners. Several parties, including those with anti-money laundering obligations, supported options for a subscription service or user fee model, depending on how often they would need to consult a registry. Alternatively, others suggested that the costs of operating the registry could be included in incorporation fees.

9) Enforcement Measures

Stakeholders generally agreed that penalties for corporations that neglect to report accurate and timely information to the registry should be proportionate and flexible, taking into account the degree and nature of non-compliance. Many stakeholders agreed that penalties ought to ensure that companies report timely

and truthful data, while not excessively penalizing deficiencies best addressed through education and guidance. Most stakeholders supported the use of a range of graduated measures including automated reminders, scaling up to administrative monetary penalties (AMPs), deregistration, and criminal liability for more serious violations.

Outreach, warnings and penalties

Stakeholders agreed that sanctions associated with the beneficial ownership regime should be flexible with a range of administrative and criminal penalties reflecting the nature and severity of non-compliance. Minor violations, such as late filings, could be addressed through education and reminders emphasizing why compliance is important, given the impacts of financial crime on communities and businesses. AMPs could be reserved for more serious violations (e.g., knowingly providing false information, repeated non-compliance), potentially scaling in severity for companies that do not promptly address outstanding deficiencies.

Directors' liability

Some stakeholders suggested that company directors and officers should be held responsible for a corporation's non-compliance with beneficial ownership reporting obligations, treated similar to a breach of fiduciary duty. Conversely, many of the same stakeholders recognized that enforcing these requirements against non-resident directors could be a challenge.

Deregistration

Deregistration of a non-compliant corporation was suggested as one of the most powerful tools available to a corporate registry. As this step could have serious practical consequences for companies, the threat of deregistration could be effective at encouraging compliance in certain circumstances.

Criminal liability

In the framework of a proportionate scheme, criminal penalties up to and including imprisonment was also raised as an appropriate response to cases of serious and deliberate non-compliance. Such provisions, some felt, were necessary to further deter the misuse of corporations, while potentially giving law enforcement leverage against companies under investigation.

10) Leveraging new technologies

A majority of stakeholders recommended that Canada capitalize on the emergence of advanced technologies and incorporate these into the design and implementation of Canada's beneficial ownership registry(ies). Many believe that the use of advanced technologies will reduce the burden on corporations, provide a seamless inquiry interface and enhance verification and security. A variety of proposals were made along the spectrum from using drop down menus and application programming interfaces (APIs) to ease registration use and access to using encryption-based services and blockchain to enhance security and using digital IDs, advanced analytics and artificial intelligence to support verification and data integrity.

Unique ID

Numerous stakeholders noted that the use of unique digital identifier could help identify beneficial owners and to provide insight into the number of corporations in which an individual beneficial owner have ownership interests. These stakeholders argued that a government issued digital ID provided the most efficient and secure method to confirm identities that could enable cross-referencing of beneficial owners of multiple corporations and businesses. Stakeholders pointed to digital ID solutions currently being studied or implemented in various federal government bodies and in some provinces. Some stakeholders suggested the federal government adopt recommendations put

forward by the Digital ID and Authentication Council of Canada in order to eliminate any coverage issues that could arise when selecting a particular solution.

Drop down menus, AI, analytics

Several stakeholders pointed to technologies currently deployed in various countries as examples of applications facilitating ease of use to those who interface with a registry. Other stakeholders pointed to the best practices documented by the FATF and the role that technology can play to facilitate the identification checking, validation and tracing of beneficial owners.

In sum, there is general agreement that the optimal use of technology will be important in the successful functioning, overall security and cost of compliance for transmitting information to a registry or registries. Leveraging existing and emerging technologies will be essential to establish a cutting-edge registry with credible and reliable beneficial ownership information and to keep compliance burden to a minimum for all parties.

11) Conclusion

Over the course of the consultations, the Government of Canada heard a clear message from stakeholders that action is needed to address the risk of corporations being misused for illicit activities. To this end, stakeholders across the spectrum supported the idea of a central registry (or registries) of beneficial ownership information as an effective tool in making sure that law enforcement, tax and other authorities obtain the information they need to identify the natural persons who own and control Canadian corporations. While there were more mixed views on the value and merits of public access, stakeholders broadly emphasized measures to encourage compliance, ensure data quality and seek regulatory alignment as crucial to an effective system.

As this consultation ends, strengthening corporate beneficial ownership

transparency remains a priority of the Government of Canada. Work should continue on advancing a coordinated approach to strengthening beneficial ownership, while respecting jurisdictional responsibilities with respect to corporations. Building on this feedback, the Government will continue to explore options for central registry (or registries) of beneficial ownership, in cooperation with provincial and territorial partners.

Footnotes

- 1 Department of Finance Canada, 2017. Agreement to Strengthen Beneficial Ownership Transparency.
<https://www.canada.ca/en/department-finance/programs/agreements/strengthen-beneficial-ownership-transparency.html>
- 2 Due to measures undertaken to combat the spread of the COVID-19 virus, the deadline for any written submissions was extended and late submissions were accepted.
- 3 Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018L0843&cookies=disabled>
- 4 The name, the month and year of birth and the country of residence and nationality of the beneficial owner as well as the nature and extent of the beneficial interest held.
- 5 Financial Action Task Force, 2019. Best Practices on Beneficial Ownership for Legal Persons.<https://www.fatf-gafi.org/media/fatf/documents/Best-Practices-Beneficial-Ownership-Legal-Persons.pdf>

6 Reasonable measures taken to confirm the accuracy of information obtained can include referring to official documents or records, such as shareholder registers, articles of incorporation and minute books. It is also acceptable to have the client sign a document to confirm the veracity of the information obtained.

7 Per the requirement to register with FINTRAC under s. 11.13 of the PCMLTFA, money service businesses must update their information on file with FINTRAC within 30 days of becoming aware of the change.

Date modified: 2021-04-06

☐ [Share this page](#)

[Contact us](#)

[Departments and agencies](#)

[Public service and military](#)

[News](#)

[Treaties, laws and regulations](#)

[Government-wide reporting](#)

[Prime Minister](#)

[How government works](#)

[Open government](#)

• [Social media](#)

• [Mobile applications](#)

• [About Canada.ca](#)

• [Terms and conditions](#)

• [Privacy](#)

[Top of Page](#)



Appendix 8

Future of Financial Intelligence Sharing (FFIS): Canada in
Context – Canadian Legislation, Supervision and Operational
Processes for Information-Sharing to Detect Money Laundering
and Underlying Crime, set in the Context of International
Practices – February 19, 2021

Future of Financial Intelligence Sharing (FFIS)

FFIS ‘The story in statistics’ appendix to main briefing paper –

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

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

Author. Nick J Maxwell, Head of the FFIS Programme
Submission on: 19 February 2021

This appendix sets out the key statistics highlights, and additional geographical comparisons based on select statistics, derived from the original FFIS Briefing Paper submitted on 4 January to the Commission of Inquiry into Money Laundering in British Columbia.

1. The threat:

In the Financial Action Task Force (FATF) methodology for evaluating the effectiveness of Anti-Money Laundering/Anti-Terror Financing (AML/ATF) systems, the first ‘immediate outcome’ of an AML/ATF system should be that “Money laundering and terrorist financing risks are understood and, where appropriate, actions coordinated domestically to combat money laundering and the financing of terrorism and proliferation.”ⁱ

However, in Canada there is limited publicly available information to understand the national-level scale of money laundering. What estimates do exist include the following:

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

(Below we use the mid-point of the RCMP 2011 estimate and assume that the annual amount laundered in Canada is at least US\$10bn (not taking account of inflation) as a conservative estimate).

2. The public sector response:

The Department of Finance Canada Results Report on the ‘horizontal initiative’ of “Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime” is a wide ranging and annual exercise to bring together performance information of the Canadian AML/ATF regime. This report provides a cross-government^v review of AML/ATF spending across 16 government programs, and details the expected results against each program, performance indicators, targets and actual results achieved.

The Departmental Results Report (DRR) 2018–19: Supplementary Information Table^{vi}

Federal organisations	Program	Ongoing funding (CAD)
Department of Finance Canada	Financial Sector Policy (1.1)	\$ 244,000.00
Department of Justice Canada	Justice Policies, Laws and Programs (2.1)	\$ 100,000.00
Public Prosecution Service of Canada	Drug, National Security and Northern Prosecutions Program (3.1)	\$ 2,108,210.00
Financial Transactions and Reports Analysis Centre of Canada	Financial Intelligence Program (4.1)	\$ 12,075,001.00
	Compliance Program (4.2)	\$ 15,671,379.00
	Strategic Policy and Review Program (4.3)	\$ 379,071.00
	Strategic Intelligence and Research Program (4.4)	\$ 1,292,218.00
	Internal Services	\$ 16,400,085.00
Royal Canadian Mounted Police	Federal Policing (5.1)	\$ 9,948,419.00
	Internal Services	\$ 1,340,454.00
Canada Revenue Agency	Domestic Compliance (6.1)	\$ 2,035,600.00
	Charities (6.2)	\$ 4,103,445.00
Canada Border Services Agency	Intelligence Collection and Analysis Targeting (7.1)	\$ 1,700,000.00
	Traveller Facilitation and Compliance Commercial-Trade Facilitation and Compliance (7.2)	\$ 1,100,000.00
	Recourse (7.3)	\$ 300,000.00
	Internal Services	\$ 600,000.00
All Partners	Total	\$ 69,397,882.00

Additional budget funding in 2019

In the 2019 budget^{vii}, the following commitments were made by the government of Canada:

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

3. The private sector response

In Canada, 30,000+^{viii} private sector reporting entities are required to respond to the threat of money laundering and terrorist financing, resulting in over 30 million transactions reported to FINTRAC per year in total.^{ix}

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

4. Understanding the numbers^{xi}

Comparing the volumes of money with a scale of kilometres distance, we can understand the numbers as follows:

	Amount per year	% of the mid-point 2011 RCMP estimate range of total money laundering in Canada per year	Scale in relation to annual money laundering estimate, understood in distance (direct line of travel)
The mid-point 2011 RCMP estimate range of total money laundering in Canada per year	CAD\$13.3bn ^{xii}	100%	The distance from Canada Place exhibition centre in Vancouver to the Parliament of Canada in Ottawa (3,538km)
Total public sector resources (on enforcement or prosecution programs identified in the AML/ATF DRR)	CAD\$17m	0.13%	The distance from Canada Place exhibition centre in Vancouver to Dickens, Vancouver (4.5 km)
Total public sector resources accounted for in all AML/ATF programs in the DRR 2018/19	CAD\$69.4m	0.52%	The distance from Canada Place exhibition centre in Vancouver to Patullo Bridge (18.5km)
Total public sector resources accounted for in all AML/ATF programs in the DRR 2018/19 in addition to peak annualized extra resources identified in the 2019 Budget for AML/ATF.	CAD\$130m	0.98%	The distance from Canada Place exhibition centre in Vancouver to Clayton (34.6km)
Private sector AML/ATF compliance spending (2019 Lexis Nexis estimate)	CAD\$6.8bn	51%	Just short of the distance from Canada Place exhibition centre in Vancouver to just short of Winnipeg (1804km)

5. Growth of reporting

Suspicious Transaction Reports (STRs) to FINTRAC are growing exponentially, increasing 64% from the 2019-20 Annual Report from the previous year and with an average annual growth rate of 37% per year over the previous three years.

The volume of case disclosures to enforcement agencies by FINTRAC is consistently less than 1% of the volume of STR reports received, with the 2019-20 Annual Report indicating that disclosures are at approximately 0.5% of STR inputs.

Total volumes of comparable transaction/activity suspicious reporting		
Canada (2019-20) ^{xiii}	STR	386,102
	Large Cash Transaction Reports	9,738,058
	Electronic Funds Transfer Reports	21,031,401
	Total	31,155,561
U.S. (2019 calendar year) ^{xiv}	SAR	5,596,620
	Currency Transaction Reports	16,087,182
	Total	21,683,802
UK (2019-20) ^{xv}	SAR	573,085
	Total	573,085

In terms of international comparisons...

- over 10million more transactions are filed to the FIU every year in Canada, compared to the U.S.
- over 30million more reports are filed to the FIU every year in Canada, compared to the UK.
- Per head of population, 12.5 times more reports are filed every year in Canada, compared to the U.S.
- Per head of population, 96 times more reports are filed every year in Canada, compared to the UK

ENDNOTES

ⁱ FATF (2020) 'Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT systems', Original February 2013, Updated November 2020.

ⁱⁱ FATF (2016), Anti-money laundering and counter-terrorist financing measures - Canada, Fourth Round Mutual Evaluation Report, FATF, Paris, p13

ⁱⁱⁱ Ibid

^{iv} Government of Canada (2015) Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada, Ch 3

^v Department of Justice Canada; Public Prosecution Service of Canada; Financial Transactions and Reports Analysis Centre of Canada; Royal Canadian Mounted Police; Canada Revenue Agency; Canada Border Services Agency.

^{vi} Government of Canada (2020) Departmental Results Report 2018–19: Supplementary Information Tables - <https://www.canada.ca/en/department-finance/corporate/transparency/plans-performance/departamental-results-report/2019/supplementary-information-tables.html>

^{vii} Government of Canada (2019) Chapter 4: Delivering Real Change: Strengthening Canada's Anti-Money Laundering and Anti-Terrorist Financing (AML/ATF) Regime <https://www.budget.gc.ca/2019/docs/plan/chap-04-en.html>

^{viii} A comprehensive number of reporting entities in the Canadian AML/ATF system is not clear to the author from publicly available material. Multiple FINTRAC references from 2016 to 2019 refer to the number of regulated entities as 31,000.

^{ix} FINTRAC (2020) 'Safe Canadians, Secure Economy' 2019–20 Annual Report

^x LEXIS NEXIS Risk Solutions (2019) 'True Cost Of AML Compliance' Study

^{xi} Author's summary from source documents referenced. Geographical distance determined through googlemaps.

^{xii} *Using 7 June 2019 rate, as per the other conversions in this table

^{xiii} FINTRAC (2020) 'Safe Canadians, Secure Economy' 2019–20 Annual Report

^{xiv} <https://www.fincen.gov/reports/sar-stats>

^{xv} UK National Crime Agency (2020) UK Financial Intelligence Unit Suspicious Activity Reports Annual Report 2020

Appendix 9

Compiled Money Laundering-Related Statistics for Cullen
Commission from FINTRAC

Compiled ML-related Statistics for Cullen Commission

Statistics

Compliance and Supervision

Table 1: FINTRAC Compliance Examinations, 2010-11 to 2019-20

Sector	Est. Number of REs (2016)	2010- 11	2011- 12	2012- 13	2013- 14	2014- 15	2015- 16	2016- 17	2017- 18	2018- 19	2019- 20
Real Estate	20,784	70	40	270	203	140	191	152	172	190	146
Financial Entities ¹	855 ²	209	447	306	183	178	142	129	66	45	48
Money Services Businesses	850	201	425	222	161	143	158	110	64	112	114
Life Insurance Companies, Brokers and Agents	89	52	5	13	123	59	60	57	53	11	1
British Columbia Notaries	336	-	-	16	1	6	35	73	53	24	10
Securities Dealers	3,829	120	136	129	167	85	102	69	47	57	58
Dealers in Precious Metals and Stones	642	-	10	166	276	2	43	62	43	49	16
Casinos	39	12	5	10	1	6	7	7	1	5	5
Agents of the Crown	-	-	1	-	-	-	-	-	1	-	-
Accountants	3,829	20	-	25	11	10	1	2	-	4	1
Total	Est. 30,398	684	1069	1157	1126	629	739	661	500	497	399

Table 2: Administrative Monetary Penalties for AML/CFT Breaches, as of November 16, 2015

Sector	# of Notice of Violation Issued	Publicly Named
Accountant	1	0
Casinos	4	0
Financial Entities	15	3
FRFI	1	0
Life Insurance	1	0
MSBs	38	25
Real Estate	11	4
Securities Dealers	7	4
Total	78	36

¹ I.e., banks, trusts and loans, credit unions and caisses populaires.

² This total includes 81 banks, 75 trusts and loans, 699 credit unions.

Table 3: FINTRAC Non-Compliance Disclosures to Law Enforcement, April 1, 2010 to March 31, 2020

2010-11	2011-12	2012-13	2013-14	2014-15	2015-16 ³	2016-17	2017-18	2018-19	2019-20	Total
1	4	0	2	0	-	1	5	7	7	27

Table 4: Outcomes on PCMLTFA Charges, 2009-10 to 2018-19

Outcome	2009-10	2010-11	2011-12	2012-13	2013-14	2014-15	2015-16	2016-17	2017-18	2018-19	Total	%
Convictions/ Guilty Pleas	2	20	24	12	12	10	3	2	1	-	86	66%
Acquittal	0	1	2	1	-	-	-	-	-	-	4	3%
Discharge	0	1	1	1	-	1	-	-	-	-	4	3%
Stay of Proceedings (Crown)	0	2	6	3	1	2	2	2	-	4	22	17%
Judicial Stay of Proceedings	0	0	2	-	-	-	-	-	-	-	2	2%
Withdrawal	0	2	2	1	-	3	2	-	-	2	12	9%
Other	0	0	-	1	-	-	-	-	-	-	1	1%
Total	2	26	37	19	13	16	7	4	1	6	131	100%

Financial Intelligence

Table 5: Reports submitted to FINTRAC by Reporting Entities, 2010-11 to 2019-20

Year	Suspicious Transaction Reports	% Increase from 2010-11	All Reports (EFTs, LCTRs, CDRs, STRs, CCRs)	% Increase from 2010-11
2010-11	58,722	-	19,265,355	-
2011-12	70,392	20%	18,528,922	-4%
2012-13	79,294	35%	19,744,923	2%
2013-14	81,375	39%	19,750,453	3%
2014-15	92,531	58%	21,088,735	9%
2015-16	114,422	95%	23,727,393	23%
2016-17	125,948	114%	24,753,663	28%
2017-18	179,172	205%	25,319,625	31%
2018-19	235,661	301%	28,119,852	46%
2019-20	386,102	558%	31,417,429	63%

Table 6: FINTRAC intelligence disclosures by recipient and total unique disclosures⁴

Recipient	2012-13	2013-14	2014-15	2015-16	2016-17	2017-18	2018-19	2019-20
RCMP	580	703	779	976	1,354	1,664	1,509	2,405
Municipal Police	182	207	331	582	806	1,198	795	914
CSIS	164	243	312	429	597	581	502	436
Provincial Police	144	135	214	303	-	557	455	703
Foreign FIUs	131	163	259	384	318	401	253	234
CBSA	96	139	169	225	-	353	324	500
CRA	149	153	173	205	-	281	252	287
Provincial Securities Regulators	-	-	-	69	-	92	74	66

³ Data not available for 2015-16.

⁴ Some disclosures are sent to multiple recipients.

CSE	32	33	23	47	-	66	20	12
Canadian Armed Forces	-	-	-	-	-	0	8	-
Total (Unique Disclosures)	919	1,143	1,260	1,655	2,015	2,466	2,276	2,057
% Increase from 2012-13	-	24%	37%	80%	119%	168%	148%	124%

Table 7: Number of police, law enforcement, national security and other partner agency major and project-level investigations supported by FINTRAC financial intelligence disclosures

Fiscal Year	Number of Investigations ⁵
2017-18	262
2018-19	296
2019-20	393

Table 8: Number of voluntary information records received by FINTRAC

Fiscal Year	2010-11	2011-12	2012-13	2013-14	2014-15	2015-16	2016-17	2017-18	2018-19	2019-20
# of Reports	1,186	1,034	1,082	1,320	1,380	1,619	1,958	2,397	2,754	2,519
% Increase from 2010-11		-13%	-9%	11%	16%	36%	65%	102%	132%	112%

Investigations and Prosecutions

Table 9: Police-reported incidents of money laundering - proceeds of crime (Part XII.2 CC), Canada, 2008 to 2018⁶

Statistics	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Actual incidents	452	520	405	379	291	263	276	248	237	328	218
Rate per 100,000 population	1.4	1.5	1.2	1.1	0.8	0.7	0.8	0.7	0.7	0.9	0.6
Percentage change in rate	-10.6	13.7	-23.0	-7.3	-24.0	-10.6	3.9	-10.8	-5.5	36.8	-34.5
Total cleared	119	117	129	150	103	117	90	82	76	58	31
Cleared by charge ⁷	51	53	46	82	72	86	58	63	50	40	21
Cleared otherwise ⁸	68	64	83	68	31	31	32	19	26	18	10
Total persons charged	62	55	54	60	59	81	66	80	69	52	22
Total adults charged	61	55	54	60	55	76	66	76	68	52	22
Total youth charged	1	0	0	0	4	5	0	4	1	0	0

Source: Statistics Canada, Canadian Centre for Justice Statistics, Uniform Crime Reporting Survey.

⁵ New indicator. Data for prior years prior to 2017-18 not available.

⁶ The offences which comprise the category of money laundering in the Uniform Crime Reporting Survey include: laundering proceeds of crime (CCC s.462.31) and restraint order violation (CCC s.462.33).

⁷ At least one accused has been identified and there is a criminal charge laid or recommended to be laid against this individual in connection with this criminal incident.

⁸ An accused has been identified by police in relation to the criminal incident, and there is sufficient evidence to lay a charge, however a charge is not laid by police and the accused is processed by other means. Examples of charges cleared otherwise include warnings, cautions, alternative measures, extrajudicial sanctions and instances where the accused has died.

Table 10: Completed court cases of money laundering, adult criminal courts, Canada, 2008-09 to 2016-17

Fiscal Year	2008-09	2009-10	2010-11	2011-12	2012-13	2013-14	2014-15	2015-16	2016-17
Completed cases where money laundering is the most serious offence	98	88	87	130	109	122	91	136	135
Completed cases where money laundering is one charge in the case	146	141	184	241	235	241	208	237	264

Source: Statistics Canada, Canadian Centre for Justice Statistics, Integrated Criminal Court Survey.

Table 11: Completed court cases where money laundering is the most serious offence, adult criminal courts, Canada, 2008-09 to 2016-17

Fiscal Year	2008-09	2009-10	2010-11	2011-12	2012-13	2013-14	2014-15	2015-16	2016-17
Number									
Guilty ⁹	26	30	16	31	30	41	33	37	27
Acquitted of offence charged ¹⁰	0	2	0	0	4	8	5	8	4
Stay of proceeding ¹¹	11	7	8	13	15	17	5	23	17
Withdrawn / Dismissed / Discharged ¹²	60	49	63	74	57	52	45	60	79
Other decision ¹³	1	0	0	12	3	4	3	8	8
Percent									
Guilty	26.5	34.1	18.4	23.8	27.5	33.6	36.3	27.2	20.0
Acquitted of offence charged	0.0	2.3	0.0	0.0	3.7	6.6	5.5	5.9	3.0
Stay of proceeding	11.2	8.0	9.2	10.0	13.8	13.9	5.5	16.9	12.6
Withdrawn / Dismissed / Discharged	61.2	55.7	72.4	56.9	52.3	42.6	49.5	44.1	58.5
Other decision	1.0	0.0	0.0	9.2	2.8	3.3	3.3	5.9	5.9

Source: Statistics Canada, Canadian Centre for Justice Statistics, Integrated Criminal Court Survey.

Table 12: Most serious sentence for guilty decisions in completed court cases where money laundering is the most serious offence, adult criminal courts, Canada, 2008-09 to 2016-17

	2008-09	2009-10	2010-11	2011-12	2012-13	2013-14	2014-15	2015-16	2016-17
Number									
Custody	17	20	8	15	18	19	16	21	12

⁹ Guilty findings include guilty of the charged offence, of an included offence, of an attempt of the charged offence, or an attempt of an included offence. This category also includes guilty pleas, and cases where an absolute or conditional discharge has been imposed.

¹⁰ Acquittal means that the accused has been found not guilty of the charges presented before the court.

¹¹ Stay of proceeding refers to stays, as well as court referrals to alternative or extrajudicial measures and restorative justice programs. These decisions all refer to the court stopping criminal proceedings against the accused.

¹² Withdrawn/Dismissed/Discharged includes withdrawals, dismissals and discharges at preliminary inquiries. These decisions all refer to the court stopping criminal proceedings against the accused.

¹³ Other decisions includes unknown sentences. This category also includes other final decisions such as waived out of province or territory, not criminally responsible, any order where a conviction was not recorded, the court's acceptance of a special plea, cases which raise Charter arguments and cases where the accused was found unfit to stand trial, among others.

Conditional sentence	4	2	3	6	5	9	4	4	7
Probation	2	3	4	6	2	10	6	7	6
Fine	1	1	1	0	2	0	3	1	0
Other sentence ¹⁴	2	4	0	4	3	3	4	4	2
Percent									
Custody	65.4	66.7	50.0	48.4	60.0	46.3	48.5	56.8	44.4
Conditional sentence	15.4	6.7	18.8	19.4	16.7	22.0	12.1	10.8	25.9
Probation	7.7	10.0	25.0	19.4	6.7	24.4	18.2	18.9	22.2
Fine	3.8	3.3	6.3	0.0	6.7	0.0	9.1	2.7	0.0
Other sentence ⁶	7.7	13.3	0.0	12.9	10.0	7.3	12.1	10.8	7.4

Source: Statistics Canada, Canadian Centre for Justice Statistics, Integrated Criminal Court Survey.

Seizures and Forfeitures

Table 13: Federally Seized, Restrained and Forfeited Assets by Appraisal Value, \$CAD, PSPC-SPMD¹⁵

Fiscal Year	Seized and Restrained Assets	Forfeited Assets
2009-10	80,533,349	46,368,328
2010-11	83,430,829	58,872,881
2011-12	72,896,801	77,698,567
2012-13	60,247,601	83,935,231
2013-14	76,466,149	75,997,602
2014-15	44,384,617	72,869,240
2015-16 ¹⁶	-	-
2016-17	30,009,589	28,366,594
2017-18	44,901,166	21,858,119
2018-19	44,990,516	25,036,816
Total	\$537,860,617	\$491,003,378

Source: Seized Property Management Directorate.

Mutual Legal Assistance

Table 14: MLA – Proceeds of Crime/Money Laundering – Incoming and outgoing requests received

Year	# of Incoming Requests	# of Outgoing Requests
MLA	720	190
Extradition	132	16

Table 15: MLA – Proceeds of Crime/Money Laundering – Outcomes of requests closed

	Year	# of Requests Executed	# of Requests Refused	# of Requests Abandoned	# of Requests Withdrawn
MLA	Incoming	455	9	59	34
	Outgoing	114	2	11	13
Extradition	Incoming	81	11	22	12

¹⁴ Other sentences include absolute and conditional discharge, suspended sentence, community service order and prohibition, among others.

¹⁵ The status of assets may change within the same period. SPMD prorates asset values by the number of acts and sections implicated in each case.

¹⁶ Data not available for 2015-16.

	Outgoing	1	1	2	2
--	-----------------	----------	----------	----------	----------

Table 16: Information exchanges with foreign financial intelligence units (FFIUs)

Type of Information Exchange	2011-12	2012-13	2013-14	2014-15	2015-16	2016-17	2017-18	2018-19	Total
Queries received from FFIUs	329	202	241	222	240	217	255	225	1,931
Queries sent to FFIUs	74	105	116	140	147	146	211	149	1088
Disclosures to FFIUs	146	131	163	178	384	318	401	253	1,974

Table 17: RCMP Assistance to Foreign Agency Files, by Reported Year

Fiscal Year	Money Laundering	Terrorist Financing	Total
2018-19	-	-	188
2017-18	145	8	163
2016-17	167	8	185
2015-16 ¹⁷	-	-	-
2014-15	130	53	183
2013-14	118	51	169
2012-13	102	42	146
2011-12	101	75	176
2010-11	91	101	192
2009-10	70	75	145
Total	924	413	1,547

¹⁷ Data not available for 2015-16.

Appendix 10

Additional Statistics from FINTRAC on Money Laundering Crime
Data

Table 1
Police-reported crime for select non-violent offences, Canada, 2015 to 2018

Type of offence	2015		2016		2017		2018		Change in rate 2015 to 2018
	number	rate	number	rate	number	rate	number	rate	percent
Total Property Crime	1,153,700	3,231.4	1,169,445	3,238.6	1,193,319	3,265.8	1,237,324	3,338.8	3.3
Theft									
Theft over \$5,000	11,081	31.0	10,897	30.2	12,391	33.9	14,749	39.8	28.2
Theft over \$5,000 from a motor vehicle	3,867	10.8	4,057	11.2	4,325	11.8	4,664	12.6	16.2
Shoplifting over \$5,000	496	1.4	574	1.6	549	1.5	700	1.9	36.0
Motor Vehicle Theft	78,758	220.6	79,010	218.8	85,068	232.8	86,078	232.3	5.3
Theft \$5,000 or under	210,685	590.1	207,373	574.3	209,446	573.2	213,823	577.0	-2.2
Theft \$5,000 or under from a motor vehicle	176,584	494.6	186,655	516.9	187,426	512.9	192,556	519.6	5.1
Shoplifting \$5,000 or under	99,907	279.8	102,948	285.1	108,313	296.4	124,933	337.1	20.5
Possession/Trafficking Stolen Goods									
Traffic stolen goods over \$5000 (incl intent)	307	0.9	319	0.9	378	1.0	325	0.9	2.0
Possession of Stolen Goods over \$5 000	7,262	20.3	8,092	22.4	11,062	30.3	10,991	29.7	45.8
Traffic stolen goods under \$5000 (incl intent)	410	1.1	528	1.5	531	1.5	524	1.4	23.1
Possession of Stolen Goods \$5 000 or under	11,976	33.5	11,567	32.0	12,215	33.4	12,045	32.5	-3.1
Fraud									
Fraud	94,425	264.5	109,630	303.6	113,166	309.7	129,409	349.2	32.0
Identity Theft	2,541	7.1	3,136	8.7	3,295	9.0	3,745	10.1	42.0
Identity Fraud	11,894	33.3	14,033	38.9	14,344	39.3	15,839	42.7	28.3
Mischief									
Altering/Removing/Destroying Vehicle Identification Number (VIN)	105	0.3	118	0.3	85	0.2	99	0.3	-9.2
Gaming and Betting									
Betting house	1	0.0	2	0.0	0	0.0	2	0.0	92.7
Gaming house	53	0.1	37	0.1	20	0.1	67	0.2	21.8
Other violations related to gaming and betting	67	0.2	81	0.2	47	0.1	62	0.2	-10.8
Common Bawdy House (to keep, to transport a person to)	18	0.1	11	0.0	17	0.0	19	0.1	1.7
Offensive Weapons									
Weapons trafficking	106	0.3	83	0.2	103	0.3	107	0.3	-2.8
Unauthorized importing or exporting of weapons	81	0.2	39	0.1	59	0.2	67	0.2	-20.3
Other Criminal Code Violations									
Counterfeiting	675	1.9	805	2.2	939	2.6	1,095	3.0	56.3
Other offences against the administration of law and justice (Part IV CC)	7,552	21.2	7,615	21.1	7,601	20.8	7,615	20.5	-2.9
Offences against rights of property (Part IX CC)	1,565	4.4	1,661	4.6	1,576	4.3	1,844	5.0	13.5
Fraudulent transactions relating to contracts and trade (Part X CC)	241	0.7	210	0.6	188	0.5	167	0.5	-33.2
Wilful and forbidden acts in respect of certain property (Part XI CC)	2,036	5.7	1,944	5.4	2,095	5.7	1,929	5.2	-8.7
Offences relating to currency (Part XII CC)	53	0.1	35	0.1	92	0.3	93	0.3	69.1
Money laundering, proceeds of crime (Part XII.2 CC)	248	0.7	237	0.7	328	0.9	218	0.6	-15.3
Attempts, conspiracies, accessories (Part XIII CC)	237	0.7	243	0.7	250	0.7	215	0.6	-12.6
Other Federal Statute Violations									
Bankruptcy Act	32	0.1	21	0.1	13	0.0	44	0.1	32.5
Income Tax Act	16	0.0	10	0.0	8	0.0	9	0.0	-45.8
Canada Shipping Act	3,634	10.2	3,999	11.1	3,559	9.7	3,875	10.5	2.7
Customs Act	554	1.6	1,140	3.2	9,716	26.6	9,221	24.9	1503.5
Competition Act	1	0.0	1	0.0	4	0.0	12	0.0	1056.1
Excise Act	315	0.9	277	0.8	215	0.6	208	0.6	-36.4
Human Trafficking	91	0.3	102	0.3	103	0.3	112	0.3	18.6
Human Smuggling fewer than 10 persons	20	0.1	11	0.0	17	0.0	10	0.0	-51.8
Human Smuggling 10 persons or more	3	0.0	1	0.0	4	0.0	0	0.0	-100.0
Firearms Act	1,229	3.4	1,201	3.3	1,215	3.3	1,038	2.8	-18.6

Note: Data reflect criminal incidents that have been substantiated through investigation by Canadian police services. The offences which comprise the category of money laundering in the Uniform Crime Reporting Survey include: laundering proceeds of crime (CCC s.462.31) and restraint order violation (CCC s.462.33).

Source: Statistics Canada, Canadian Centre for Justice Statistics, Uniform Crime Reporting Survey.

Table 2
Police-reported crime for select non-violent offences, by province and territory, 2019

Type of offence	Canada		Newfoundland and Labrador		Prince Edward Island		Nova Scotia		New Brunswick		Quebec		Ontario		Manitoba		Saskatchewan		Alberta		British Columbia		Yukon		Northwest Territories		Nunavut	
	number	rate	number	rate	number	rate	number	rate	number	rate	number	rate	number	rate	number	rate	number	rate	number	rate	number	rate	number	rate	number	rate	number	rate
Total Property Crime	1,237,324	3,338.8	15,605	2,970.4	4,646	2,966.5	27,488	2,863.5	23,433	3,040.7	148,817	1,773.6	375,402	2,621.0	75,580	5,589.6	74,800	6,436.8	234,076	5,434.6	238,141	4,770.8	3,847	9,504.4	9,284	20,798.8	6,325	16,473.1
Theft																												
Theft over \$5,000	14,749	39.8	171	32.5	23	15.0	226	23.5	206	26.7	2,366	28.2	4,470	31.2	426	31.5	493	42.4	2,985	69.3	3,330	66.7	26	64.2	16	35.9	11	28.6
Theft over \$5,000 from a motor vehicle	4,864	12.6	31	5.9	4	2.6	69	7.2	28	3.6	1,098	13.1	1,158	8.1	112	8.3	103	8.9	898	20.8	1,156	23.2	5	12.4	2	4.5	0	0.0
Shoplifting over \$5,000	700	1.9	52	9.9	2	1.3	10	1.0	13	1.7	80	1.1	259	1.8	23	1.7	22	1.9	125	2.9	94	1.9	5	12.4	2	4.5	4	10.4
Motor Vehicle Theft	86,078	232.3	490	93.3	127	82.9	892	92.9	1,319	171.2	12,448	148.4	23,916	167.0	4,705	348.0	5,699	490.4	23,499	545.6	12,570	251.8	132	326.1	181	406.4	100	260.4
Theft \$5,000 or under	213,823	577.0	2,320	441.6	761	496.6	7,828	815.5	4,249	551.4	26,255	312.9	80,227	560.1	9,467	700.1	11,070	952.8	32,356	751.2	37,918	759.6	566	1,373.7	582	1,306.7	234	609.4
Theft \$5,000 or under from a motor vehicle	192,556	519.6	224	175.9	740	482.9	3,165	329.7	2,492	323.4	17,385	207.2	53,470	373.3	9,210	688.5	7,572	651.6	38,415	891.9	58,816	1,178.3	197	486.7	65	145.9	5	13.0
Shoplifting \$5,000 or under	124,933	337.1	1,483	282.3	386	251.9	634	86.9	1,360	176.5	12,271	146.2	52,140	364.0	6,283	464.7	3,865	332.6	21,677	503.3	24,233	485.5	219	541.1	103	231.2	79	205.6
Possession/Trafficking Stolen Goods																												
Traffic stolen goods over \$5000 (incl intent)	325	0.9	0	0.0	0	0.0	9	0.9	3	0.4	38	0.5	79	0.6	10	0.7	15	1.3	159	3.7	11	0.2	0	0.0	1	2.2	0	0.0
Possession of Stolen Goods over \$5 000	10,991	29.7	35	6.7	20	13.1	63	6.6	138	17.9	520	6.2	2,064	14.4	506	37.4	1,047	90.1	5,574	129.4	1,006	20.2	8	19.8	10	22.5	0	0.0
Traffic stolen goods under \$5000 (incl intent)	524	1.4	5	1.0	6	3.9	4	0.4	10	1.3	76	0.9	76	0.5	30	2.6	286	6.6	20	0.4	2	4.9	2	4.9	2	4.5	0	0.0
Possession of Stolen Goods \$5 000 or under	12,045	32.5	54	10.3	60	39.2	486	50.6	206	26.7	916	10.9	2,622	18.3	575	42.5	722	62.1	3,906	90.7	2,447	49.0	21	51.9	22	49.4	8	20.6
Fraud																												
Fraud	129,409	349.2	1,602	304.9	508	330.2	4,338	451.7	3,588	465.6	16,924	201.7	49,193	343.5	4,630	342.4	5,957	512.6	22,096	513.0	20,160	403.9	175	432.4	168	377.2	74	192.7
Identity Theft	3,745	10.1	26	4.9	3	2.0	43	4.5	54	7.0	1,834	21.9	426	3.0	87	6.4	80	6.9	724	16.8	465	9.3	1	2.5	1	2.2	1	2.6
Identity Fraud	15,839	42.7	45	8.6	25	16.3	192	19.0	137	17.8	4,143	49.4	4,907	34.3	273	20.2	604	53.7	2,281	53.0	3,203	64.2	6	14.8	10	22.5	3	7.8
Mischief																												
Altering/Removing/Destroying Vehicle Identification Number (VIN)	99	0.3	0	0.0	1	0.7	1	0.1	2	0.3	41	0.5	17	0.1	2	0.1	2	0.2	27	0.6	6	0.1	0	0.0	0	0.0	0	0.0
Gaming and Betting																												
Betting house	2	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	2	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0
Gaming house	67	0.2	1	0.2	0	0.0	0	0.0	0	0.0	4	0.0	51	0.4	0	0.0	1	0.1	2	0.0	8	0.2	0	0.0	0	0.0	0	0.0
Other violations related to gaming and betting	62	0.2	9	1.7	1	0.7	2	0.2	1	0.1	3	0.0	22	0.2	3	0.2	6	0.5	2	0.0	13	0.3	0	0.0	0	0.0	0	0.0
Common Bawdy House (to keep, to transport a person to)	19	0.1	0	0.0	0	0.0	0	0.0	4	0.5	1	0.0	1	0.0	0	0.0	1	0.1	0	0.0	12	0.2	0	0.0	0	0.0	0	0.0
Offensive Weapons																												
Weapons trafficking	107	0.3	3	0.6	0	0.0	2	0.2	3	0.4	16	0.2	38	0.3	10	0.7	7	0.6	12	0.3	14	0.3	0	0.0	1	2.2	1	2.6
Unauthorized importing or exporting of weapons	67	0.2	3	0.6	0	0.0	2	0.2	1	0.1	3	0.0	50	0.3	1	0.1	0	0.0	4	0.1	3	0.1	0	0.0	0	0.0	0	0.0
Other Criminal Code Violations																												
Counterfeiting	1,095	3.0	6	1.1	1	0.7	26	2.7	59	7.7	197	2.3	376	2.6	31	2.3	51	4.4	175	4.1	168	3.4	3	7.4	1	2.2	1	2.6
Other offences against the administration of law and justice (Part IV CC)	7,815	20.5	83	15.8	52	33.9	183	19.1	107	13.9	1,042	12.4	1,846	12.9	959	70.9	350	30.1	1,760	40.9	944	18.9	60	148.2	131	294.1	98	255.2
Offences against rights of property (Part IX CC)	1,844	5.0	5	1.0	3	2.0	11	1.1	14	1.8	100	1.2	538	3.8	77	5.7	93	8.0	406	9.4	596	11.9	0	0.0	0	0.0	1	2.6
Fraudulent transactions relating to contracts and trade (Part X CC)	167	0.5	3	0.6	0	0.0	15	1.6	9	1.2	75	0.9	36	0.3	0	0.0	3	0.3	19	0.4	7	0.1	0	0.0	0	0.0	0	0.0
Willful and forbidden acts in respect of certain property (Part XI CC)	1,929	5.2	34	6.5	8	5.2	59	6.1	43	5.6	280	3.3	486	3.4	98	7.2	148	12.7	431	10.0	290	5.8	10	24.7	22	49.4	20	52.1
Offences relating to currency (Part XII CC)	93	0.3	0	0.0	0	0.0	1	0.1	0	0.0	55	0.7	4	0.0	1	0.1	7	0.6	13	0.3	12	0.2	0	0.0	0	0.0	0	0.0
Money laundering, proceeds of crime (Part XIII.2 CC)	218	0.6	8	1.5	0	0.0	11	1.1	2	0.3	56	0.7	54	0.4	15	1.1	10	0.9	33	0.8	27	0.5	1	2.5	1	2.2	0	0.0
Attempts, conspiracies, accessories (Part XIII CC)	215	0.6	1	0.2	1	0.7	5	0.5	14	1.8	101	1.2	71	0.5	3	0.2	4	0.3	8	0.2	7	0.1	0	0.0	0	0.0	0	0.0
Other Federal Statute Violations																												
Bankruptcy Act	44	0.1	0	0.0	0	0.0	0	0.0	2	0.3	21	0.3	7	0.0	1	0.1	3	0.3	9	0.2	1	0.0	0	0.0	0	0.0	0	0.0
Income Tax Act	9	0.0	0	0.0	0	0.0	0	0.0	1	0.1	2	0.0	2	0.0	0	0.0	2	0.2	1	0.0	1	0.0	0	0.0	0	0.0	0	0.0
Canada Shipping Act	3,875	10.5	1	0.2	5	3.3	6	0.6	4	0.5	97	1.2	1,375	9.6	83	6.1	6	0.5	15	0.3	2,283	45.7	0	0.0	0	0.0	0	0.0
Customs Act	9,221	24.9	4	0.8	0	0.0	0	0.0	11	1.4	8,837	105.3	54	0.4	178	13.2	23	2.0	15	0.3	98	2.0	1	2.5	0	0.0	0	0.0
Competition Act	12	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	9	0.1	0	0.0	0	0.0	1	0.0	2	0.0	0	0.0	0	0.0	0	0.0
Excise Act	208	0.6	19	3.6	6	3.9	17	1.8	42	5.5	36	0.5	65	0.5	8	0.6	4	0.3	2	0.0	4	0.1	0	0.0	3	6.7	0	0.0
Human Trafficking	112	0.3	2	0.4	0	0.0	8	0.8	0	0.0	3	0.0	94	0.7	1	0.1	1	0.1	2	0.0	1	0.0	0	0.0	0	0.0	0	0.0
Human Smuggling fewer than 10 persons	10	0.0	0	0.0	0	0.0	0	0.0	0	0.0	4	0.0	5	0.0	0	0.0	0	0.0	0	0.0	1	0.0	0	0.0	0	0.0	0	0.0
Human Smuggling 10 persons or more	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0
Firearms Act	1,038	2.8	56	10.7	5	3.3	19	2.0	15	1.9	28	0.3	82	0.4	36	2.7	162	13.9	262	6.1	369	7.4	15	37.1	7	15.7	2	5.2

Note: Data reflect criminal incidents that have been substantiated through investigation by Canadian police services. The offences which comprise the category of money laundering in the Uniform Crime Reporting Survey include: laundering proceeds of crime (CCC s.462.31) and restraint order violation (CCC s.462.33).
Source: Statistics Canada, Canadian Centre for Justice Statistics, Uniform Crime Reporting Survey.

Table 3
Police-reported incidents of money laundering - proceeds of crime (Part XII.2 CC), Canada, 2008 to 2018

Statistics	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
						number					
Actual incidents	452	520	405	379	291	263	276	248	237	328	218
						rate					
Rate per 100,000 population	1.4	1.5	1.2	1.1	0.8	0.7	0.8	0.7	0.7	0.9	0.6
						percent					
Percentage change in rate	-10.6	13.7	-23.0	-7.3	-24.0	-10.6	3.9	-10.8	-5.5	36.8	-34.5
						number					
Total cleared	119	117	129	150	103	117	90	82	76	58	31
Cleared by charge ¹	51	53	46	82	72	86	58	63	50	40	21
Cleared otherwise ²	68	64	83	68	31	31	32	19	26	18	10
						number					
Total persons charged	62	55	54	60	59	81	66	80	69	52	22
Total adults charged	61	55	54	60	55	76	66	76	68	52	22
Total youth charged	1	0	0	0	4	5	0	4	1	0	0

1. At least one accused has been identified and there is a criminal charge laid or recommended to be laid against this individual in connection with this criminal incident.

2. An accused has been identified by police in relation to the criminal incident, and there is sufficient evidence to lay a charge, however a charge is not laid by police and the accused is processed by other means. Examples of charges cleared otherwise include warnings, cautions, alternative measures, extrajudicial sanctions and instances where the accused has died.

Note: Data reflect criminal incidents that have been substantiated through investigation by Canadian police services. The offences which comprise the category of money laundering in the Uniform Crime Reporting Survey include: laundering proceeds of crime (CCC s.462.31) and restraint order violation (CCC s.462.33).

Source: Statistics Canada, Canadian Centre for Justice Statistics, Uniform Crime Reporting Survey.

Table 4
Police-reported incidents of money laundering - proceeds of crime (Part XII.2 CC), by province and territory, 2018

Statistics	Canada	Newfoundland and Labrador	Prince Edward Island	Nova Scotia	New Brunswick	Quebec	Ontario	Manitoba	Saskatchewan	Alberta	British Columbia	Yukon	Northwest Territories	Nunavut
Actual incidents	218	8	0	11	2	56	54	15	10	33	27	1	1	0
Rate per 100,000 population	0.6	1.5	...	1.1	0.3	0.7	0.4	1.1	0.9	0.8	0.5	2.5	2.2	...
Total cleared	31	1	0	1	0	6	10	3	7	2	1	0	0	0
Cleared by charge ¹	21	0	0	1	0	3	7	2	6	1	1	0	0	0
Cleared otherwise ²	10	1	0	0	0	3	3	1	1	1	0	0	0	0
Total cleared	14.2	12.5	...	9.1	0.0	10.7	18.5	20.0	70.0	6.1	3.7	0.0	0.0	...
Cleared by charge ¹	9.6	0.0	...	9.1	0.0	5.4	13.0	13.3	60.0	3.0	3.7	0.0	0.0	...
Cleared otherwise ²	4.6	12.5	...	0.0	0.0	5.4	5.6	6.7	10.0	3.0	0.0	0.0	0.0	...
Total persons charged	22	0	0	0	0	3	7	2	9	0	1	0	0	0
Total adults charged	22	0	0	0	0	3	7	2	9	0	1	0	0	0
Total youth charged	0	0	0	0	0	0	0	0	0	0	0	0	0	0

1. At least one accused has been identified and there is a criminal charge laid or recommended to be laid against this individual in connection with this criminal incident.

2. An accused has been identified by police in relation to the criminal incident, and there is sufficient evidence to lay a charge, however a charge is not laid by police and the accused is processed by other means. Examples of charges cleared otherwise include warnings, cautions, alternative measures, extrajudicial sanctions and instances where the accused has died.

Note: Data reflect criminal incidents that have been substantiated through investigation by Canadian police services. The offences which comprise the category of money laundering in the Uniform Crime Reporting Survey include: laundering proceeds of crime (CCC s.462.31) and restraint order violation (CCC s.462.33).

Source: Statistics Canada, Canadian Centre for Justice Statistics, Uniform Crime Reporting Survey.

Table 5
Police-reported incidents involving money laundering - proceeds of crime (Part XII.2 CC), Canada, 2008 to 2018

	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
	number										
Number of police reported incidents that include money laundering	783	750	684	716	596	607	634	589	496	656	462
Number of police reported incidents where the most serious violation is money laundering	437	514	395	373	284	262	276	247	234	322	216
Number of police reported incidents that include money laundering but the most serious violation is not money laundering	346	236	289	343	312	345	358	342	262	334	246
Other most common violations in incidents that include money laundering	number of incidents that include the specified violation										
Money laundering, proceeds of crime (Part XII.2 CC)	783	750	684	716	596	607	634	589	496	656	462
Cocaine - trafficking	149	74	84	90	120	140	146	104	76	106	79
Fraud	70	37	61	111	81	95	89	115	89	114	63
Cannabis - trafficking (pre-legalization)	62	57	78	69	76	62	54	58	34	47	37
Fail to comply with order	29	23	33	49	61	77	63	56	47	44	27
Possession - cannabis (pre-legalization)	49	42	56	50	44	71	41	39	28	41	25
Other Controlled Drugs and Substances Act - trafficking	77	32	42	26	23	30	47	55	44	56	29
Possess stolen property ¹	65	78	100	68	22	13	1	1
Breach of probation	64	19	23	42	33	32	24	28	16	21	16
Possession of weapons	19	20	10	16	27	20	52	39	28	39	42
Possession - cocaine	34	30	20	27	32	35	15	27	18	15	10
Possession of Stolen Goods \$5 000 or under ²	33	28	48	35	30	33	25	19
Possession of Stolen Goods over \$5 000 ²	14	23	11	43	48	32	29	25
Other Controlled Drugs and Substances Act - possession	19	12	14	23	29	31	20	12	22	14	7
Methamphetamines (Crystal meth) - trafficking	3	5	4	2	8	7	15	16	31	52	46
Weapons possession contrary to order	3	3	2	3	7	9	15	14	11	12	19
Attempts, conspiracies, accessories (Part XIII CC)	8	8	10	12	10	14	8	7	7	10	3
Other most common violations in incidents that include money laundering	percent of incidents that include the specified violation										
Money laundering, proceeds of crime (Part XII.2 CC)	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0
Cocaine - trafficking	19.0	9.9	12.3	12.6	20.1	23.1	23.0	17.7	15.3	16.2	17.1
Fraud	8.9	4.9	8.9	15.5	13.6	15.7	14.0	19.5	17.9	17.4	13.6
Cannabis - trafficking (pre-legalization)	7.9	7.6	11.4	9.6	12.8	10.2	8.5	9.8	6.9	7.2	8.0
Fail to comply with order	3.7	3.1	4.8	6.8	10.2	12.7	9.9	9.5	9.5	6.7	5.8
Possession - cannabis (pre-legalization)	6.3	5.6	8.2	7.0	7.4	11.7	6.5	6.6	5.6	6.3	5.4
Other Controlled Drugs and Substances Act - trafficking	9.8	4.3	6.1	3.6	3.9	4.9	7.4	9.3	8.9	8.5	6.3
Possess stolen property ¹	8.3	10.4	14.6	9.5	3.7	2.1	0.2	0.2
Breach of probation	8.2	2.5	3.4	5.9	5.5	5.3	3.8	4.8	3.2	3.2	3.5
Possession of weapons	2.4	2.7	1.5	2.2	4.5	3.3	8.2	6.6	5.6	5.9	9.1
Possession - cocaine	4.3	4.0	2.9	3.8	5.4	5.8	2.4	4.6	3.6	2.3	2.2
Possession of Stolen Goods \$5 000 or under ²	4.6	4.7	7.9	5.5	5.1	6.7	3.8	4.1
Possession of Stolen Goods over \$5 000 ²	2.0	3.9	1.8	6.8	8.1	6.5	4.4	5.4
Other Controlled Drugs and Substances Act - possession	2.4	1.6	2.0	3.2	4.9	5.1	3.2	2.0	4.4	2.1	1.5
Methamphetamines (Crystal meth) - trafficking	0.4	0.7	0.6	0.3	1.3	1.2	2.4	2.7	6.3	7.9	10.0
Weapons possession contrary to order	0.4	0.4	0.3	0.4	1.2	1.5	2.4	2.4	2.2	1.8	4.1
Attempts, conspiracies, accessories (Part XIII CC)	1.0	1.1	1.5	1.7	1.7	2.3	1.3	1.2	1.4	1.5	0.6

1. The offence possess stolen property expired April 28, 2011 and was replaced with the offences possession of stolen goods \$5,000 or under and possession of stolen goods over \$5,000.

2. The offences possession of stolen goods \$5,000 or under and possession of stolen goods over \$5,000 were introduced April 29, 2011.

Note: Data reflect criminal incidents that have been substantiated through investigation by Canadian police services. The offences which comprise the category of money laundering in the Uniform Crime Reporting Survey include: laundering proceeds of crime (CCC s.462.31) and restraint order violation (CCC s.462.33). The Uniform Crime Reporting Survey captures up to four violations for each incident. Information on associated violations and persons accused of police-reported crimes are drawn from the Incident-based Uniform Crime Reporting Survey which, as of 2009, covered 99% of the population of Canada.

Source: Statistics Canada, Canadian Centre for Justice Statistics, Incident-based Uniform Crime Reporting Survey.

Table 6

Accused identified in relation to police-reported incidents of money laundering - proceeds of crime (Part XII.2 CC), Canada, 2008 to 2018

	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
	number										
Number of police reported incidents where the most serious violation is money laundering	437	514	395	373	284	262	276	247	234	322	216
Total number of accused	152	138	134	152	133	155	102	110	90	77	39
Gender ¹	number										
female	29	22	23	25	30	31	13	26	12	19	12
male	123	116	111	127	103	124	88	84	77	57	27
Gender ¹	percent										
female	19.1	15.9	17.2	16.4	22.6	20.0	12.9	23.6	13.5	25.0	30.8
male	80.9	84.1	82.8	83.6	77.4	80.0	87.1	76.4	86.5	75.0	69.2
Age ²	number										
Under 18	5	1	2	3	3	5	0	5	1	2	0
18 to 24	43	30	29	26	34	22	29	25	23	17	10
25 to 34	37	43	35	60	44	70	39	33	32	29	18
35 to 44	33	33	29	26	22	33	19	29	12	18	7
45 to 54	23	14	27	29	25	23	7	13	15	8	1
55 and older	11	17	12	8	5	2	8	5	7	2	2
Age ²	percent										
Under 18	3.3	0.7	1.5	2.0	2.3	3.2	0.0	4.5	1.1	2.6	0.0
18 to 24	28.3	21.7	21.6	17.1	25.6	14.2	28.4	22.7	25.6	22.4	26.3
25 to 34	24.3	31.2	26.1	39.5	33.1	45.2	38.2	30.0	35.6	38.2	47.4
35 to 44	21.7	23.9	21.6	17.1	16.5	21.3	18.6	26.4	13.3	23.7	18.4
45 to 54	15.1	10.1	20.1	19.1	18.8	14.8	6.9	11.8	16.7	10.5	2.6
55 and older	7.2	12.3	9.0	5.3	3.8	1.3	7.8	4.5	7.8	2.6	5.3

1. Excludes accused where the gender was unknown or invalid.

2. Excludes accused with an unknown or invalid age.

Note: Data reflect criminal incidents that have been substantiated through investigation by Canadian police services. The offences which comprise the category of money laundering in the Uniform Crime Reporting Survey include: laundering proceeds of crime (CCC s.462.31) and restraint order violation (CCC s.462.33). The Uniform Crime Reporting Survey captures up to four violations for each incident. Information on associated violations and persons accused of police-reported crimes are drawn from the Incident-based Uniform Crime Reporting Survey which, as of 2009, covered 99% of the population of Canada.

Source: Statistics Canada, Canadian Centre for Justice Statistics, Incident-based Uniform Crime Reporting Survey.

Table 7

Accused identified in relation to police-reported incidents involving money laundering - proceeds of crime (Part XII.2 CC), Canada, 2008 to 2018

	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
	number										
Number of police reported incidents that include money laundering	783	750	684	716	596	607	634	589	496	656	462
Total number of accused	678	548	602	727	701	803	720	673	565	601	463
	number										
Gender ¹											
female	140	96	130	151	168	200	163	161	142	163	134
male	537	452	471	576	532	603	552	512	422	436	328
	percent										
Gender ¹											
female	20.7	17.5	21.6	20.8	24.0	24.9	22.8	23.9	25.2	27.2	29.0
male	79.3	82.5	78.4	79.2	76.0	75.1	77.2	76.1	74.8	72.8	71.0
	number										
Age ²											
Under 18	27	23	33	19	30	26	32	28	5	12	17
18 to 24	198	177	182	183	198	225	205	156	167	148	114
25 to 34	180	163	164	277	237	282	258	238	192	245	200
35 to 44	157	107	108	116	114	150	117	138	111	121	87
45 to 54	88	46	80	103	93	96	71	84	56	50	31
55 and older	27	32	35	29	29	24	34	29	34	23	13
	percent										
Age ²											
Under 18	4.0	4.2	5.5	2.6	4.3	3.2	4.5	4.2	0.9	2.0	3.7
18 to 24	29.2	32.3	30.2	25.2	28.2	28.0	28.6	23.2	29.6	24.7	24.7
25 to 34	26.6	29.7	27.2	38.1	33.8	35.1	36.0	35.4	34.0	40.9	43.3
35 to 44	23.2	19.5	17.9	16.0	16.3	18.7	16.3	20.5	19.6	20.2	18.8
45 to 54	13.0	8.4	13.3	14.2	13.3	12.0	9.9	12.5	9.9	8.3	6.7
55 and older	4.0	5.8	5.8	4.0	4.1	3.0	4.7	4.3	6.0	3.8	2.8

1. Excludes accused where the gender was unknown or invalid.

2. Excludes accused with an unknown or invalid age.

Note: Data reflect criminal incidents that have been substantiated through investigation by Canadian police services. The offences which comprise the category of money laundering in the Uniform Crime Reporting Survey include: laundering proceeds of crime (CCC s.462.31) and restraint order violation (CCC s.462.33). The Uniform Crime Reporting (UCR) Survey captures up to four violations for each incident. Information on associated violations and persons accused of police-reported crimes are drawn from the Incident-based Uniform Crime Reporting Survey which, as of 2009, covered 99% of the population of Canada.

Source: Statistics Canada, Canadian Centre for Justice Statistics, Incident-based Uniform Crime Reporting Survey.

Table 8
Completed cases of money laundering, adult criminal courts, Canada, 2008/2009 to 2016/2017

	2008/2009	2009/2010	2010/2011	2011/2012	2012/2013	2013/2014	2014/2015	2015/2016	2016/2017
number									
Completed court cases where money laundering is the most serious offence	98	88	87	130	109	122	91	136	135
Court decision									
number									
Guilty	26	30	16	31	30	41	33	37	27
Acquitted of offence charged ²	0	2	0	0	4	8	5	8	4
Stay of proceeding ³	11	7	8	13	15	17	5	23	17
Withdrawn/Dismissed/Discharged ⁴	60	49	63	74	57	52	45	60	79
Other decision ⁵	1	0	0	12	3	4	3	8	8
percent									
Guilty ¹	26.5	34.1	18.4	23.8	27.5	33.6	36.3	27.2	20.0
Acquitted of offence charged ²	0.0	2.3	0.0	0.0	3.7	6.6	5.5	5.9	3.0
Stay of proceeding ³	11.2	8.0	9.2	10.0	13.8	13.9	5.5	16.9	12.6
Withdrawn/Dismissed/Discharged ⁴	61.2	55.7	72.4	56.9	52.3	42.6	49.5	44.1	58.5
Other decision ⁵	1.0	0.0	0.0	9.2	2.8	3.3	3.3	5.9	5.9
Most serious sentence for guilty decisions									
number									
Custody	17	20	8	15	18	19	16	21	12
Conditional sentence	4	2	3	6	5	9	4	4	7
Probation	2	3	4	6	2	10	6	7	6
Fine	1	1	1	0	2	0	3	1	0
Other sentence ⁶	2	4	0	4	3	3	4	4	2
percent									
Custody	65.4	66.7	50.0	48.4	60.0	46.3	48.5	56.8	44.4
Conditional sentence	15.4	6.7	18.8	19.4	16.7	22.0	12.1	10.8	25.9
Probation	7.7	10.0	25.0	19.4	6.7	24.4	18.2	18.9	22.2
Fine	3.8	3.3	6.3	0.0	6.7	0.0	9.1	2.7	0.0
Other sentence ⁶	7.7	13.3	0.0	12.9	10.0	7.3	12.1	10.8	7.4
Most common charges in cases where the most serious offence was money laundering									
number of cases with at least one other specified charge									
Money laundering, proceeds of crime (Part XII.2 CC)	98	88	87	130	109	122	91	136	135
Fraud	39	27	39	63	56	58	50	80	79
Possession of Stolen Goods \$5 000 or under ⁷	29	64	51	62	42	66	59
Attempts, conspiracies, accessories (Part XIII CC)	45	29	24	39	30	34	21	36	45
Possession of Stolen Goods over \$5 000 ⁷	11	27	25	19	10	16	25
Other Controlled Drugs and Substances Act - trafficking	23	11	23	10	14	10	9	12	15
Possess stolen property ⁸	44	45	8	1
Other federal statutes	12	5	2	3	4	10	14	23	22
Fail to comply with order	6	10	4	11	10	9	13	8	4
Theft over \$5,000	6	6	5	0	1	12	12	12	16
Other Controlled Drugs and Substances Act - possession	14	13	4	9	9	4	1	3	11
Theft \$5,000 or under	4	3	8	15	6	8	8	8	5
percent of cases with at least one other specified charge									
Money laundering, proceeds of crime (Part XII.2 CC)	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0
Fraud	39.8	30.7	44.8	48.5	51.4	47.5	54.9	58.8	58.5
Possession of Stolen Goods \$5 000 or under ⁷	33.3	49.2	46.8	50.8	46.2	48.5	43.7
Attempts, conspiracies, accessories (Part XIII CC)	45.9	33.0	27.6	30.0	27.5	27.9	23.1	26.5	33.3
Possession of Stolen Goods over \$5 000 ⁷	12.6	20.8	22.9	15.6	11.0	11.8	18.5
Other Controlled Drugs and Substances Act - trafficking	23.5	12.5	26.4	7.7	12.8	8.2	9.9	8.8	11.1
Possess stolen property ⁸	44.9	51.1	9.2	0.8
Other federal statutes	12.2	5.7	2.3	2.3	3.7	8.2	15.4	16.9	16.3
Fail to comply with order	6.1	11.4	4.6	8.5	9.2	7.4	14.3	5.9	3.0
Theft over \$5,000	6.1	6.8	5.7	0.0	0.9	9.8	13.2	8.8	11.9
Other Controlled Drugs and Substances Act - possession	14.3	14.8	4.6	6.9	8.3	3.3	1.1	2.2	8.1
Theft \$5,000 or under	4.1	3.4	9.2	11.5	5.5	6.6	8.8	5.9	3.7

1. Guilty findings include guilty of the charged offence, of an included offence, of an attempt of the charged offence, or an attempt of an included offence. This category also includes guilty pleas, and cases where an absolute or conditional discharge has been imposed.

2. Acquittal means that the accused has been found not guilty of the charges presented before the court.

3. Stay of proceeding refers to stays, as well as court referrals to alternative or extrajudicial measures and restorative justice programs. These decisions all refer to the court stopping criminal proceedings against the accused.

4. Withdrawn/Dismissed/Discharged includes withdrawals, dismissals and discharges at preliminary inquiries. These decisions all refer to the court stopping criminal proceedings against the accused.

5. Other decisions includes unknown sentences. This category also includes other final decisions such as waived out of province or territory, not criminally responsible, any order where a conviction was not recorded, the court's acceptance of a special plea, cases which raise Charter arguments and cases where the accused was found unfit to stand trial, among others.

6. Other sentences include absolute and conditional discharge, suspended sentence, community service order and prohibition, among others.

7. The offences possession of stolen goods \$5,000 or under and possession of stolen goods over \$5,000 were introduced April 29, 2011.

8. The offence possess stolen property expired April 28, 2011 and was replaced with the offences possession of stolen goods \$5,000 or under and possession of stolen goods over \$5,000.

Note: This product is based on data from the adult component of the Integrated Criminal Court Survey (ICCS). The ICCS is administered by the Canadian Centre for Justice Statistics (Statistics Canada) in collaboration with provincial and territorial government departments responsible for criminal courts in Canada. The survey collects statistical information on adult and youth court cases involving Criminal Code and other federal statute offences. Data contained in this table represent the adult criminal court portion of the survey, namely, individuals who were 18 years of age or older at the time of the offence. Data are based on a fiscal year (April 1 through March 31). A case is one or more charges against an accused person or company that were processed by the courts at the same time and received a final decision. Cases are counted according to the fiscal year in which they are completed. Each year, the ICCS database is considered final at the end of March for the production of court statistics pertaining to the preceding fiscal year. However, these counts do not include cases that were pending a final decision at the end of the reference period. If a final decision is reached in the next fiscal year, then these cases are included in the completed case counts for that fiscal year. However, if a one-year period of inactivity elapses, then these cases are deemed complete and the originally published counts for the previous fiscal year are subsequently updated and reported in the next year's release of the data. Data exclude information from superior courts in Prince Edward Island, Ontario, Manitoba and Saskatchewan as well as municipal courts in Quebec due to the unavailability of data. In concordance with the Uniform Crime Reporting (UCR) Survey, money laundering comprises laundering proceeds of crime (CCC s.462.31) and restraint order violation (CCC s.462.33).

Source: Statistics Canada, Canadian Centre for Justice Statistics, Integrated Criminal Court Survey.

Table 9
Completed cases where money laundering is one charge in the case, adult criminal courts, Canada, 2008/2009 to 2016/2017

Year	2008/2009	2009/2010	2010/2011	2011/2012	2012/2013	2013/2014	2014/2015	2015/2016	2016/2017
Completed court cases where money laundering is one charge in the case	146	141	184	241	235	241	208	237	264
Most serious offence in a case with at least one money laundering charge									
Crimes against the person	number								
Murder 1st degree	0	0	0	0	0	0	0	1	0
Manslaughter	0	0	0	0	0	1	1	0	0
Conspire to commit murder	0	0	0	0	0	0	0	0	1
Using firearm in commission of offence	0	0	1	0	0	1	0	0	0
Hostage-taking	0	0	0	0	0	0	1	0	0
Robbery	1	0	1	2	1	1	1	2	1
Extortion	0	0	1	0	1	0	0	0	0
Uttering threats	1	0	0	0	0	0	1	0	0
Crimes against property									
Breaking and entering	0	2	5	5	5	3	1	5	0
Theft over \$5,000	0	1	2	2	2	3	3	1	2
Motor Vehicle Theft	0	0	0	0	0	0	0	0	1
Theft \$5,000 or under	0	0	3	3	1	8	1	2	1
Possess stolen property ¹	6	11	0	0	0	0	0	0	0
Traffic stolen goods over \$5000 (incl intent)	0	0	0	0	0	0	0	0	2
Possession of Stolen Goods over \$5 000 ²	0	0	2	3	3	3	3	2	4
Possession of Stolen Goods \$5 000 or under ²	0	0	11	9	6	12	12	5	6
Fraud	9	12	26	55	55	51	62	47	48
Identity Theft	0	0	0	2	6	3	2	4	10
Identity Fraud	0	0	1	0	0	0	0	0	0
Mischief	0	0	0	0	0	0	0	0	2
Altering/Removing/Destroying Vehicle Identification Number (VIN)	0	0	0	0	0	0	0	0	2
Other Criminal Code Violations									
Obtains or communicates with a person under 18 for purpose of sex	0	0	0	0	0	0	0	0	1
Other violations related to gaming and betting	0	1	0	0	0	0	0	0	0
Offensive weapons: explosives	0	0	0	1	0	0	0	0	0
Weapons trafficking	0	0	0	0	0	0	0	2	0
Weapons possession contrary to order	0	0	1	0	0	1	0	0	0
Possession of weapons	0	0	0	0	2	0	1	0	4
Unauthorized importing or exporting of weapons	0	1	0	0	0	0	0	0	0
Fail to comply with order	1	0	0	2	0	2	0	1	1
Counterfeiting	0	0	0	1	0	0	3	2	4
Making, or distribution of child pornography	0	0	0	0	0	0	0	0	1
Obstruct public/peace officer	0	0	0	0	1	0	0	0	0
Fail to appear	0	0	0	1	0	0	1	0	0
Breach of probation	3	1	3	0	0	0	0	0	0
Firearms and other offensive weapons (Part III CC)	1	0	0	0	0	0	0	0	0
Other offences against the administration of law and justice (Part IV CC)	0	0	0	0	1	0	0	1	0
Offences against rights of property (Part IX CC)	0	0	0	0	1	0	0	1	1
Fraudulent transactions relating to contracts and trade (Part X CC)	0	0	0	1	1	0	0	0	0
Offences relating to currency (Part XII CC)	0	0	0	0	0	0	0	0	3
Money laundering, proceeds of crime (Part XII.2 CC)	98	88	87	130	109	122	91	136	135
Attempts, conspiracies, accessories (Part XIII CC)	1	5	9	4	3	4	2	2	5
Instruct offence for criminal organization	0	0	1	0	4	3	0	1	0
Commit offence for criminal organization	3	0	7	4	14	6	8	10	18
Participate in activities of criminal organization	0	0	0	4	2	1	0	0	0
All other Criminal Code (includes Part XII.1 CC)	1	0	0	0	0	0	0	0	0
Controlled Drugs and Substances Act									
Other Controlled Drugs and Substances Act - possession	5	3	2	4	5	5	2	0	2
Other Controlled Drugs and Substances Act - trafficking	12	10	15	4	9	9	8	10	7
Other Controlled Drugs and Substances Act - importation and exportation	1	0	0	0	0	0	0	0	0
Other Controlled Drugs and Substances Act - production	0	1	1	1	0	0	0	0	0
Other Federal Statutes									
Excise Act	0	0	0	0	0	0	1	0	0
Youth Criminal Justice Act	0	0	0	0	1	0	0	0	0
Firearms Act	1	0	0	0	0	0	0	0	0
Other federal statutes	2	4	5	2	1	1	2	0	1
Traffic Violations									
Dangerous operation of motor vehicle, vessel or aircraft	0	1	0	1	0	0	0	1	0
Dangerous operation of motor vehicle evading police	0	0	0	0	1	0	0	0	1
Impaired operation - failure to provide breath sample	0	0	0	0	0	0	0	1	0
Driving while prohibited	0	0	0	0	0	1	1	0	0

1. The offence possess stolen property expired April 28, 2011 and was replaced with the offences possession of stolen goods \$5,000 or under and possession of stolen goods over \$5,000.

2. The offences possession of stolen goods \$5,000 or under and possession of stolen goods over \$5,000 were introduced April 29, 2011

Note: This product is based on data from the adult component of the Integrated Criminal Court Survey (ICCS). The ICCS is administered by the Canadian Centre for Justice Statistics (Statistics Canada) in collaboration with provincial and territorial government departments responsible for criminal courts in Canada. The survey collects statistical information on adult and youth court cases involving Criminal Code and other federal statute offences. Data contained in this table represent the adult criminal court portion of the survey, namely, individuals who were 18 years of age or older at the time of the offence. Data are based on a fiscal year (April 1 through March 31). A case is one or more charges against an accused person or company that were processed by the courts at the same time and received a final decision. Cases are counted according to the fiscal year in which they are completed. Each year, the ICCS database is considered final at the end of March for the production of court statistics pertaining to the preceding fiscal year. However, these counts do not include cases that were pending a final decision at the end of the reference period. If a final decision is reached in the next fiscal year, then these cases are included in the completed case counts for that fiscal year. However, if a one-year period of inactivity elapses, then these cases are deemed complete and the originally published counts for the previous fiscal year are subsequently updated and reported in the next year's release of the data. Data exclude information from superior courts in Prince Edward Island, Ontario, Manitoba and Saskatchewan as well as municipal courts in Quebec due to the unavailability of data. In concordance with the Uniform Crime Reporting (UCR) Survey, money laundering comprises laundering proceeds of crime (CCC s.462.31) and restraint order violation (CCC s.462.33).

Source: Statistics Canada, Canadian Centre for Justice Statistics, Integrated Criminal Court Survey.

Appendix 11

Guide on Using Money Laundering and Proceeds of Crime Data
from Uniform Reporting Survey (UCR) and the Integrated Criminal
Courts Survey (ICCS)

Data on Money Laundering/Proceeds of Crime from the Uniform Crime Reporting Survey (UCR) and the Integrated Criminal Courts Survey (ICCS)

What do data users need to know?

The Uniform Crime Reporting Survey

How does the UCR collect information on proceeds of Crime?

The UCR Survey, administered by the Canadian Centre for Justice and Community Safety Statistics (CCJCSS), collects information only on those crimes that come to the attention of, and are substantiated by, the police. The UCR data, therefore, do not contain a count of all crimes in Canada: some crimes are never detected and, of those that are, some are never brought to the attention of the police.

Data are collected directly from the police services and extracted from their administrative files. The response rate in terms of police respondents complying with the UCR Survey is virtually 100 percent. There are more than 1,000 separate police services (including detachments) responding to the survey, comprising of 193 different police forces.

The UCR captures money laundering/proceeds of crime information using the survey's violation code of 3825 Proceeds of Crime (Part XII.2 CC) (effective 1998-01-01)

The following sections of the *Criminal Code of Canada* are included in this violation code:

- 462.31(1)(a)(b) 3825 LAUNDERING PROCEEDS OF CRIME - DEFINITION
- 462.31(2)(a) 3825 10 LAUNDERING PROCEEDS OF CRIME - PUN - IND
- 462.31(2)(b) 3825 2 LAUNDERING PROCEEDS OF CRIME - PUN - SC
- 462.33(11) 3825 2 RESTRAINT ORDER VIOLATION - PUN - IND
- 462.33(11) 3825 2 RESTRAINT ORDER VIOLATION - PUN - SC

Where to find the data?

Table: 35-10-0177-01, "Incident-based crime statistics, by detailed violations, Canada, provinces, territories and Census Metropolitan Areas" contains UCR proceeds of crime data covering the period from 1998 to 2018. It is available free, at the following Statistics Canada web link:

<https://www150.statcan.gc.ca/t1/tbl1/en/tv.action?pid=3510017701>

To access the requested data in the link above, please follow these steps:

1. Click on the Add/Remove data tab
2. Select desired Geography
3. From the Violations list you can use the filter to search for the appropriate violation. In this case, 3825 for "Proceeds of crime (Part XII.2 Criminal Code) [3825]"

4. From the Statistics list select: A) cleared by charge (*Item 1- charges*); (B) cleared otherwise (*Item 2- without charges*); (C) total cleared (*Item 8 - concluded*)
5. From the Time frame select your desired time frame
6. Click the Apply button

What do these data represent?

The resulting data table presents “total cleared” police-reported counts of proceeds of crime incidents, broken down by the count of incidents that are “cleared by charge” or “cleared otherwise”.

In other words:

Data which falls under Total Cleared includes those cases which were cleared by charge, or cleared otherwise. “Cleared” is sometimes more commonly referred to as “solved”.

Cleared by charge (includes charges recommended) – At least one CSC (Charged Suspect Chargeable) or accused has been identified and there is a criminal charge laid or recommended to be laid against this individual in connection with this criminal incident.

Cleared otherwise – The police do not proceed with a charge for one of several possible reasons (e.g., death of CSC, Diplomatic immunity, CSC under 12 years of age, CSC committed to mental health facility, among others).

In order for a case to be cleared otherwise, the following criteria must be met

1. At least one accused person has been identified, and
2. There is sufficient evidence to lay a charge in connection with the incident, but for some reason, the accused person is processed by other means (e.g., accused is placed in an official diversionary program).

Total Cleared (*concluded*) = Cleared by charge (*charges*) + cleared otherwise (*without charges*)

On the other hand, counts of incidents which are open (under investigation) are included in the category of not cleared (sometimes referred to as “not solved”). *This indicator is not included in this data table*; however it can be calculated by taking Actual incidents minus Total cleared.

Not cleared includes the following situations:

- Incidents which are open/still under investigation
- Incidents where there is insufficient evidence to proceed
- Incidents where the victim/complainant declines to proceed (and therefore no accused person can be identified)

The following link is to the UCR IMDB Survey documentation:

<https://www23.statcan.gc.ca/imdb/p2SV.pl?Function=getSurvey&Id=1244230#a3>

What are other important UCR data notes?

1. Defining an Incident in the UCR – An incident is defined as a set of connected events usually constituting a police occurrence report. An incident may involve several victims, several CSCs, and multiple violations of the law.
2. Counts are based on the most serious violation in the incident. An incident can contain one to four violation codes. The most serious violation (MSV) of an incident is determined by the maximum penalty as outlined in the *Criminal Code of Canada*. In categorizing incidents, violent offences always take precedence over non-violent offences. For example, an incident involving both a breaking and entering offence and an assault is counted as an incident of assault.

As a result of the MSV scoring rule, less serious offences are under-counted by the aggregate survey. However, the incident-based survey allows up to four violations per incident, permitting the identification of lesser offences.

In the case of money laundering, we can still calculate any incident with a money laundering violation, as long as it is one of the four most serious violations reported within an incident.

3. Police reported statistics may be affected by differences in the way police services deal with minor offences. In some instances, police or municipalities might chose to deal with some minor offences using municipal by-laws or provincial provisions rather than Criminal Code provisions. This should not affect money laundering incidents.
4. The quality and accuracy of data submitted through to the UCR Survey is checked through a series of programs which identify duplicates, missing or incorrect information. Issues identified through this processes are shared with police services so that corrections can be made. The CCJS does not conduct audits of police department's records management units to ensure complete and accurate reporting. Nor does the CCJS examine records which the police have processed and determined to be outside the scope of the survey.
5. During each data production cycle, data are always sent back to police services for verification and sign-off. This allows police the opportunity to correct any records. In the case of money laundering, police receive tables with their UCR data for review before counts are publish by the Canadian Centre for Justice and Community Safety Statistics (CCJCSS).

The Integrated Criminal Court Survey (ICCS)

The Integrated Criminal Court Survey (ICCS) collects statistical information on adult criminal and youth court cases involving *Criminal Code* and other federal statute offences. The ICCS draws on information from the administrative databases in operation in the youth and adult criminal courts in the provinces and territories. Micro-data are extracted electronically from administrative databases by means of a software interface and submitted to Statistics Canada in an electronic format.

For the timeframe covered by the accompanying data table, information from superior courts in Prince Edward Island, Ontario, Manitoba and Saskatchewan was not available for extraction from their electronic reporting systems and was therefore not reported to the survey.

Understanding the Primary Unit of Count – The Case

The ICCS collects appearance level data for federal statute charges. This is done in a “snapshot” manner, where each data extraction includes all court appearances pertaining to the reference period. Some of these appearances are rolled up to charges, and charges to cases. The primary unit of analysis for the ICCS is the case.

The ICCS defines a case as one or more charges against an accused person or company that were processed by the courts at the same time and received a final disposition. A case combines all charges against the same person having one or more key overlapping dates (i.e., date of offence, date of initiation, date of first appearance or date of decision) into a single case.

Cases are counted according to the fiscal year in which they are completed. Each year, the ICCS database is considered final at the end of March for the production of court statistics pertaining to the preceding fiscal year. These counts do not include cases that were pending a final decision at the end of the reference period.

How cases are represented in the ICCS Data – The ‘Most Serious Offence’ (MSO)

Cases frequently have more than one charge. These cases are typically represented by the charge with the ‘most serious offence’ (MSO) in ICCS data tables. When a case has multiple charges for multiple offences with varying decisions and sentencing outcomes, one of the charges in the case has to be selected to represent that case; otherwise you would be presenting multiple views of the same case. There are a series of rules that are applied during processing of the data in order to choose the charge where the accused received the “greatest punishment”, or in other words, the charge with the most serious offence (MSO).

Characteristics specific to this request

The data provided in response to this request represent adult criminal court cases where money laundering (*Criminal Code* section 462.31) was the most serious offence in the case. Related offences that were not included in the data are: possession of property obtained by crime (*Criminal Code* section 354), trafficking/importation of property obtained by crime (*Criminal Code* sections 355.2, 355.3), and bringing into Canada property obtained by crime (*Criminal Code* section 357). The inclusion of these offences would have added to the counts.

Similarly, only cases from adult criminal courts were included. The ICCS also contains data from youth courts. The inclusion of youth court cases would have led to a small increase in counts.

Data presented represent only completed cases where money laundering was the charge that was recorded by the courts on the final court appearance. There may be instances where an accused plead

or was found guilty of a lesser charge, or otherwise was initially charged with money laundering, which was modified to a different offence, during the life of the court case.

Comparing ICCS data with UCR data as well as data from other sectors of the criminal justice system

It is difficult to make comparisons between data reported by provincial and territorial government departments responsible for criminal courts in Canada and data from other sectors of the criminal justice system such as police services and corrections for the following reasons:

- There is no single unit of count (i.e., incidents, offences, charges, cases or persons) which is defined consistently across the major sectors of the justice system.
- Charges actually laid can be different from the most serious offence by which incidents are categorized in the UCR.
- Not all persons in conflict with the law appear in court. Court counts are not an indicator of total criminal activity in Canada, but rather, the counts describe the process and response to criminal activity in criminal courts.
- The number and type of charges laid by police may change at the pre-court stage or during the court process.
- Time lags between the various stages of the justice process also make comparisons difficult.

Appendix 12

ICCS Data Table

Money laundering (*Criminal Code* s.462.31) cases, by province and territory, adult criminal court, 2008/2009 to 2018/2019

Province/Territory	2008/09				2009/10			
	Total cases	Guilty cases	Guilty cases with prohibition order	Guilty cases with no/unknown prohibition order	Total cases	Guilty cases	Guilty cases with prohibition order	Guilty cases with no/unknown prohibition order
Newfoundland and Labrador	0	0	0	0	1	1	0	1
Prince Edward Island	0	0	0	0	0	0	0	0
Nova Scotia	2	2	1	1	3	0	0	0
New Brunswick	0	0	0	0	2	2	2	0
Quebec	9	4	0	4	21	16	0	16
Ontario	75	16	1	15	46	7	1	6
Manitoba	2	1	0	1	4	1	0	1
Saskatchewan	3	0	0	0	2	0	0	0
Alberta	1	0	0	0	3	0	0	0
British Columbia	5	2	2	0	6	3	0	3
Yukon	0	0	0	0	0	0	0	0
Northwest Territories	1	1	0	1	0	0	0	0
Nunavut	0	0	0	0	0	0	0	0
Canada	98	26	4	22	88	30	3	27

2010/11				2011/12				2012/13			
Total cases	Guilty cases	Guilty cases with prohibition order	Guilty cases with no/unknown prohibition order	Total cases	Guilty cases	Guilty cases with prohibition order	Guilty cases with no/unknown prohibition order	Total cases	Guilty cases	Guilty cases with prohibition order	Guilty cases with no/unknown prohibition order
1	1	0	1	2	1	1	0	2	1	0	1
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	2	0	0	0	1	1	0	1
0	0	0	0	2	1	0	1	0	0	0	0
3	2	0	2	12	10	0	10	15	7	0	7
65	9	0	9	95	14	0	14	73	19	0	19
2	0	0	0	4	0	0	0	1	0	0	0
5	1	0	1	4	2	0	2	7	0	0	0
8	1	0	1	1	0	0	0	5	0	0	0
1	0	0	0	6	3	1	2	1	1	1	0
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	1	0	0	0	1	0	0	0
1	1	0	1	1	0	0	0	2	0	0	0
86	15	0	15	130	31	2	29	108	29	1	28

2013/14				2014/15				2015/16			
Total cases	Guilty cases	Guilty cases with prohibition order	Guilty cases with no/unknown prohibition order	Total cases	Guilty cases	Guilty cases with prohibition order	Guilty cases with no/unknown prohibition order	Total cases	Guilty cases	Guilty cases with prohibition order	Guilty cases with no/unknown prohibition order
3	1	0	1	1	0	0	0	5	1	0	1
0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	3	1	1	0
2	0	0	0	0	0	0	0	1	1	0	1
14	8	2	6	16	10	0	10	20	9	1	8
75	25	0	25	60	18	0	18	84	15	0	15
3	0	0	0	0	0	0	0	3	1	0	1
7	4	0	4	1	0	0	0	3	1	0	1
8	2	0	2	8	4	0	4	4	0	0	0
4	2	1	1	5	1	0	1	4	3	0	3
0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	1	1	1	0	0	0	0	0
2	1	0	1	0	0	0	0	0	0	0	0
121	43	3	40	92	34	1	33	127	32	2	30

2016/17				2017/18				2018/19			
Total cases	Guilty cases	Guilty cases with prohibition order	Guilty cases with no/unknown prohibition order	Total cases	Guilty cases	Guilty cases with prohibition order	Guilty cases with no/unknown prohibition order	Total cases	Guilty cases	Guilty cases with prohibition order	Guilty cases with no/unknown prohibition order
4	1	0	1	2	1	0	1	1	1	0	1
0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	4	0	0	0	4	0	0	0
0	0	0	0	0	0	0	0	4	0	0	0
12	5	1	4	16	9	3	6	3	3	0	3
91	12	0	12	70	14	0	14	48	9	0	9
1	1	0	1	2	0	0	0	0	0	0	0
1	1	0	1	6	1	0	1	3	2	0	2
15	4	1	3	13	3	0	3	6	2	1	1
0	0	0	0	1	1	0	1	3	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0
126	24	2	22	114	29	3	26	72	17	1	16

Source: Statistics Canada, Canadian Centre for Justice and Community Safety Statistics, Integrated Criminal Court Survey.

Notes:

1. This product is based on data from the adult component of the Integrated Criminal Court Survey (ICCS). The ICCS is administered by the Canadian Centre for Justice and Community Safety Statistics (Statistics Canada) in collaboration with provincial and territorial government departments responsible for criminal courts in Canada. The survey collects statistical information on adult and youth court cases involving Criminal Code and other federal statute offences. Data contained in this table represents the adult criminal court portion of the survey, namely, individuals who were 18 years of age or older at the time of the offence. Data are based on a fiscal year (April 1 through March 31).
2. As of 2005/2006, adult criminal courts in ten provinces and three territories reported to the survey. Information from superior courts in Ontario, Manitoba and Saskatchewan as well as municipal courts in Quebec was not available for extraction from their electronic reporting systems and was therefore not reported to the survey. Superior court information for Prince Edward Island was unavailable until 2018/2019.
3. A case is one or more charges against an accused person or company, which were processed by the courts at the same time (date of offence, date of initiation, date of first appearance, or date of decision), and received a final decision. The definition attempts to reflect court processing. All data have been processed using this case definition. The case definition changed for the 2006/2007 release of data. The former definition (used in releases prior to October 2007) combined all charges against the same person disposed of in court on the same day into a case. Consequently, comparisons should not be made with data tables and reports released before that time.
4. Cases are counted according to the fiscal year in which they are completed. Each year, the Integrated Criminal Court Survey (ICCS) database is considered final at the end of March for the production of court statistics pertaining to the preceding fiscal year. These counts do not include cases that were pending a final decision at the end of the reference period. If a final decision is reached in the next fiscal year, then these cases are included in the completed case counts for that fiscal year. However, if a one-year period of inactivity elapses, then these cases are deemed complete and the originally published counts for the previous fiscal year are subsequently updated and reported in the next year's release of the data. Historically, updates to a previous year's counts have resulted in an increase of about 2%.

5. A case that has more than one charge is represented by the charge with the "most serious offence" (MSO). The most serious offence is selected using the following rules. First, court decisions are considered and the charge with the "most serious decision" (MSD) is selected. Court decisions for each charge in a case are ranked from most to least serious as follows: (1) guilty, (2) guilty of a lesser offence, (3) acquitted, (4) stay of proceeding, (5) withdrawn, dismissed or discharged, (6) not criminally responsible, (7) other, and (8) transfer of court jurisdiction. Second, in cases where two or more charges result in the same MSD (for example, guilty), Criminal Code sanctions are considered. The charge with the most serious offence type is selected according to an offence seriousness scale, based on actual sentences handed down by courts in Canada (The offence seriousness scale is calculated using data from both the adult and youth components of the Integrated Criminal Court Survey). Each offence type is ranked by looking at (1) the proportion of guilty charges where custody was imposed and (2) the average (mean) length of custody for the specific type of offence. These values are multiplied together to arrive at the final seriousness ranking for each type of offence. If, after looking at the offence seriousness scale, two or more charges remain tied then information about the sentence type and duration of the sentence are considered (for example, custody and length of custody, then probation and length of probation, etcetera).

6. Guilty findings include guilty of the charged offence, of an included offence, of an attempt of the charged offence, or of an attempt of an included offence. This category also includes guilty pleas, and cases where an absolute or conditional discharge has been imposed.

7. In this table, a prohibition order refers to a prohibition, seizure, or forfeiture order. A court may make any order of prohibition, seizure or forfeiture that may be imposed under any Act of Parliament or any regulation made under it if an accused is found guilty or convicted of that offence, other than an order under section 161 of the *Criminal Code*.

Appendix 13

Additional Statistics from Canada, Updated February 18th, 2021

Table 1
Police-reported crime for select non-violent offences, Canada, 2015 to 2019

Type of offence	2015		2016		2017		2018		2019		Change in rate 2015 to 2019
	number	rate	number	rate	number	rate	number	rate	number	rate	percent
Total property crime	1,153,700	3,231.4	1,169,445	3,238.6	1,193,319	3,265.5	1,241,083	3,349.0	1,319,562	3,510.5	8.6
Theft											
Theft over \$5,000	11,081	31.0	10,897	30.2	12,391	33.9	14,795	39.9	15,863	42.2	36.0
Theft over \$5,000 from a motor vehicle	3,867	10.8	4,057	11.2	4,325	11.8	4,643	12.5	4,785	12.7	17.5
Shoplifting over \$5,000	496	1.4	574	1.6	549	1.5	666	1.8	709	1.9	35.8
Motor Vehicle Theft	78,800	220.7	79,055	218.9	85,115	232.9	86,192	232.6	87,066	231.6	4.9
Theft \$5,000 or under	210,685	590.1	207,373	574.3	209,446	573.1	214,484	578.8	226,468	602.5	2.1
Theft \$5,000 or under from a motor vehicle	176,584	494.6	186,655	516.9	187,426	512.9	193,083	521.0	197,971	526.7	6.5
Shoplifting \$5,000 or under	99,907	279.8	102,948	285.1	108,313	296.4	124,896	337.0	140,286	373.2	33.4
Possession/trafficking stolen goods											
Traffic stolen goods over \$5,000 (incl intent)	307	0.9	319	0.9	378	1.0	349	0.9	397	1.1	22.8
Possession of stolen goods over \$5,000	7,262	20.3	8,092	22.4	11,062	30.3	11,199	30.2	11,051	29.4	44.5
Traffic stolen goods under \$5,000 (incl intent)	410	1.1	528	1.5	531	1.5	540	1.5	741	2.0	71.7
Possession of stolen goods \$5,000 or under	11,976	33.5	11,567	32.0	12,215	33.4	12,257	33.1	13,562	36.1	7.6
Fraud											
Fraud	94,425	264.5	109,630	303.6	113,166	309.7	130,008	350.8	142,140	378.1	43.0
Identity theft	2,541	7.1	3,136	8.7	3,295	9.0	3,815	10.3	4,683	12.5	75.0
Identity fraud	11,894	33.3	14,033	38.9	14,344	39.3	15,848	42.8	19,664	52.3	57.0
Mischief											
Altering/removing/destroying Vehicle Identification Number (VIN)	105	0.3	118	0.3	85	0.2	101	0.3	115	0.3	4.0
Gaming and betting											
Betting house	1	0.0	2	0.0			2	0.0	8	0.0	659.9
Gaming house	53	0.1	37	0.1	20	0.1	69	0.2	24	0.1	-57.0
Other violations related to gaming and betting	67	0.2	81	0.2	47	0.1	65	0.2	82	0.2	16.2
Common bawdy house (to keep, to transport a person to) ^{1,2}	18	0.1	11	0.0	17	0.0	20	0.1	16	0.0	-15.6
Offensive weapons											
Weapons trafficking	106	0.3	83	0.2	103	0.3	115	0.3	159	0.4	42.5
Unauthorized importing or exporting of weapons	81	0.2	39	0.1	59	0.2	28	0.1	56	0.1	-34.3
Other Criminal Code violations											
Counterfeiting	675	1.9	805	2.2	939	2.6	1,088	2.9	1,152	3.1	62.1
Other offences against the administration of law and justice (Part IV CC) ³	7,552	21.2	7,615	21.1	7,601	20.8	7,667	20.7	8,518	22.7	7.1
Offences against rights of property (Part IX CC)	1,565	4.4	1,661	4.6	1,576	4.3	1,864	5.0	2,002	5.3	21.5
Fraudulent transactions relating to contracts and trade (Part X CC)	241	0.7	210	0.6	188	0.5	167	0.5	165	0.4	-35.0
Wilful and forbidden acts in respect of certain property (Part XI CC)	2,036	5.7	1,944	5.4	2,095	5.7	1,939	5.2	2,677	7.1	24.9
Offences relating to currency (Part XII CC)	53	0.1	35	0.1	92	0.3	95	0.3	101	0.3	81.0
Money laundering, proceeds of crime (Part XII.2 CC)	248	0.7	237	0.7	328	0.9	232	0.6	249	0.7	-4.6
Attempts, conspiracies, accessories (Part XIII CC)	237	0.7	243	0.7	250	0.7	237	0.6	258	0.7	3.4
Other federal statute violations											
Bankruptcy Act	32	0.1	21	0.1	13	0.0	35	0.1	12	0.0	-64.4
Income Tax Act	16	0.0	10	0.0	8	0.0	8	0.0	13	0.0	-22.8
Canada Shipping Act	3,634	10.2	3,999	11.1	3,559	9.7	3,881	10.5	3,456	9.2	-9.7
Customs Act	554	1.6	1,140	3.2	9,716	26.6	9,276	25.0	8,562	22.8	1367.9
Competition Act	1	0.0	1	0.0	4	0.0	12	0.0	1	0.0	-5.0
Excise Act ³	315	0.9	277	0.8	215	0.6	218	0.6	217	0.6	-34.6
Human trafficking	91	0.3	102	0.3	103	0.3	117	0.3	170	0.5	77.4
Human smuggling fewer than 10 persons	20	0.1	11	0.0	17	0.0	10	0.0	18	0.0	-14.5
Human smuggling 10 persons or more	3	0.0	1	0.0	4	0.0	0	0.0	3	0.0	-5.0
Firearms Act	1,229	3.4	1,201	3.3	1,215	3.3	892	2.4	1,065	2.8	-17.7

1. Bill C-36 came into effect in December 2014. The new legislation targets "the exploitation that is inherent in prostitution and the risks of violence posed to those who engage in it" (Criminal Code Chapter 25, preamble). New violations classified as "Commodification of sexual activity" under "violations against the person" include: the purchasing of sexual services or communicating for that purpose, receiving a material benefit deriving from the purchase of sexual services, procuring of persons for the purpose of prostitution, and advertising sexual services offered for sale. In addition, a number of other offences related to prostitution continue to be considered non-violent offences and are classified under "Other Criminal Code offences". These include communicating to provide sexual services for consideration, and; stopping or impeding traffic for the purpose of offering, providing or obtaining sexual services for consideration. At the same time, the survey was amended to classify the violations codes of Parent or guardian procuring sexual activity, and Householder permitting prohibited sexual activity under "violations against the person". The following violations officially expired on December 5, 2014: bawdy house, living off the avails of prostitution of a person under 18, procuring, obtains/communicates with a person under 18 for purpose of sex, and other prostitution. Police services are able to utilize these codes as their Records Management Systems are updated to allow it. As a result, these data should be interpreted with caution.

2. Effective December 2014, Bill C-36 amended the definition of the term "common bawdy house" in the Criminal Code to remove reference to prostitution. As a result of this amendment, the Uniform Crime Reporting Survey (UCR) violation of "Bawdy house" was terminated, and the new violation of "Common bawdy house" was introduced. Police services are able to utilize this amendment as their Records Management Systems are updated to allow it. As a result, these data should be interpreted with caution.

3. On April 10, 2015, Bill C-10 Tackling Contraband Tobacco Act came into effect. As a result, this law created the Criminal Code offence of trafficking in contraband tobacco which is counted under the violation "Offences against the administration of law and justice". Prior to April 2015, the offence was counted under "Excise Act". As such, comparisons of these two violations to previous years should be made with caution.

Note: Data reflect criminal incidents that have been substantiated through investigation by Canadian police services. The offences which comprise the category of money laundering in the Uniform Crime Reporting Survey (UCR) include: laundering proceeds of crime (CCC s.462.31) and restraint order violation (CCC s.462.33).

Source: Statistics Canada, Canadian Centre for Justice and Community Safety Statistics, Uniform Crime Reporting Survey, Aggregate Database.

Table 2
Police-reported crime for select non-violent offences, by province and territory, 2019

Type of offence	Canada		Newfoundland and Labrador		Prince Edward Island		Nova Scotia		New Brunswick		Quebec		Ontario		Manitoba		Saskatchewan		Alberta		British Columbia		Yukon		Northwest Territories		Nunavut	
	number	rate	number	rate	number	rate	number	rate	number	rate	number	rate	number	rate	number	rate	number	rate	number	rate	number	rate	number	rate	number	rate	number	rate
Total property crime	1,319,662	3,616.6	16,497	3,163.1	4,892	3,180.7	27,648	2,846.3	25,619	3,297.4	145,859	1,720.2	387,468	3,669.7	84,881	6,196.1	76,063	6,476.4	256,216	6,861.3	279,330	6,336.6	4,669	11,161.7	11,292	26,196.7	7,821	20,435.6
Theft																												
Theft over \$5,000	15,863	42.2	154	29.5	24	15.3	217	22.3	273	35.1	2,074	24.4	4,666	32.0	398	29.1	538	45.8	3,410	78.0	4,049	79.8	37	90.6	17	37.9	6	15.5
Theft over \$5,000 from a motor vehicle	4,785	12.7	23	4.4	5	3.2	73	7.6	35	4.5	1,007	11.9	1,203	8.3	107	7.8	123	10.5	1,017	23.3	1,188	23.4	3	7.3	1	2.2	0	0.0
Shoplifting over \$5,000	709	1.9	45	8.6	1	0.6	6	0.6	6	0.8	92	1.1	247	1.7	35	2.6	21	1.8	137	3.1	109	2.1	2	4.9	8	17.8	0	0.0
Motor vehicle theft	87,066	231.6	434	83.2	142	90.5	927	95.4	1,464	188.5	11,961	141.0	23,962	164.7	5,546	405.0	5,284	449.9	23,535	538.4	13,352	263.3	142	347.6	179	399.3	108	278.5
Theft \$5,000 or under	226,468	602.5	2,537	486.4	911	593.2	6,113	635.2	4,763	615.7	25,998	306.4	88,018	604.2	9,933	725.3	11,332	964.9	30,689	702.1	42,379	935.7	698	1,708.5	816	1,820.4	241	621.5
Theft \$5,000 or under from a motor vehicle	197,971	526.7	761	145.9	910	579.8	2,605	268.2	2,120	272.9	15,528	183.0	53,243	365.5	10,414	760.4	7,145	608.4	43,061	985.1	61,862	1,220.2	197	482.2	100	223.1	5	12.9
Shoplifting \$5,000 or under	140,286	373.2	1,534	294.1	321	204.5	1,051	108.2	1,599	205.8	12,482	147.1	49,616	340.6	9,432	688.7	4,487	382.0	30,376	694.9	29,952	570.9	246	602.1	125	278.9	65	167.6
Possession/trafficking stolen goods																												
Traffic stolen goods over \$5,000 (incl intent)	397	1.1	1	0.2	1	0.6	2	0.2	4	0.5	54	0.6	102	0.7	3	0.2	20	1.7	203	4.6	6	0.1	1	2.4	0	0.0	0	0.0
Possession of stolen goods over \$5,000	11,051	29.4	37	7.1	26	16.6	61	6.3	186	23.9	542	6.4	2,176	14.9	610	44.5	955	81.3	5,236	119.8	1,195	23.6	12	29.4	11	24.5	4	10.3
Traffic stolen goods under \$5,000 (incl intent)	741	2.0	0	0.0	0	0.0	10	1.0	18	2.3	120	1.4	94	0.6	6	0.4	38	3.2	414	9.5	37	0.7	0	0.0	4	8.9	0	0.0
Possession of stolen goods \$5,000 or under	13,562	36.1	52	10.0	76	48.4	191	19.7	270	34.8	896	10.6	2,462	16.9	711	51.9	773	65.8	4,021	92.0	4,057	80.0	28	68.5	16	35.7	8	23.2
Fraud																												
Fraud	142,140	378.1	1,574	301.8	578	368.3	3,988	410.5	3,241	417.2	16,617	216.4	55,842	383.4	5,717	417.5	5,861	498.0	23,375	534.7	22,816	449.9	251	614.4	211	470.7	69	177.9
Identity theft	4,683	12.5	51	9.8	9	5.7	90	9.3	88	11.3	2,028	23.9	710	4.9	164	12.0	127	10.8	807	19.8	538	10.6	7	17.1	2	4.5	2	5.2
Identity fraud	19,664	52.3	61	11.7	28	17.8	198	20.4	207	26.6	5,816	68.5	5,880	40.4	348	25.3	680	57.9	2,580	59.0	3,851	75.9	5	12.2	8	17.8	4	10.3
Mischief																												
Altering/moving/destroying Vehicle Identification Number (VIN)	115	0.3	0	0.0	0	0.0	0	0.0	1	0.1	48	0.6	9	0.1	0	0.0	5	0.4	51	1.2	1	0.0	0	0.0	0	0.0	0	0.0
Gaming and betting																												
Betting house	8	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	8	0.1	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0
Gaming house	24	0.1	1	0.2	2	1.3	0	0.0	0	0.0	1	0.0	12	0.1	0	0.0	4	0.3	1	0.0	2	0.0	0	0.0	1	2.2	0	0.0
Other violations related to gaming and betting	82	0.2	5	1.0	0	0.0	2	0.2	16	2.1	1	0.0	25	0.2	0	0.0	5	0.4	8	0.2	17	0.3	0	0.0	3	6.7	0	0.0
Common bawdy house (to keep, to transport a person to) ^{1,2}	16	0.0	0	0.0	0	0.0	2	0.2	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	1	0.0	13	0.3	0	0.0	0	0.0	0	0.0
Offensive weapons																												
Weapons trafficking	159	0.4	0	0.0	0	0.0	2	0.2	5	0.6	21	0.2	42	0.3	14	1.0	22	1.9	31	0.7	21	0.4	1	2.4	0	0.0	0	0.0
Unauthorized importing or exporting of weapons	56	0.1	2	0.4	0	0.0	0	0.0	0	0.0	1	0.1	13	0.2	6	0.4	4	0.3	0	0.0	8	0.2	0	0.0	0	0.0	0	0.0
Other Criminal Code violations																												
Counterfeiting	1,152	3.1	19	3.6	11	7.0	19	2.0	80	10.3	192	2.3	374	2.6	17	1.2	84	7.2	196	4.5	154	3.0	4	9.8	1	2.2	1	2.6
Other offences against the administration of law and justice (Part IV CC)	8,518	22.7	121	23.2	51	32.5	192	19.8	133	17.1	1,003	11.8	1,892	13.0	1,095	80.0	314	26.7	2,146	49.1	1,271	25.1	75	183.6	136	303.4	89	229.5
Offences against rights of property (Part IX CC)	2,002	5.3	8	1.5	5	3.2	9	0.9	24	3.1	102	1.2	515	3.5	84	6.1	88	7.5	490	11.2	673	13.3	2	4.9	2	4.5	0	0.0
Fraudulent transactions relating to contracts and trade (Part X CC)	165	0.4	1	0.2	0	0.0	10	1.0	9	1.2	55	0.6	50	0.3	1	0.1	6	0.5	22	0.5	11	0.2	0	0.0	0	0.0	0	0.0
Willful and forbidden acts in respect of certain property (Part XI CC)	2,877	7.1	51	9.8	11	7.0	91	9.4	38	4.9	326	3.8	556	3.8	117	8.5	161	13.7	531	12.1	722	14.2	14	34.3	28	62.5	31	79.9
Offences relating to currency (Part XII CC)	101	0.3	0	0.0	0	0.0	1	0.1	12	0.3	46	0.5	12	0.1	2	0.1	11	0.9	5	0.1	21	0.4	0	0.0	0	0.0	0	0.0
Money laundering, proceeds of crime (Part XIII.2 CC)	249	0.7	4	0.8	3	1.9	12	1.2	0	0.0	72	0.8	47	0.3	9	0.7	10	0.9	46	1.1	40	0.8	0	0.0	4	8.9	2	5.2
Attempts, conspiracies, accessories (Part XIII CC)	258	0.7	3	0.6	2	1.3	3	0.3	17	2.2	108	1.3	104	0.7	3	0.2	5	0.4	9	0.2	4	0.1	0	0.0	0	0.0	0	0.0
Other federal statute violations																												
Bankruptcy Act	12	0.0	0	0.0	0	0.0	1	0.1	0	0.0	1	0.0	4	0.0	1	0.1	0	0.0	3	0.1	2	0.0	0	0.0	0	0.0	0	0.0
Income Tax Act	13	0.0	2	0.4	0	0.0	0	0.0	2	0.3	3	0.0	2	0.0	0	0.0	0	0.0	2	0.0	2	0.0	0	0.0	0	0.0	0	0.0
Canada Shipping Act	3,456	9.2	1	0.2	3	1.9	5	0.5	6	0.8	58	0.7	1,337	8.2	58	4.2	9	0.8	10	0.2	1,969	38.8	0	0.0	0	0.0	0	0.0
Customs Act	6,562	22.8	10	1.9	0	0.0	2	0.2	6	1.0	8,291	97.7	38	0.2	116	8.5	24	2.0	32	0.7	69	1.0	1	2.4	0	0.0	0	0.0
Competition Act	1	0.0	0	0.0	0	0.0	0	0.0	1	0.1	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0
Excise Act	217	0.6	29	5.6	3	1.9	20	2.1	47	6.1	27	0.3	54	0.4	8	0.6	14	1.2	5	0.1	9	0.2	0	0.0	0	0.0	0	0.0
Human trafficking	170	0.5	0	0.0	0	0.0	15	1.5	3	0.4	3	0.0	129	0.9	0	0.0	7	0.6	10	0.2	3	0.1	0	0.0	0	0.0	0	0.0
Human smuggling fewer than 10 persons	18	0.0	0	0.0	0	0.0	0	0.0	1	0.1	7	0.1	8	0.1	0	0.0	0	0.0	0	0.0	2	0.0	0	0.0	0	0.0	0	0.0
Human smuggling 10 persons or more	3	0.0	0	0.0	0	0.0	0	0.0	0	0.0	1	0.0	2	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0
Firearms Act	1,095	2.9	69	11.5	8	5.1	20	2.1	24	3.1	34	0.4	67	0.5	51	3.7	40	3.4	371	8.5	347	6.8	21	51.4	19	42.4	3	7.7

1. Bill C-56 came into effect in December 2014. The new legislation targets "the exploitation that is inherent in prostitution and the risks of violence posed to those who engage in it" (Criminal Code Chapter 26, preamble). New violations classified as "Communication of sexual activity" under "Violations against the person" include: the purchasing of sexual services or communicating for that purpose, receiving a material benefit deriving from the purchase of sexual services, procuring or persons for the purpose of prostitution, and advertising sexual services offered for sale. In addition, a number of other offences related to prostitution continue to be considered non-violent offences and are classified under "Other Criminal Code offences." These include communicating to provide sexual services for consideration, and; stopping or impeding traffic for the purpose of offering, providing or obtaining sexual services for consideration. At the same time, the survey was amended to classify the violations codes of Parent or guardian procuring sexual activity, and Household member permitting prohibited sexual activity under "Violations against the person". The following violations officially reported on December 5, 2014: bawdy house, keeping off the avails of prostitution of a person under 18, procuring, obtaining, communicating with a person under 18 for purpose of sex, and other prostitution. Police services are able to utilize these codes as their Records Management Systems are updated to allow it. As a result, these data should be interpreted with caution.

2. Effective December 2014, Bill C-56 amended the definition of the term "common bawdy house" in the Criminal Code to remove reference to prostitution. As a result of this amendment, the Uniform Crime Reporting Survey (UCR) violation of "Bawdy house" was terminated, and the new violation of "Common bawdy house" was introduced. Police services are able to utilize this amendment as their Records Management Systems are updated to allow it. As a result, these data should be interpreted with caution.

Note: Data reflect criminal incidents that have been substantiated through investigation by Canadian police services. The offences which comprise the category of money laundering in the Uniform Crime Reporting Survey (UCR) include: laundering proceeds of crime (CCC s.462.31) and restraint order violation (CCC s.462.33).

Source: Statistics Canada, Canadian Centre for Justice and Community Safety Statistics, Uniform Crime Reporting Survey, Aggregate Database.

Table 3
Police-reported incidents of money laundering - proceeds of crime (Part XII.2 CC), Canada, 2008 to 2019

Statistics	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Actual incidents	452	520	405	379	291	number 263	276	248	237	328	232	249
Rate per 100,000 population	1.4	1.5	1.2	1.1	0.8	rate 0.7	0.8	0.7	0.7	0.9	0.6	0.7
Percentage change in rate	-10.6	13.7	-23.0	-7.3	-24.0	percent -10.6	3.9	-10.8	-5.5	36.8	-30.3	5.81
Total cleared	119	117	129	150	103	number 117	90	82	76	58	31	57
Cleared by charge ¹	51	53	46	82	72	86	58	63	50	40	21	43
Cleared otherwise ²	68	64	83	68	31	31	32	19	26	18	10	14
Total persons charged	62	55	54	60	59	number 81	66	80	69	52	22	40
Total adults charged	61	55	54	60	55	76	66	76	68	52	22	36
Total youth charged	1	0	0	0	4	5	0	4	1	0	0	4

1. At least one accused has been identified and there is a criminal charge laid or recommended to be laid against this individual in connection with this criminal incident.

2. An accused has been identified by police in relation to the criminal incident, and there is sufficient evidence to lay a charge, however a charge is not laid by police and the accused is processed by other means.

Examples of charges cleared otherwise include warnings, cautions, alternative measures, extrajudicial sanctions and instances where the accused has died.

Note: Data reflect criminal incidents that have been substantiated through investigation by Canadian police services. The offences which comprise the category of money laundering in the Uniform Crime Reporting Survey (UCR) include: laundering proceeds of crime (CCC s.462.31) and restraint order violation (CCC s.462.33).

Source: Statistics Canada, Canadian Centre for Justice and Community Safety Statistics, Uniform Crime Reporting Survey, Aggregate Database.

Table 4
Police-reported incidents of money laundering - proceeds of crime (Part XII.2 CC), by province and territory, 2019

Statistics	Canada	Newfoundland and Labrador	Prince Edward Island	Nova Scotia	New Brunswick	Quebec	Ontario	Manitoba	Saskatchewan	Alberta	British Columbia	Yukon	Northwest Territories	Nunavut
Actual incidents	249	4	3	12	0	72	number 47	9	10	46	40	0	4	2
Rate per 100,000 population	0.7	0.8	1.9	1.2	0.0	0.8	rate 0.3	0.7	0.9	1.1	0.8	0.0	8.9	5.2
Total cleared	57	1	0	1	1	20	number 18	4	6	4	2	0	0	0
Cleared by charge ¹	43	0	0	1	0	14	16	4	6	0	2	0	0	0
Cleared otherwise ²	14	1	0	0	1	6	2	0	0	4	0	0	0	0
Total cleared	22.9	25.0	0.0	8.3	...	27.8	percent 38.3	44.4	60.0	8.7	5.0	...	0.0	0.0
Cleared by charge ¹	17.3	0.0	0.0	8.3	...	19.4	34.0	44.4	60.0	0.0	5.0	...	0.0	0.0
Cleared otherwise ²	5.6	25.0	0.0	0.0	...	8.3	4.3	0.0	0.0	8.7	0.0	...	0.0	0.0
Total persons charged	40	0	0	1	0	12	number 15	3	7	0	2	0	0	0
Total adults charged	36	0	0	1	0	11	15	3	4	0	2	0	0	0
Total youth charged	4	0	0	0	0	0	0	0	3	0	0	0	0	0

... not applicable

1. At least one accused has been identified and there is a criminal charge laid or recommended to be laid against this individual in connection with this criminal incident.

2. An accused has been identified by police in relation to the criminal incident, and there is sufficient evidence to lay a charge, however a charge is not laid by police and the accused is processed by other means. Examples of charges cleared otherwise include warnings, cautions, alternative measures, extrajudicial sanctions and instances where the accused has died.

Note: Data reflect criminal incidents that have been substantiated through investigation by Canadian police services. The offences which comprise the category of money laundering in the Uniform Crime Reporting Survey include: laundering proceeds of crime (CCC s.462.31) and restraint order violation (CCC s.462.33).

Source: Statistics Canada, Canadian Centre for Justice and Community Safety Statistics, Uniform Crime Reporting Survey, Aggregate Database.

Table 5
Police-reported incidents involving money laundering - proceeds of crime (Part XII.2 CC), Canada, 2009 to 2019

	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
	number										
Number of police reported incidents that include money laundering	750	684	716	596	604	633	574	495	653	507	474
Number of police reported incidents where the most serious violation is money laundering	514	395	373	284	261	275	245	233	321	229	240
Number of police reported incidents that include money laundering but the most serious violation is not money laundering	236	289	343	312	343	358	329	262	332	278	234
Other most common violations in incidents that include money laundering	number										
Money laundering, proceeds of crime (Part XII.2 CC)	750	684	716	596	604	633	574	495	653	507	474
Cocaine - trafficking	74	84	90	120	139	146	96	76	106	82	73
Fraud ¹	37	61	111	81	95	89	115	89	114	93	80
Cannabis - trafficking (pre-legalization) ²	57	78	69	76	62	54	52	34	46	36	0
Fail to comply with order ³	23	33	49	61	77	63	56	47	43	27	28
Cannabis - possession (pre-legalization) ²	42	56	50	44	71	41	36	27	40	26	0
Other Controlled Drugs and Substances Act - trafficking	32	42	26	23	28	47	53	44	55	28	32
Possession of weapons	20	10	16	27	20	52	38	28	39	41	19
Possess stolen property ^{4,5}	78	100	68	22	13	1	1	0	0	0	1
Possession of stolen goods \$5,000 or under ^{4,5}	33	28	47	35	30	33	25	22	22
Possession of stolen goods over \$5,000 ^{4,5}	14	23	11	43	48	32	29	37	32
Breach of probation ³	19	23	42	33	32	24	27	16	21	16	9
Cocaine - possession	30	20	27	32	35	15	27	18	15	10	11
Methamphetamines (crystal meth) - trafficking	5	4	2	8	7	15	16	31	52	46	29
Other Controlled Drugs and Substances Act - possession	12	14	23	29	30	20	11	21	14	8	7
Weapons possession contrary to order	3	2	3	7	9	15	14	11	12	19	6
Attempts, conspiracies, accessories (Part XIII CC)	8	10	12	10	14	8	7	7	10	5	4
Other most common violations in incidents that include money laundering	percent										
Money laundering, proceeds of crime (Part XII.2 CC)	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0
Cocaine - trafficking	9.9	12.3	12.6	20.1	23.0	23.1	16.7	15.4	16.2	16.2	15.4
Fraud ¹	4.9	8.9	15.5	13.6	15.7	14.1	20.0	18.0	17.5	18.3	16.9
Cannabis - trafficking (pre-legalization) ²	7.6	11.4	9.6	12.8	10.3	8.5	9.1	6.9	7.0	7.1	0.0
Fail to comply with order ³	3.1	4.8	6.8	10.2	12.7	10.0	9.8	9.5	6.6	5.3	5.9
Cannabis - possession (pre-legalization) ²	5.6	8.2	7.0	7.4	11.8	6.5	6.3	5.5	6.1	5.1	0.0
Other Controlled Drugs and Substances Act - trafficking	4.3	6.1	3.6	3.9	4.6	7.4	9.2	8.9	8.4	5.5	6.8
Possession of weapons	2.7	1.5	2.2	4.5	3.3	8.2	6.6	5.7	6.0	8.1	4.0
Possess stolen property ^{4,5}	10.4	14.6	9.5	3.7	2.2	0.2	0.2	0.0	0.0	0.0	0.2
Possession of stolen goods \$5,000 or under ^{4,5}	4.6	4.7	7.8	5.5	5.2	6.7	3.8	4.3	4.6
Possession of stolen goods over \$5,000 ^{4,5}	2.0	3.9	1.8	6.8	8.4	6.5	4.4	7.3	6.8
Breach of probation ³	2.5	3.4	5.9	5.5	5.3	3.8	4.7	3.2	3.2	3.2	1.9
Cocaine - possession	4	2.9	3.8	5.4	5.8	2.4	4.7	3.6	2.3	2.0	2.3
Methamphetamines (crystal meth) - trafficking	0.7	0.6	0.3	1.3	1.2	2.4	2.8	6.3	8.0	9.1	6.1
Other Controlled Drugs and Substances Act - possession	1.6	2.0	3.2	4.9	5.0	3.2	1.9	4.2	2.1	1.6	1.5
Weapons possession contrary to order	0.4	0.3	0.4	1.2	1.5	2.4	2.4	2.2	1.8	3.7	1.3
Attempts, conspiracies, accessories (Part XIII CC)	1.1	1.5	1.7	1.7	2.3	1.3	1.2	1.4	1.5	1.0	0.8

... Data not available

1. In January 2010, the Uniform Crime Reporting Survey (UCR) was modified to create new violation codes for identity fraud and identity theft. Prior to 2010, those offences would have been coded as fraud.

2. On October 17, 2018, Bill C-45 "An Act respecting cannabis and to amend the Controlled Drugs and Substances Act, the Criminal Code and other Acts" came into effect. As a result, all prior pre-legalization cannabis-related legislation under the Controlled Drugs and Substances Act (CDSA) has been expired and replaced with 22 new violation codes under the Cannabis Act.

3. Coming into effect on July 17th, 2015, Bill C-26 increased the maximum penalties for certain sexual offences against children, including failure to comply with orders and probation conditions relating to sexual offences against children. In the Uniform Crime Reporting Survey (UCR), the most serious violation is partially determined by the maximum penalty. As such, changes in maximum penalty may affect the most serious violation in an incident reported by police. Police services are able to utilize these amendments as their Records Management Systems are updated to allow them.

4. The offence possess stolen property expired April 28, 2011 and was replaced with the offences possession of stolen goods \$5,000 or under and possession of stolen goods over \$5,000.

5. In April 2011, legislation came into effect making it an offence to traffic in property obtained by crime, including possession with intent to traffic property obtained by crime. In addition to creating new Uniform Crime Reporting Survey (UCR) violation codes to capture these offences, the existing UCR violation code pertaining to possession of stolen property was modified. The UCR now separates possession of stolen property into possession of stolen property under \$5,000 and possession of stolen property over \$5,000 in order to be more in line with the Criminal Code of Canada. As a result of this change, a number of incidents of possession of stolen property under \$5,000 are now being reported as secondary offences when they occur in conjunction with more serious offences, leading to a decrease in the number of possession of stolen property incidents reported in 2011.

Note: Data reflect criminal incidents that have been substantiated through investigation by Canadian police services. The offences which comprise the category of money laundering in the Uniform Crime Reporting Survey (UCR) include: laundering proceeds of crime (CCC s.462.31) and restraint order violation (CCC s.462.33). The Uniform Crime Reporting Survey (UCR) captures up to four violations for each incident. Information on associated violations and persons accused of police-reported crimes are drawn from the Incident-based Uniform Crime Reporting Survey which, as of 2009, covered 99% of the population of Canada.

Source: Statistics Canada, Canadian Centre for Justice and Community Safety Statistics, Uniform Crime Reporting Survey, Trend Database.

Table 6

Accused identified in relation to police-reported incidents of money laundering - proceeds of crime (Part XII.2 CC), Canada, 2009 to 2019

	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
	number										
Number of police reported incidents where the most serious violation is money laundering	514	395	373	284	261	275	245	233	321	229	240
Total number of accused	138	134	152	133	154	98	109	88	77	50	69
Gender ¹	number										
female	22	23	25	30	31	12	26	11	19	15	10
male	116	111	127	103	123	85	83	76	57	35	58
Gender ¹	percent										
female	15.9	17.2	16.4	22.6	20.1	12.4	23.9	12.6	25.0	30.0	14.7
male	84.1	82.8	83.6	77.4	79.9	87.6	76.1	87.4	75.0	70.0	85.3
Age ²	number										
12 to 17	1	2	3	3	5	0	4	1	2	0	7
18 to 24	30	29	26	34	22	25	24	23	17	13	9
25 to 34	43	35	60	44	70	39	33	32	29	24	22
35 to 44	33	29	26	22	32	19	29	12	18	9	17
45 to 54	14	27	29	25	23	7	13	14	8	1	8
55 and older	17	12	8	5	2	8	5	6	2	2	6
Age ²	percent										
12 to 17	0.7	1.5	2.0	2.3	3.2	0.0	3.7	1.1	2.6	0.0	10.1
18 to 24	21.7	21.6	17.1	25.6	14.3	25.5	22.2	26.1	22.4	26.5	13.0
25 to 34	31.2	26.1	39.5	33.1	45.5	39.8	30.6	36.4	38.2	49.0	31.9
35 to 44	23.9	21.6	17.1	16.5	20.8	19.4	26.9	13.6	23.7	18.4	24.6
45 to 54	10.1	20.1	19.1	18.8	14.9	7.1	12.0	15.9	10.5	2.0	11.6
55 and older	12.3	9.0	5.3	3.8	1.3	8.2	4.6	6.8	2.6	4.1	8.7

1. Excludes accused where the gender was unknown or invalid. Given that small counts of victims and accused persons identified as "gender diverse" may exist, the aggregate Uniform Crime Reporting Survey (UCR) data available to the public has been recoded to assign these counts to either "male" or "female", in order to ensure the protection of confidentiality and privacy. Victims and accused persons identified as gender diverse have been assigned to either male or female based on the regional distribution of victims' or accused persons' gender.

2. Accused refers to those aged 12 to 89 years. Children under 12 years of age cannot be prosecuted for criminal activities. Excludes accused with an unknown or invalid age.

Note: Data reflect criminal incidents that have been substantiated through investigation by Canadian police services. The offences which comprise the category of money laundering in the Uniform Crime Reporting Survey (UCR) include: laundering proceeds of crime (CCC s.462.31) and restraint order violation (CCC s.462.33). The Uniform Crime Reporting Survey (UCR) captures up to four violations for each incident. Information on associated violations and persons accused of police-reported crimes are drawn from the Incident-based Uniform Crime Reporting Survey which, as of 2009, covered 99% of the population of Canada.

Source: Statistics Canada, Canadian Centre for Justice and Community Safety Statistics, Uniform Crime Reporting Survey, Trend Database.

Table 7

Accused identified in relation to police-reported incidents involving money laundering - proceeds of crime (Part XII.2 CC), Canada, 2009 to 2019

	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Number of police reported incidents that include money laundering	750	684	716	596	604	633	574	495	653	507	474
Total number of accused	548	602	727	701	800	716	650	563	597	525	426
Gender ¹											
female	96	130	151	168	200	162	155	141	162	152	109
male	452	471	576	532	600	549	495	421	433	370	316
Gender ¹											
female	17.5	21.6	20.8	24.0	25.0	22.8	23.8	25.1	27.2	29.1	25.6
male	82.5	78.4	79.2	76.0	75.0	77.2	76.2	74.9	72.8	70.9	74.4
Age ²											
12 to 17	23	33	19	30	26	32	24	5	12	17	21
18 to 24	177	182	183	198	225	201	155	167	146	126	79
25 to 34	163	164	277	237	282	258	229	192	243	217	144
35 to 44	107	108	116	114	147	117	134	111	121	103	102
45 to 54	46	80	103	93	96	71	78	55	50	35	40
55 and older	32	35	29	29	24	34	29	33	23	26	40
Age ²											
12 to 17	4.2	5.5	2.6	4.3	3.3	4.5	3.7	0.9	2.0	3.2	4.9
18 to 24	32.3	30.2	25.2	28.2	28.1	28.2	23.9	29.7	24.5	24.0	18.5
25 to 34	29.7	27.2	38.1	33.8	35.3	36.2	35.3	34.1	40.8	41.4	33.8
35 to 44	19.5	17.9	16.0	16.3	18.4	16.4	20.6	19.7	20.3	19.7	23.9
45 to 54	8.4	13.3	14.2	13.3	12.0	10.0	12.0	9.8	8.4	6.7	9.4
55 and older	5.8	5.8	4.0	4.1	3.0	4.8	4.5	5.9	3.9	5.0	9.4

1. Excludes accused where the gender was unknown or invalid. Given that small counts of victims and accused persons identified as "gender diverse" may exist, the aggregate Uniform Crime Reporting Survey (UCR) data available to the public has been recoded to assign these counts to either "male" or "female", in order to ensure the protection of confidentiality and privacy. Victims and accused persons identified as gender diverse have been assigned to either male or female based on the regional distribution of victims' or accused persons' gender.

2. Accused refers to those aged 12 to 89 years. Children under 12 years of age cannot be prosecuted for criminal activities. Excludes accused with an unknown or invalid age.

Note: Data reflect criminal incidents that have been substantiated through investigation by Canadian police services. The offences which comprise the category of money laundering in the Uniform Crime Reporting Survey (UCR) include: laundering proceeds of crime (CCC s.462.31) and restraint order violation (CCC s.462.33). The Uniform Crime Reporting Survey (UCR) captures up to four violations for each incident. Information on associated violations and persons accused of police-reported crimes are drawn from the Incident-based Uniform Crime Reporting Survey which, as of 2009, covered 99% of the population of Canada.

Source: Statistics Canada, Canadian Centre for Justice and Community Safety Statistics, Uniform Crime Reporting Survey, Trend Database.

Appendix 14

Additional Statistics on Money Laundering Cases 2008-2018

Table 6. Results of Single Charge ML Cases

Decision	2008/2009	2009/2010	2010/2011	2011/2012	2012/2013	2013/2014	2014/2015	2015/2016	2016/2017	2017/2018	2018/2019	Total	%
Guilty	0	2	2	4	3	1	1	1	1	1	0	16	26.7
Acquitted	0	0	0	0	0	1	0	0	0	0	0	1	1.7
Stay / Withdrawn	3	2	5	7	3	3	4	3	3	2	3	37	61.7
Other	0	0	0	1	0	2	1	2	0	0	0	6	10
Total	3	4	7	12	6	7	6	6	3	3	3	60	100

Source: Statistics Canada, Canadian Centre for Justice and Community Safety Statistics, Integrated Criminal Court Survey.

Notes:

1. This product is based on data from the adult component of the Integrated Criminal Court Survey (ICCS). The ICCS is administered by the Canadian Centre for Justice Statistics (Statistics Canada) in collaboration with provincial and territorial government departments responsible for criminal courts in Canada. The survey collects statistical information on adult and youth court cases involving Criminal Code and other federal statute offences. Data contained in this table represent the adult criminal court portion of the survey, namely, individuals who were 18 years of age or older at the time of the offence. Data are based on a fiscal year (April 1 through March 31).
2. A case is one or more charges against an accused person or company, which were processed by the courts at the same time (date of offence, date of initiation, date of first appearance, or date of decision), and received a final decision. The definition attempts to reflect court processing. All data have been processed using this case definition. The case definition changed for the 2006/2007 release of data. The former definition (used in releases prior to October 2007) combined all charges against the same person disposed of in court on the same day into a case. Consequently, comparisons should not be made with data tables and reports released before that time.
3. Cases are counted in the fiscal year in which they are completed. Every year, the Integrated Criminal Court Survey (ICCS) database is considered final at the end of March for the production of court statistics for the previous fiscal year. These counts do not include cases pending an outcome at the end of the reference period. If an outcome is reached in the next fiscal year, these cases are included in the completed case counts for that fiscal year. However, cases that are inactive for one year are deemed complete and the originally published counts for the previous fiscal year are updated and reported in the next fiscal year's data release.
4. A case that has more than one charge is represented by the charge with the "most serious offence" (MSO). The most serious offence is selected using the following rules. First, court decisions are considered and the charge with the "most serious decision" (MSD) is selected. Court decisions for each charge in a case are ranked from most to least serious as follows: (1) guilty, (2) guilty of a lesser offence, (3) acquitted, (4) stay of proceeding, (5) withdrawn, dismissed or discharged, (6) not criminally responsible, (7) other, and (8) transfer of court jurisdiction. Second, in cases where two or more charges result in the same MSD (for example, guilty), Criminal Code sanctions are considered. The charge with the most serious offence type is selected according to an offence seriousness scale, based on actual sentences handed down by courts in Canada (The offence seriousness scale is calculated using data from both the adult and youth components of the Integrated Criminal Court Survey). Each offence type is ranked by looking at (1) the proportion of guilty charges where custody was imposed and (2) the average (mean) length of custody for the specific type of offence. These values are multiplied together to arrive at the final seriousness ranking for each type of offence. If, after looking at the offence seriousness scale, two or more charges remain tied then information about the sentence type and duration of the sentence are considered (for example, custody and length of custody, then probation and length of probation, etcetera).
5. As of 2005/2006, all provincial and territorial courts in 10 provinces and 3 territories reported to the survey. Information from superior courts in Ontario, Manitoba and Saskatchewan as well as municipal courts in Quebec was not available for extraction from their electronic reporting systems and was therefore not reported to the survey. Superior court information for Prince Edward Island was unavailable until 2018/2019.
6. Guilty findings include guilty of the charged offence, of an included offence, of an attempt of the charged offence, or of an attempt of an included offence. This category also includes guilty pleas, and cases where an absolute or conditional discharge has been imposed.
7. Stayed/withdrawn includes includes stays, withdrawals, dismissals and discharges at preliminary inquiry as well as court referrals to alternative or extrajudicial measures and restorative justice programs. These decisions all refer to the court stopping criminal proceedings against the accused.
8. Other decisions include waived out of province or territory. This category also includes any order where a guilty decision was not recorded, the court's acceptance of a special plea, cases which raise Charter arguments and cases where the accused was found unfit to stand trial.
9. Money laundering is defined as *Criminal Code* section 462.31, RSC 1985.

Table 8. Results of ML-Related Cases

Decision	2008/2009	2009/2010	2010/2011	2011/2012	2012/2013	2013/2014	2014/2015	2015/2016	2016/2017	2017/2018	2018/2019	Total	%
Guilty	71	82	108	140	136	153	145	121	134	130	85	1305	57.5
Acquitted	0	2	0	0	4	6	5	10	4	3	4	38	1.7
Stay / Withdrawn	72	57	75	89	90	88	55	88	101	102	58	875	38.5
Other	3	0	0	12	4	5	4	10	7	6	1	52	2.3
Total	146	141	183	241	234	252	209	229	246	241	148	2270	100

Source: Statistics Canada, Canadian Centre for Justice and Community Safety Statistics, Integrated Criminal Court Survey.

Notes:

1. This product is based on data from the adult component of the Integrated Criminal Court Survey (ICCS). The ICCS is administered by the Canadian Centre for Justice Statistics (Statistics Canada) in collaboration with provincial and territorial government departments responsible for criminal courts in Canada. The survey collects statistical information on adult and youth court cases involving Criminal Code and other federal statute offences. Data contained in this table represent the adult criminal court portion of the survey, namely, individuals who were 18 years of age or older at the time of the offence. Data are based on a fiscal year (April 1 through March 31).
2. A case is one or more charges against an accused person or company, which were processed by the courts at the same time (date of offence, date of initiation, date of first appearance, or date of decision), and received a final decision. The definition attempts to reflect court processing. All data have been processed using this case definition. The case definition changed for the 2006/2007 release of data. The former definition (used in releases prior to October 2007) combined all charges against the same person disposed of in court on the same day into a case. Consequently, comparisons should not be made with data tables and reports released before that time.
3. Cases are counted in the fiscal year in which they are completed. Every year, the Integrated Criminal Court Survey (ICCS) database is considered final at the end of March for the production of court statistics for the previous fiscal year. These counts do not include cases pending an outcome at the end of the reference period. If an outcome is reached in the next fiscal year, these cases are included in the completed case counts for that fiscal year. However, cases that are inactive for one year are deemed complete and the originally published counts for the previous fiscal year are updated and reported in the next fiscal year's data release.
4. A case that has more than one charge is represented by the charge with the "most serious offence" (MSO). The most serious offence is selected using the following rules. First, court decisions are considered and the charge with the "most serious decision" (MSD) is selected. Court decisions for each charge in a case are ranked from most to least serious as follows: (1) guilty, (2) guilty of a lesser offence, (3) acquitted, (4) stay of proceeding, (5) withdrawn, dismissed or discharged, (6) not criminally responsible, (7) other, and (8) transfer of court jurisdiction. Second, in cases where two or more charges result in the same MSD (for example, guilty), Criminal Code sanctions are considered. The charge with the most serious offence type is selected according to an offence seriousness scale, based on actual sentences handed down by courts in Canada (The offence seriousness scale is calculated using data from both the adult and youth components of the Integrated Criminal Court Survey). Each offence type is ranked by looking at (1) the proportion of guilty charges where custody was imposed and (2) the average (mean) length of custody for the specific type of offence. These values are multiplied together to arrive at the final seriousness ranking for each type of offence. If, after looking at the offence seriousness scale, two or more charges remain tied then information about the sentence type and duration of the sentence are considered (for example, custody and length of custody, then probation and length of probation, etcetera).
5. As of 2005/2006, all provincial and territorial courts in 10 provinces and 3 territories reported to the survey. Information from superior courts in Ontario, Manitoba and Saskatchewan as well as municipal courts in Quebec was not available for extraction from their electronic reporting systems and was therefore not reported to the survey. Superior court information for Prince Edward Island was unavailable until 2018/2019.
6. Guilty findings include guilty of the charged offence, of an included offence, of an attempt of the charged offence, or of an attempt of an included offence. This category also includes guilty pleas, and cases where an absolute or conditional discharge has been imposed.
7. Stayed/withdrawn includes includes stays, withdrawals, dismissals and discharges at preliminary inquiry as well as court referrals to alternative or extrajudicial measures and restorative justice programs. These decisions all refer to the court stopping criminal proceedings against the accused.
8. Other decisions include waived out of province or territory. This category also includes any order where a guilty decision was not recorded, the court's acceptance of a special plea, cases which raise Charter arguments and cases where the accused was found unfit to stand trial.
9. Money laundering is defined as *Criminal Code* section 462.31, RSC 1985.

Table 9. Results of ML-Charges

Decision	2008/2009	2009/2010	2010/2011	2011/2012	2012/2013	2013/2014	2014/2015	2015/2016	2016/2017	2017/2018	2018/2019	Total	%
Guilty	53	38	21	35	31	47	43	38	31	40	21	398	10.1
Acquitted	0	5	1	8	6	7	13	12	6	3	6	67	1.7
Stay / Withdrawn	195	149	216	510	372	348	345	307	375	383	184	3384	85.7
Other	4	2	2	14	7	8	5	12	13	24	7	98	2.5
Total	252	194	240	567	416	410	406	369	425	450	218	3947	100

Source: Statistics Canada, Canadian Centre for Justice and Community Safety Statistics, Integrated Criminal Court Survey.

Notes:

1. This product is based on data from the adult component of the Integrated Criminal Court Survey (ICCS). The ICCS is administered by the Canadian Centre for Justice Statistics (Statistics Canada) in collaboration with provincial and territorial government departments responsible for criminal courts in Canada. The survey collects statistical information on adult and youth court cases involving Criminal Code and other federal statute offences. Data contained in this table represent the adult criminal court portion of the survey, namely, individuals who were 18 years of age or older at the time of the offence. Data are based on a fiscal year (April 1 through March 31).

2. A charge refers to a formal accusation against an accused person or company involving a federal statute offence that has been processed by the courts and received a final decision. A charge is considered to be completed under any of the following conditions: the accused is acquitted or found guilty and sentenced (if applicable); the accused is found unfit to stand trial; the charge is stayed, withdrawn, dismissed, or discharged at preliminary hearing; the charge has been waived out of the province or territory.

3. As of 2005/2006, all provincial and territorial courts in 10 provinces and 3 territories reported to the survey. Information from superior courts in Ontario, Manitoba and Saskatchewan as well as municipal courts in Quebec was not available for extraction from their electronic reporting systems and was therefore not reported to the survey. Superior court information for Prince Edward Island was unavailable until 2018/2019.

4. Guilty findings include guilty of the charged offence, of an included offence, of an attempt of the charged offence, or of an attempt of an included offence. This category also includes guilty pleas, and cases where an absolute or conditional discharge has been imposed.

5. Stayed/withdrawn includes includes stays, withdrawals, dismissals and discharges at preliminary inquiry as well as court referrals to alternative or extrajudicial measures and restorative justice programs. These decisions all refer to the court stopping criminal proceedings against the accused.

6. Other decisions include waived out of province or territory. This category also includes any order where a guilty decision was not recorded, the court's acceptance of a special plea, cases which raise Charter arguments and cases where the accused was found unfit to stand trial.

7. Money laundering is defined as *Criminal Code* section 462.31, RSC 1985.

Table 12. Sanctions in ML Cases Where ML was the Most Serious Offense, from 2008 to 2018

	2008/2009	2009/2010	2010/2011	2011/2012	2012/2013	2013/2014	2014/2015	2015/2016	2016/2017	2017/2018	2018/2019	Total	%
Custodial Sentence Total	17	19	8	15	18	21	17	15	9	10	8	157	55.1
Less than 1 year	7	9	2	9	6	11	4	8	4	2	2	64	22.5
One year to less than two years	8	8	3	3	7	6	7	5	2	3	2	54	18.9
Two years or more	2	2	3	3	5	4	6	2	3	5	4	39	13.7
Other sentence	8	10	7	12	11	19	13	11	14	14	9	128	44.9
Total	25	29	15	27	29	40	30	26	23	24	17	285	100

Source: Statistics Canada, Canadian Centre for Justice and Community Safety Statistics, Integrated Criminal Court Survey.

Notes:

1. This product is based on data from the adult component of the Integrated Criminal Court Survey (ICCS). The ICCS is administered by the Canadian Centre for Justice Statistics (Statistics Canada) in collaboration with provincial and territorial government departments responsible for criminal courts in Canada. The survey collects statistical information on adult and youth court cases involving Criminal Code and other federal statute offences. Data contained in this table represent the adult criminal court portion of the survey, namely, individuals who were 18 years of age or older at the time of the offence. Data are based on a fiscal year (April 1 through March 31).

2. A case is one or more charges against an accused person or company, which were processed by the courts at the same time (date of offence, date of initiation, date of first appearance, or date of decision), and received a final decision. The definition attempts to reflect court processing. All data have been processed using this case definition. The case definition changed for the 2006/2007 release of data. The former definition (used in releases prior to October 2007) combined all charges against the same person disposed of in court on the same day into a case. Consequently, comparisons should not be made with data tables and reports released before that time.

3. Cases are counted in the fiscal year in which they are completed. Every year, the Integrated Criminal Court Survey (ICCS) database is considered final at the end of March for the production of court statistics for the previous fiscal year. These counts do not include cases pending an outcome at the end of the reference period. If an outcome is reached in the next fiscal year, these cases are included in the completed case counts for that fiscal year. However, cases that are inactive for one year are deemed complete and the originally published counts for the previous fiscal year are updated and reported in the next fiscal year's data release.

4. A case that has more than one charge is represented by the charge with the "most serious offence" (MSO). The most serious offence is selected using the following rules. First, court decisions are considered and the charge with the "most serious decision" (MSD) is selected. Court decisions for each charge in a case are ranked from most to least serious as follows: (1) guilty, (2) guilty of a lesser offence, (3) acquitted, (4) stay of proceeding, (5) withdrawn, dismissed or discharged, (6) not criminally responsible, (7) other, and (8) transfer of court jurisdiction. Second, in cases where two or more charges result in the same MSD (for example, guilty), Criminal Code sanctions are considered. The charge with the most serious offence type is selected according to an offence seriousness scale, based on actual sentences handed down by courts in Canada (The offence seriousness scale is calculated using data from both the adult and youth components of the Integrated Criminal Court Survey). Each offence type is ranked by looking at (1) the proportion of guilty charges where custody was imposed and (2) the average (mean) length of custody for the specific type of offence. These values are multiplied together to arrive at the final seriousness ranking for each type of offence. If, after looking at the offence seriousness scale, two or more charges remain tied then information about the sentence type and duration of the sentence are considered (for example, custody and length of custody, then probation and length of probation, etcetera).

5. As of 2005/2006, all provincial and territorial courts in 10 provinces and 3 territories reported to the survey. Information from superior courts in Ontario, Manitoba and Saskatchewan as well as municipal courts in Quebec was not available for extraction from their electronic reporting systems and was therefore not reported to the survey. Superior court information for Prince Edward Island was unavailable until 2018/2019.

6. Guilty findings include guilty of the charged offence, of an included offence, of an attempt of the charged offence, or of an attempt of an included offence. This category also includes guilty pleas, and cases where an absolute or conditional discharge has been imposed.

7. Other sentences include absolute and conditional sentence, probation, fine, conditional discharge, suspended sentence, community service order and prohibition order among others.

8. Custodial sentence lengths are intended to reflect the amount of time remaining to be served on a custodial sentence after credit has been awarded for time spent in pre-sentence custody. However, in some jurisdictions, the length of custody information represents the total length of custody imposed by court.

9. Length of custody data are not available from Manitoba.

10. Money laundering is defined as *Criminal Code* section 462.31, RSC 1985.

Appendix 15

CAN-001812 – FINTRAC Report to the Minister of Finance on
Compliance and Related Activities – Sept 30, 2020



Financial Transactions and
Reports Analysis Centre
of Canada

Centre d'analyse des opérations
et déclarations financières
du Canada

PROTECTED B

FINTRAC Report to the Minister of Finance on Compliance and Related Activities

September 30, 2020

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY	2
II. ABOUT FINTRAC AND ITS COMPLIANCE PROGRAM.....	4
III. COMPLIANCE ACTIVITY HIGHLIGHTS FOR 2019–20.....	5
A) Enhancing Regulatory Transparency	5
B) Assistance and Engagement Activities.....	5
1. Engaging on the Implementation of June 2019 Regulatory Amendments	6
2. Increasing Awareness of Money Laundering and Terrorist Financing Risks Through Engagement with High-Risk Sectors	7
3. Strengthening current MOUs and Establishing New Ones	9
4. Engagement with Other Reporting Entity Sectors and Domestic and International Stakeholders	10
C) Assessment Activities.....	12
1. New Developments in the Compliance Program	12
2. Examination Findings by Key Sectors	13
3. Results of Follow-up Examinations in All Sectors	24
4. Third Party Analysis of Suspicious Transaction Reports (STRs)	25
D) Enforcement Activities	26
1. Update on AMPs Review and AMPs Activity	26
2. Public Naming – Legislative Requirement	26
3. Non-compliance Disclosures to Law Enforcement.....	26
4. Voluntary Self-declaration of Non-compliance (VSDONC).....	27
IV. FINTRAC’s CONTRIBUTION TO IMPROVING THE EFFECTIVENESS OF CANADA’s AML/ATF EFFORTS.....	27
A) Development and Implementation of Regulatory Amendments	27
B) Update on 2018 Parliamentary Review	28
C) Contribution to Canada’s National Inherent ML/TF Risk Assessment	28
D) Strategic Analysis of Canada-Linked Illicit Finance Dynamics	29
E) Engagements with the Department of Finance Canada and Other Government of Canada initiatives	30
F) Engagement with Financial Action task Force (FATF)	30
G) FINTRAC Contributions to the Commission of Inquiry into Money Laundering in British Columbia	30
V. UPCOMING COMPLIANCE PRIORITIES	31
VI. SUPPORT FOR REPORTING ENTITIES DURING the COVID-19 PANDEMIC	32
VII. CONCLUSION.....	33

I. EXECUTIVE SUMMARY

An essential part of FINTRAC's mandate is to work with Canadian businesses to ensure compliance with the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA or the Act). Compliance with the Act helps prevent and deter criminals from using Canada's economy to launder the proceeds of their crimes or to finance terrorist activities. This report highlights the principal activities and initiatives that FINTRAC carried out in 2019–20 in pursuit of this mandate under the three main pillars of its Compliance Framework, namely, Assistance (including transparency and engagement activities); Assessment, and Enforcement. The report also underscores FINTRAC's ongoing efforts to improve the effectiveness of Canada's anti-money laundering and anti-terrorist financing (AML/ATF) regime and points to the Centre's upcoming compliance priorities for 2020–21.

Over the course of fiscal year 2019–20, FINTRAC continued to build on its major initiatives from previous fiscal years. For example, the Centre added to its transparency initiative by publishing new administrative monetary penalty (AMP) harm guides and updates to its Assessment Manual. FINTRAC remains committed to ensuring that reporting entities (RE) clearly understand their requirements under the Act and associated Regulations, as well as to what they should expect from FINTRAC in the areas of assistance, assessment and enforcement.

This year's Report also introduces FINTRAC's new five-year Compliance Engagement Strategy, which is comprised of four priorities, as described in this report. These four priorities guided FINTRAC's engagement activities over the last fiscal year, with a particular emphasis put on working with industry and other government stakeholders towards the implementation of the regulatory amendments that are coming into force in 2021.

As this report highlights, FINTRAC continues to engage directly and specifically with sectors that face higher risk of exploitation for the purposes of money laundering or terrorist financing. In December 2019, FINTRAC engaged closely with the casino sector during its second Casino Forum. During the Forum, compliance and law enforcement approaches were discussed, as were common challenges faced by this sector, and upcoming legislative changes. Other examples of engagement include those with provincial governments, regulatory bodies and industry associations in the real estate sector to ensure money laundering and terrorist financing risks are well understood and properly mitigated, and to ensure that relevant transaction reports are submitted to FINTRAC.

FINTRAC continues to contribute to the Federal-Provincial-Territorial Working Group on Beneficial Ownership, and continuously seeks opportunities to strengthen operational relationships with other regulators through memorandum of understanding (MOU) negotiations.

FINTRAC also participated in general engagement activities across all business sectors subject to the PCMLTFA, as well as with Canadian regulators, industry associations, and

foreign counterparts. Some highlights include the 6th Annual Major Reporters Forum (which includes the participation of Canada's major financial institutions, contributions to the Commission of Inquiry into Money Laundering in British Columbia (known as the Cullen Commission), and participation in the Wolfsberg Forum.

Fiscal year 2019–20 saw many changes to FINTRAC's assessment activities. The most important continues to be the work towards the transition from the Office of the Superintendent of Financial Institutions (OSFI) to FINTRAC in assuming full responsibility for the supervision of Federally Regulated Financial Institutions (FRFIs) for AML/ATF compliance. With 2019–20 being the first year in a two-year transition, FINTRAC and OSFI undertook numerous activities to ensure the smooth transition of AML/ATF supervision of FRFIs. In addition, FINTRAC also continued to improve its compliance officer training. On April 1, 2021, FINTRAC will be the sole AML/ATF regulator for FRFI supervision.

The report presents key examination findings across RE sectors including casinos, banks, money services businesses (MSBs), and real estate. Trends, challenges and case examples in each of these sectors are also provided.

As part of the final pillar of FINTRAC's Compliance Framework, the report also covers FINTRAC's enforcement activities for non-compliance. With the AMP program review officially complete, FINTRAC has begun to issue notices of violation again in 2019–20. This fiscal year, FINTRAC issued two penalties applying the new calculation methodology. FINTRAC also implemented the new legislative requirement, as of June 20, 2019, requiring that all AMPs imposed by the Centre after that date be made public as soon as feasible. The Centre also provided seven non-compliance disclosures (NCDs) to law enforcement and witnessed an increase in interest among these partners to pursue non-compliance investigations and charges.

II. ABOUT FINTRAC AND ITS COMPLIANCE PROGRAM

As Canada's financial intelligence unit and AML/ATF regulator, FINTRAC helps to combat money laundering, terrorist activity financing and threats to the security of Canada.

The Centre produces actionable financial intelligence in support of investigations of Canada's police, law enforcement and national security agencies in relation to these threats. FINTRAC also generates valuable strategic financial intelligence, including specialized research reports and trends analysis, for regime partners and policy decision-makers, businesses and international counterparts. This strategic financial intelligence shines a light on the nature, scope and threat posed by money laundering and terrorism financing.

The Centre is able to fulfill its financial intelligence mandate by working with Canadian businesses to ensure compliance with the PCMLTFA (the Act) and associated Regulations. Compliance with this Act helps to prevent and deter criminals from using Canada's economy to launder the proceeds of their crimes or to finance terrorist activities. It also ensures the Centre receives the information that it needs to produce financial intelligence for Canada's police, law enforcement and national security agencies.

Overall, FINTRAC had a budget of over \$55 million in fiscal year 2019–20 to support achieving its mandate. The Centre had a total of 352 Full-Time Equivalents (FTEs) in 2019–20. A sizeable fraction of these resources is dedicated to supporting and advancing FINTRAC's role of ensuring regulatory compliance with the PCMLTFA.

In the 2019–20 fiscal year, the compliance sector had 85 FTEs and a budget of \$8,273,687.¹ The sector is comprised of regional compliance officers involved in conducting examinations through the three FINTRAC regional offices located in Vancouver, Toronto and Montréal. The regional offices are also responsible for providing assistance to reporting entities and maintaining key relationships with other regulators and industry associations. Last fiscal year, the regional offices comprised a total of 43 FTEs, and a budget of \$3,846,370.

Divided among three unit functions, the headquarters (HQ) in Ottawa had 42 FTEs and a budget of \$4,427,317. HQ is responsible for, among other activities, coordinating the strategic and operational initiatives of the compliance program and providing national leadership for regional operations, as well as providing assistance to reporting entities, managing the MSB registry, providing policy interpretations, administering FINTRAC's AMP and Non-Compliance Disclosures programs, and maintaining compliance MOUs with external regime partners.

RC6

s.21(1)(a)

¹ The FTE count and budget figures in this report represent resources specifically allocated for compliance activities and do not cover internal services in support of those activities. The FTE count does not include students.

III. COMPLIANCE ACTIVITY HIGHLIGHTS FOR 2019–20

A) Enhancing Regulatory Transparency

FINTRAC continued its significant efforts to enhance the transparency of its Compliance Program in 2019–20. Building on the publication of its Compliance Framework and Assessment Manual, FINTRAC updated and published its AMP policy and harm guides, which were highly anticipated and well received by REs. The Government of Canada's Community of Federal Regulators (CFR) recognized all of the above work as a particularly exemplary effort by presenting the Centre with the 2019 Award for Excellence in Regulatory Openness and Transparency.

Publication of AMP Harm Guides

In August 2019, the Centre completed the final stage of the AMP program review. This resulted in the publication of seven user guides that describe FINTRAC's approach to assessing the harm done by the 200 violations prescribed in the *Proceeds of Crime (Money Laundering) and Terrorist Financing Administrative Monetary Penalties Regulations*, and clearly explain the methodology used in determining the corresponding penalty amounts. This publication marks the completion of the review of FINTRAC's AMP program that was initiated following two federal court decisions² on past AMP cases.

Updates to the Assessment Manual

In addition to the publication of the AMP harm guides in summer 2019, FINTRAC continued to provide updates to the publicly available Assessment Manual, including changes made to reflect upcoming regulatory amendments and to align with other FINTRAC publications. FINTRAC will release the updated version of the manual in fiscal year 2020–21 in plain language and in an accessible format on its website, as well as distribute it to industry associations representing reporting entity sectors. Extensive outreach and engagement have taken place to share the new compliance assessment methodology with REs, which is now clearly communicated on FINTRAC's website to foster compliance.

B) Assistance and Engagement Activities

As part of FINTRAC's priority to cultivate strategic relationships with key external stakeholders, the Centre is committed to working closely with them when drafting guidance material that have the most impact on REs. Assistance is the first pillar of FINTRAC's Compliance Framework and involves not only the assistance provided through the proactive publication of guidance, but also active engagement with stakeholders in Canada's AML/ATF regime. FINTRAC's Compliance sector engages with REs, industry associations, provincial

² *Canada v. Kabul Farms Inc.* 2016 FCA 143 and *Max Realty Solutions Ltd. v. Canada* 2016 FC 620

regulators, and other Canadian government departments through conferences, forums, training, presentations, meetings, and teleconferences.

This past fiscal year marks the beginning of FINTRAC's five-year Compliance Engagement Strategy. The Strategy was completed in the fall of 2019 and sets priorities for FINTRAC's engagement activities until 2024.

This section of the report will provide progress updates on each of the Engagement Strategy priorities:

1. Work closely with existing and new REs, industry associations and other federal/provincial/territorial regulators to effectively implement regulatory amendments published in June 2019.
2. Enhance the understanding and compliance of the real estate and casino sectors with their PCMLTFA obligations through new and innovative approaches in collaboration with the Government of British Columbia, provincial regulators, industry associations and REs in the real estate and casino sectors.
3. Assess and strengthen relationships with current domestic and international MOU partners, as well as establish new ones.
4. Continue to engage with all RE sectors and other stakeholders through different forums and approaches in support of the Compliance Program pillars.

1. Engaging on the Implementation of June 2019 Regulatory Amendments

Engagement on Guidance and Information Technology (IT) Systems Changes

FINTRAC makes effective use of many methods to engage with REs on changes made to the PCMLTFA and its regulations. Examples of how FINTRAC works closely with REs on implementing regulatory changes and consults them on draft guidance are provided below. In addition, FINTRAC proactively publishes policy interpretations (PIs) on its website to clarify obligations under the PCMLTFA.

The FINTRAC Reporting Working Group (FRWG) was launched in February 2019 to work closely with REs on all matters pertaining to reporting, including in relation to the implementation of regulatory amendments published in July 2019. For example, the FRWG serves to seek feedback from REs on the implementation of amendments affecting FINTRAC's reporting forms, as well as IT systems of both FINTRAC and REs. A sub-group of virtual currency-MSBs created under the FRWG is used to seek input and feedback regarding the new Large Virtual Currency Transaction Report.

FINTRAC also chairs the Guidance and Policy Interpretation Working Group (GPIWG), which is a sub-committee of the Advisory Committee on Money Laundering and Terrorist Financing (ACMLTF) with representation across all reporting entity sectors. The GPIWG is the main forum used to consult all RE sectors on draft guidance documents that explain to

REs the new regulatory requirements and FINTRAC's expectations. The feedback received from GPIWG members contributes to better clarity and awareness of the final published guidance for REs. For example, in November 2019 and following extensive consultations with businesses, FINTRAC published updated guidance respecting methods to verify the identity of an individual and confirm the existence of a corporation or an entity other than a corporation. The updated guidance reflects amendments to the regulations that came into force in June 2019, and the feedback received from Canadian businesses. The change allows for the use of new technologies to verify identity and authenticate documents, which provides more flexibility for business activities to take place online.

In addition to the engagement with members of the FRWG and GPIWG, FINTRAC holds meetings with the Canadian Bankers Association (CBA) and its members on a regular basis to discuss challenges relating to the implementation of the regulatory amendments and to find collective solutions. Given their interest and resources, CBA members are typically providing the preponderance of detailed feedback that FINTRAC receives and it has assisted the Centre in making better-informed decisions, in particular in regards to the approach to making changes to reporting systems.

Policy Interpretations (PIs)

In 2019–20, FINTRAC developed and published 357 PIs to help REs fulfill PCMLTFA obligations and better understand legislative and regulatory amendments. PIs were issued on a broad range of topics in relation to the Regulations currently in force and the amendments to the Regulations coming into force on June 1, 2020 and June 1, 2021. PI discussions on these issues were brought to the ACMLTF, the FRWG, the Virtual Currency (VC) Dealers Working Group, and the GPIWG.

In advance of the publication of the regulatory amendments in July 2019, FINTRAC reviewed the policy interpretations published on its website. FINTRAC undertook this exercise to revise or remove PIs that would contain outdated legislative or regulatory references, as well as to remove PIs that would be incorrect when regulatory amendments came into force. Recognizing that REs regularly use the published PIs, a document indicating which PIs would be edited and which would be removed, along with the reason for removal was provided to REs through the GPIWG. This exercise provided REs with the opportunity to understand the rationale behind FINTRAC's decisions, as well as to plan accordingly and either revise any internal materials or processes that referred to a published PI; or retain, in their own holdings, copies of PIs that would no longer be available once removed from FINTRAC's website.

2. Increasing Awareness of Money Laundering and Terrorist Financing Risks Through Engagement with High-Risk Sectors

Casino Forum

FINTRAC hosted its second Casino Forum in December 2019, which was well received by industry representatives. A large majority of those invited participated in the forum, and

discussion topics included compliance and law enforcement approaches, common challenges experienced in this sector, and upcoming legislative changes. REs have since expressed interest in recurring casino forum events in the future. The 2019 Casino Forum was also the venue for the official launch of the newest Public-Private Partnership (PPP) in which FINTRAC is participating and its associated operational alert. This PPP, named Project Athena, focuses on combatting the laundering of proceeds of crime through casino-related underground banking schemes.

In addition, this was the first time that FINTRAC invited the Chief Anti-Money Laundering Officers (CAMLOs) of B8³ financial entities to discuss crosscutting issues for REs in the casino sector and the banking industry. The banks appreciated the opportunity to connect with CAMLOs of the large lottery corporations and recommended that the approach be considered for future casino forums.

FINTRAC received very positive feedback for the Forum, as attested by the following two quotes from the participants, which perfectly sum up the overall feedback received:

- “Great conference very informative and great chance to network with colleagues. Great atmosphere and venue. Topics covered were very relevant to today’s world. Look forward to the next one.”
- “I found the forum to be very informative. I liked that it was only for the casino sector, so each jurisdiction was able to get ideas of what could be done differently or share ideas on how our compliance program is run.”

Other Engagement in the Casino Sector

FINTRAC’s Vancouver Office participated in a panel discussion at the June 2019 Canadian Gaming Summit, which was attended by over 120 participants from the casino sector. In addition, the Vancouver Office participated in meetings with the Gaming Policy and Enforcement Branch of British Columbia, a FINTRAC MOU partner, to discuss how to implement recommendations from Peter German’s review of money laundering in Lower Mainland casinos. FINTRAC also provided its views on proposed BC legislative changes. In addition, compliance officers met with the British Columbia Lottery Corporation (BCLC) a number of times to discuss ongoing compliance observations, strategies and sector trends.

Engagement with Real Estate Sector

FINTRAC performed extensive engagement with the real estate sector in 2019–20 including working with provincial governments, regulatory bodies and industry associations. Through assistance and engagement activities, the Centre aims to increase the understanding of REs in

³ The B8 consist of the National Bank of Canada, Caisses Populaires and the Fédération des Caisses Desjardins du Québec, Royal Bank of Canada, HSBC Bank Canada, the Canadian Imperial Bank of Commerce, the Bank of Montreal, the Bank of Nova Scotia, and Toronto Dominion Bank.

mitigating their money laundering and terrorist financing (ML/TF) risks relevant to the real estate sector and of their AML/ATF obligations. In 2019-20, FINTRAC participated in numerous working group meetings and forums across the country to enhance awareness of real estate sector ML/TF activities and trends. The following examples illustrate the outreach conducted by FINTRAC in the real estate sector.

The Centre is a member of the BC-Government of Canada Working Group on Real Estate and has contributed to this group's work by delivering presentations, identifying ML and compliance challenges affecting this sector, and defining key issues that require attention as the AML/ATF regime moves towards identifying policy options to address gaps.

FINTRAC also contributed to the Real Estate Council of British Columbia's (RECBC) development of AML/ATF training modules for new registrants, which were launched in January 2020. Furthermore, FINTRAC held in-person meetings and teleconferences with RECBC to discuss FINTRAC's examination processes, provided an overview of AML/ATF requirements under the PCMLTFA and associated Regulations, and shared the Centre's compliance examination findings of entities also regulated by RECBC. Conversely, RECBC shared its list of real estate entities, which greatly assisted FINTRAC in identifying the current RE population in the BC real estate sector.

Similarly, FINTRAC's engagement with the Real Estate Council of Ontario (RECO) contributed to the development of AML/ATF training of new registrants and ongoing learning for real estate agents in Ontario. RECO training modules were launched in December 2019.

RC6

s.21(1)(c)

At the national level, FINTRAC engaged with the Canadian Real Estate Association (CREA), and in August 2019, provided a presentation to CREA's Committee for Federal Affairs, with representation from all Canadian provinces. The presentation highlighted FINTRAC's Transparency Initiative, including the Assessment Manual published on FINTRAC's website, as well as changes to the AMP program and public naming policy.

Other activities with real estate regulators included a presentation by the Vancouver Office at the June 2019 Conference of Real Estate Regulators of Canada, and the recording of a 20-minute FINTRAC podcast, which was published by the Alberta Real Estate Association with other podcasts by industry representatives.

3. Strengthening current MOUs and Establishing New Ones

In 2019-20, FINTRAC made significant progress on several regulatory MOUs with various organizations at both the provincial and national levels. These MOUs help foster stronger relationships between FINTRAC and stakeholders across sectors of the economy that are subject to the Act and at risk for money laundering and terrorist financing. MOUs help FINTRAC fulfill its mandate by formalizing relationships that allow industry organizations to

share compliance-related data and information with the Centre. Access to this information helps FINTRAC in its AML/ATF mandate and further integrates the financial sector in the fight against financial crime.

As an example, FINTRAC's Compliance sector worked closely with the Investment Industry Regulatory Organization of Canada (IIROC) to revise its MOU. FINTRAC signed the revised MOU on May 13, 2019 that provides a framework within which the Centre and IIROC can share compliance-related information. This MOU strengthens the compliance of Canada's securities dealer sector with the PCMLTFA, and helps to enhance FINTRAC and IIROC's awareness of new and evolving trends within the Canadian securities sector.

RC6

s.21(1)(c)

4. Engagement with Other Reporting Entity Sectors and Domestic and International Stakeholders

In 2019–20, FINTRAC participated in a total of 166 engagement events with various stakeholders including 123 events divided as follows: 35 conferences/symposiums/forums, 31 teleconferences and 57 meetings/correspondence with MOU partners or other government departments. For example, FINTRAC provided presentations at conferences such as the Canadian Institute Regulatory Compliance Conference in November 2019 and seminars organized by the Canadian MSB Association in May and November 2019. The presentations focused on helping REs and other relevant stakeholders better understand current obligations and regulatory amendments published in the summer of 2019.

In addition, FINTRAC's three regional offices conducted another 43 proactive engagement activities with Canada's largest financial institutions in relation to examinations, follow-ups and reports monitoring.

Engagement with the Banking Sector

FINTRAC continued to engage with the B5⁴, who are responsible for over 90% of all reports received by FINTRAC. This fiscal year, the Centre logged in at least 46 instances where it provided assistance to these banks on matters involving policy interpretations, technical support and feedback related to financial transaction reporting. FINTRAC's engagement tracking tool for monitoring interactions with these entities was optimized only mid-way through fiscal 2019–20 (June 2019); as such, the number of instances where assistance was provided to this group is likely far higher. In addition, FINTRAC held its 6th annual Major

⁴ The B5 consist of the Royal Bank of Canada, The Bank of Montreal, Canadian Imperial Bank of Commerce, The Bank of Nova Scotia, and TD Canada Trust.

Reporters Forum on February 11, 2020. The Forum brought together representatives from the eight major reporters, various FINTRAC functions, and the Department of Finance Canada. The Forum served to further enhance the transparency and strategic direction of FINTRAC's Compliance Program. Participants provided valuable feedback and insight, which will lay the foundation for future collaborative work.

Agenda items at the Forum included the following:

- FINTRAC's assessment approach, reporting statistics, compliance examination trends, future expectations and way forward.
- Updates on the implementation of regulatory amendments published in July 2019.
- Updates on current PPP projects and the proposed Public-Private Collaboration Steering Committee.
- Discussions on best practices and challenges experienced by major reporters.

In addition, brainstorming sessions were held for the first time at this Forum, which focused on how to further improve the effectiveness of the AML/ATF regime by reducing the regulatory burden, piloting technology, and investing in skills development in the workforce of REs and at FINTRAC.

Wolfsberg Forum and the International Supervisory Forum

FINTRAC participated in the Wolfsberg Forum from May 22-24, 2019. The main theme for the forum was Financial Crime Compliance. FINTRAC's Director and CEO, Nada Semaan, was one of the speakers at the opening panel of the forum titled, "Unlocking Effectiveness: Modernizing the Fight against Financial Crime". In her opening remarks, she focused on

- Canada's approach to combatting money laundering and terrorist activity financing;
- FINTRAC's commitment to working collaboratively with regulatory partners, Canadian businesses, and Canada's law enforcement and national security agencies; and
- the results that FINTRAC has achieved through strategic information sharing, particularly in relation to our project-based, public-private sector partnerships.

Overall, the discussions at the forum were extremely productive and relevant to FINTRAC and the Director's remarks were very well received by the forum attendees.

Also at the international level, FINTRAC promoted its supervisory program amongst the Five Eyes community, regularly participating in the International Supervisors Forum teleconferences and guiding the work of the group while promoting FINTRAC's Compliance Program and the Centre's latest achievements and activities.

RC3

s.13(1)(a)

s.15(1) I.A

C) Assessment Activities

1. New Developments in the Compliance Program

Transfer of Assessment Responsibility from the Office of the Superintendent of Financial Institutions (OSFI) to FINTRAC

Fiscal year 2019–20 marked the first year of transition to the new assessment approach between FINTRAC and OSFI for AML/ATF assessments of FRFIs. The development of a comprehensive implementation and operational plan guided the successful transfer of AML/ATF supervision to FINTRAC as the primary AML/ATF regulator for FRFIs. As a part of this implementation and operational plan, FINTRAC and OSFI undertook multiple activities to ensure a smooth and effective transition of responsibilities. The following is a summary of these activities:

- Developing a communications plan to announce the new approach to industry stakeholders and employees. External information sessions were held in Toronto in June 2019.
- Organizing national training sessions and job shadowing to learn, share and allow for knowledge transfer from OSFI to FINTRAC in areas such as risks assessment and correspondent banking. This allowed FINTRAC to conduct full scope bank assessments.
- Expanding and diversifying FINTRAC's assessment expertise by decentralizing the point of contact from its Toronto Office to all regional offices (i.e., Toronto, Vancouver and Montréal). The FINTRAC regional office that serves the geographical area where a FRFI is headquartered is now respectively managing that FRFI relationship and acting as the dedicated point of contact.
- Assigning a dedicated “portfolio” compliance officer to each of the B8 entities and establishing a dedicated inbox for those entities for all activities relating to the PCMLTFA and associated Regulations. This provides enhanced relationship management with these strategically important REs.

- Developing a governance framework to ensure ongoing interaction and communication between the agencies, which also serves to monitor and evaluate progress of transition and adjust as needed.
- Developing a business case requesting funds to successfully implement this new approach.

Overall, the implementation of the new approach was seen as relatively seamless and was well received by industry and the agencies alike. The new approach delivers a strong and effective AML/ATF regime while reducing duplication through better alignment with FINTRAC and OSFI's respective mandates and authorities.

Compliance Officer Training

Following the successful delivery of in-person, scenario-based and ad-hoc regional training last fiscal on FINTRAC's assessment approach, the agency made a landmark shift in 2019–20 to restructure and transform its compliance training program.

Continuous knowledge sharing and ongoing training are critical activities to ensure that regional compliance officers remain up to date on operational processes and maintain subject matter expertise. As such, and in line with an ever-growing trend in training, FINTRAC committed to transforming its current training program from a traditional, instructor-led platform to an e-learning platform.

This new platform will consist of a standing inventory of e-learning courses. The courses will focus on the hands-on skills compliance officers need to undertake their work, including applying FINTRAC's assessment approach effectively. Where needed, FINTRAC will supplement these e-learning courses with targeted instructor-led interventions to address more complex or recurring training needs. FINTRAC plans to release its suite of e-learning courses on a progressive basis over the next two years.

Restructuring of FINTRAC Operations Sector

To further improve FINTRAC's effectiveness as both a regulator and financial intelligence unit, FINTRAC's Operations Sector, which reported to a single Deputy Director, underwent a restructuring in 2019–20 to better serve the two main functions of the Centre. This fiscal year, FINTRAC separated its two principle operational functions into two independent sectors, Compliance and Intelligence, each led by its own Deputy Director. This segregation of the Operations Sectors strengthens governance and the independent accountability for both functions.

2. Examination Findings by Key Sectors

FINTRAC employs an assessment framework to ensure that examinations are conducted in a consistent and effective manner. Under the framework, the REs are selected for examinations based on risk. This approach is dynamic, meaning that the risks identified one year may

change in the next, as the environment changes (e.g., if new products are introduced or new vulnerabilities emerge within the financial system). FINTRAC's risk-based approach ensures that compliance activities are proportionate to the risk, which is generally based on the consequence and likelihood of non-compliance. The consequence of non-compliance is determined by assessing the reporting volume and size of the entity in question (therefore an analysis of the potential impact of non-compliance on AML/ATF; while the likelihood of non-compliance is assessed by considering a variety of factors under four main categories: the RE's business profile; compliance history; reporting behaviour; and other information or intelligence. An RE that is likely to be non-compliant based on these factors, and that presents considerable consequences if they are in non-compliance will score higher in this risk-based approach to selecting examinations.

Once it has evaluated an RE's risks, FINTRAC selects assessment methods that it will use as part of its examination. FINTRAC uses these methods to assess how the RE complies with the legal requirements set out in the PCMLTFA and associated Regulations. When applying assessment methods, FINTRAC reviews the RE's documents, client records, records of transactions and financial transaction reports, as well as conducts interviews of key RE staff.

Examinations are divided into three phases: planning the exam and scoping in which AML/CFT compliance requirements to focus on; conducting the examination and assessment; and developing the findings and finalizing the examination. In the planning phase, FINTRAC selects the examination scope and requirements that it will examine and the assessment methods it will apply. The examination scope is unique to every examination and considers, among other elements, the RE's business model, environment, activities, operations, and risks.

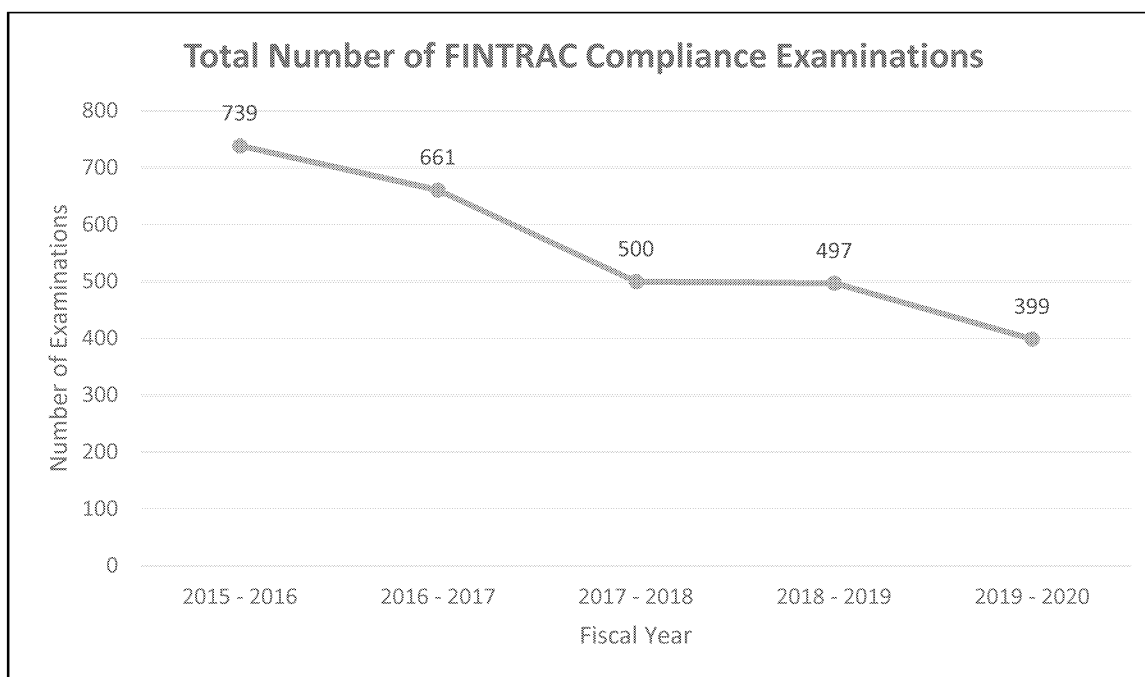
In the last phase, FINTRAC assesses the harm done of identified deficiencies, the extent of non-compliance, and any mitigating or aggravating factors. Though technical non-compliance with PCMLTFA and regulatory requirements is verified and noted, a FINTRAC examination pays special attention to the overall soundness and application of the RE's compliance program.

After an examination, the Centre may follow up to make sure that the RE has addressed the deficiencies identified in FINTRAC's findings letter. FINTRAC may conduct a follow-up examination, monitor the RE's transaction reports submitted to the Centre, and monitor progress in the RE's action plan. In some circumstances, an enforcement action may also be considered.

In 2019–20, FINTRAC conducted 399 examinations across all reporting entity sectors, as demonstrated in Table 1 below. The trend in the number of examinations experienced a 20% drop this fiscal year (from 497 examinations in 2018–19). This decrease reflects the complexity and resource intensive nature of examinations, especially those required for examinations of large REs (e.g., casinos and banks). Another factor contributing to the lower

number of examinations is the continued transition from an audit approach to an assessment approach for examinations at FINTRAC. As reported in last year's report, FINTRAC's assessment approach to compliance examinations places less emphasis on identifying technical deficiencies and more on the effectiveness of reporting entities in meeting obligations under the PCMLTFA, as well as on the impact of non-compliance on the objectives of the PCMLTFA and on FINTRAC's mandate. The benefits of the assessment approach helps the Centre better assist reporting entities to address areas for improvement and encourage compliance, while taking enforcement actions when required.

The effects of this transition on the total number of compliance examinations over the last five fiscal years are displayed in the chart below.



In 2019–20, FINTRAC completed three bank examinations within the Financial Entities sector. A number of other bank examinations were initiated and some work was completed in the reporting period. FINTRAC will be reporting on those examinations in next year's report. These large RE examinations required significantly more resources, specifically in terms of hours dedicated by regional compliance officers to prepare for and conduct these examinations compared to examinations in other sectors.

Examinations per Sector	
Sector	Number of examinations completed in 2019–20
Casinos	5
Financial Entities (i.e., banks, credit unions and caisses populaires)	47
Money Services Businesses (MSBs)	114
Real Estate Sector	146
Securities Dealers	58
Dealers in Precious Metals and Stones (DPMS)	16
Accountants	1
Life Insurance Companies, Brokers, Agents	1
British Columbia Notaries	10
Trust and Loans	1
Total	399

Casino Sector

RC6

For the casino sector, FINTRAC follows a cycle-based examination strategy that ensures that all 18 casino REs are examined every two to five years depending on their size, compliance history, and risk factors. In fiscal year 2019–20, FINTRAC examined five casino entities

s.16(1)(c)

s.20(1)(b)

s.20(1)(c)

Casinos have a unique challenge with the customer due diligence obligations under the PCMLTFA. As approximately 90% of their relationships with customers are one-off transactions, only 10% involve regular transactions that constitute a business relationship and, therefore, have ongoing monitoring requirements. Given the nature of casino operations, casino clients are often unknown and transactions often remain anonymous because there are no customer identification requirements until threshold transactions are triggered (i.e., \$10,000 or more) or an account is opened with the casino.

Overall, casinos remain cash intensive businesses and most clients continue to participate in casino play using cash. In early 2018, the British Columbia Lottery Corporation (BCLC), which oversees 30 casinos in the province, implemented new stringent cash reducing measures for its establishments, in which any client gambling \$10,000 or more with cash or negotiable instruments must provide proof of the source of funds (bank receipt, copy of bank draft purchase, etc.). Since implementation, the 2018 BCLC measures have likely contributed to a considerable reduction in cash gambling, and in turn, a decrease in the number of large cash transaction reports (LCTRs) received by FINTRAC from BC casinos. To FINTRAC's knowledge, casino REs in other provinces have not implemented similar measures, nor has the Centre seen any significant decreases in LCTR reporting elsewhere.

Casino Sector Examination Findings

RC6

All of the five casino exams conducted in 2019–20 were conducted on-site. The five completed examinations [REDACTED] and included 59 casino locations or 45% of the total casino population. In terms of size, FINTRAC examined two large and three small casinos. It is important to note that the revised casino definition (changed to align the casino definition in the PCMLTFA with the “Conduct and Manage” provision in the *Criminal Code* in 2017⁵) created new reporting structures in Canada. This resulted in consistent RE determination across Canada. As for compliance examinations, although the sites of the three small casinos were visited in the past under the old casino RE structure, this was the first time that they were examined under the new casino structure. In terms of deficiencies, we found

s.16(1)(c)

s.20(1)(b)

s.20(1)(c)

- no deficiencies with reporting quality, though we noted deficiencies related to timing of reporting for one casino;
- no record keeping deficiencies;
- three out of the five casinos examined had deficiencies related to incomplete policies and procedures;
- one out of five had an incomplete risk assessment;
- one out of five had inadequate training;
- two casinos were cited for missing a total of five suspicious transaction reports (STRs) over the examination period; and
- one out of five examined casinos was required to provide an action plan on how it would address the deficiencies noted during its examination as a matter of priority.

FINTRAC also applies a cycle approach to all casino REs in Canada when it comes to follow-up examinations. FINTRAC did not issue any AMPs in this sector in 2019–20. Although some STR reporting deficiencies were identified, the casino sector continues to exhibit positive results regarding reporting obligations for all other report types (Large Cash Transaction Reports and Casino Disbursement Reports). The casinos that were examined were found to be fully compliant with obligations to identify clients and to keep records.

⁵ For the purpose of the PCMLTFA, a casino is an entity in Canada (authorized to do business in Canada) if it is

- a lottery scheme, located at a fixed place of business that includes games of roulette or card games; or
- games, located at a fixed place of business, where there are more than 50 slot machines or similar electronic gaming device in the establishment. This could include a place of business such as a restaurant that has these electronic gaming machines; or
- a lottery scheme accessible to the public through the Internet or other digital network. This does not include an entity if it is solely offering online bingo or the sale of lottery tickets through the Internet or other digital network.

RC6

s.16(1)(c)

s.20(1)(b)

s.20(1)(c)

Banking Sector

As mentioned earlier, FINTRAC and OSFI are in the process of streamlining the supervision of the banking sector's AML/ATF compliance under the responsibility of one organization. FINTRAC will officially be the sole federal regulator for AML/ATF supervision starting on April 1, 2021. Following the 2018–19 pilot of joint-examinations with OSFI, FINTRAC has acquired significant expertise from conducting joint-examinations and participating in cross-training from its counterparts at OSFI in examining and assessing the compliance of FRFIs. Overall, FINTRAC notes that banks are investing significant resources in their AML/ATF programs; however, each bank seems to be at a different level in terms of the robustness and sophistication of its processes and compliance program. Therefore, FINTRAC examination results may vary widely within this sector year-to-year.

Of all businesses subject to the PCMLTFA, banks represent the largest REs, with multiple lines of business and presence throughout Canada and other jurisdictions. Key challenges they face as a sector include dealing with large volumes of clients and transactions, and identifying areas on which to focus when conducting their two-year review⁶ of their AML/CFT compliance program. FINTRAC examinations in this sector often identify a lack of awareness or consistent application of AML/ATF policies, procedures and training within bank operations. A major challenge for the FRFIs is to ensure that all internal units are working together to monitor clients, transactions and STR indicators.

⁶ Pursuant to Subsection 9.6(1) of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and Subsection 71(1) (e) of the associated Regulations.

Banking Sector Examination Findings

Among the three bank examinations that FINTRAC conducted in 2019–20, each FRFI was required to submit an action plan to address its identified deficiencies. Due to the nature of deficiencies and important role that this entity plays within the Canadian financial system,

RC6

Another observation that the Centre made in some examinations in this sector in 2019–20 was concerning policies and procedures where the threshold to report an STR seems to be assessed at a higher level than PCMLTFA requirements (i.e., reasonable grounds to believe versus to “suspect”⁷). When such deficiencies are found, they are noted in FINTRAC’s examination findings letters sent to the RE with the expectation that they will be rectified. While gaps are being found in these examinations, it is important to note that FRFIs are investing more resources on AML/ATF compliance, which is a positive step and a sign of progress in this sector. With continued investment, FRFIs will be better prepared to manage the massive volumes of clients and transactions under their purview and effectively fulfill the AML/ATF compliance requirements in the PCMLTFA and associated regulations.

s.16(1)(c)

s.20(1)(b)

s.20(1)(c)

⁷ Pursuant to Section 7 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*

RC6

s.16(1)(c)

s.20(1)(b)

s.20(1)(c)

Money Services Business Sector

FINTRAC has conducted 114 examinations of money services businesses (MSB), consisting of 41 desk exams and 73 on-site exams. REs are selected based on their [REDACTED] as assessed by FINTRAC's risk model. [REDACTED]

[REDACTED] this year, MSBs consisted of 29% of the examination plan.

Of the total 114 examinations, two were recommended for enforcement actions (2%), 39 were recommended for a follow-up activity (34%), and 73 required no further activity (63%). These percentages are consistent with the average of all examinations conducted by FINTRAC: 13 recommended for enforcement (3%); 135 recommended for follow-up activity (34%); and 251 required no further activity (63%).

Follow-Up Activities

A follow-up activity is one of the main outcomes following an examination along with *no further activity* and *enforcement activity*.

When an RE is recommended for a *follow-up activity* there are a number of options that FINTRAC can pursue including a follow-up examination, an action-plan, a database examination, or a compliance meeting.

RC6

s.16(1)(c)

s.20(1)(b)

s.20(1)(c)

For the MSB sector in 2019–20, FINTRAC conducted five follow-up examinations. As a result, three entities required no further activities and two will require follow-up activities. Of the latter two, one was recommended for a data integrity monitoring activity and the other will require a compliance meeting for FINTRAC to assess the progress of the entity. No follow-up examinations were deemed necessary.

Also in the MSB sector, FINTRAC issued one AMP c [REDACTED] and, across the overall sector, seven non-compliance disclosures were issued.

FINTRAC identified challenges and trends in this sector during this fiscal year's examinations. Lingering challenges FINTRAC faces with this sector include determining whether all MSBs have registered with FINTRAC, and/or are still in operation (including those that have registered) at a given time. Due to the short lifespan and transient nature of some MSBs (with some operating less than three years), FINTRAC encounters an ongoing challenge in identifying MSBs and conducting compliance examinations before they cease to operate.

To mitigate these issues, FINTRAC conducts annual MSB validations to identify those that may be operating with expired, ceased, revoked or denied registrations, and those that may no

longer be operating. MSBs that are suspected of operating, but that are not registered, are promptly contacted and action is taken to bring them into compliance.

In the realm of virtual currencies (VC), FINTRAC continues to develop strong bilateral relationships with international partners to enhance knowledge sharing. In 2019–20, to prepare for the coming into force of the VC legislation,

s.13(1)(a)

s.15(1) I.A

RC3

FINTRAC also regularly consults with FinCEN to leverage its expertise and experience in regulating the VC sector.

Real Estate Sector

In 2019–20, FINTRAC continued to prioritize the real estate sector in its examination strategy due to the known sector-wide vulnerabilities and risks of money laundering. Ongoing scrutiny and elevated risk in this sector are driving factors for its increased focus in FINTRAC's compliance examinations plans. As a result, FINTRAC conducted 59 desk exams and 87 on-site examinations in the real estate sector, for a total of 146 assessments compared to 190 in 2018–19. Overall, this represents a similar percentage of compliance examinations for both fiscal years. In 2018–19 approximately 38% (197/497) of the yearly examination plan focused on the real estate sector, and in 2019–2020 approximately 37% (146/399) of the yearly plan focused on that sector.

FINTRAC implemented a new approach for real estate examinations, whereby a greater focus is placed on assessing compliance program elements, such as policies and procedures, client identification, and the reporting of STRs. It also includes an outreach component on identifying and reporting STRs. This also partly explains the lower number of examinations, as it requires additional time and resources. However, as a result, FINTRAC observed that STR reporting increased from 100 in 2018–19 to 138 this fiscal year (the highest yearly total yet). Although this represents a 38% increase year over year, the sector still retains one of the lowest STR reporting levels from a perspective of overall numbers. The STR reporting volume for the prior five years is indicated in the figure below.

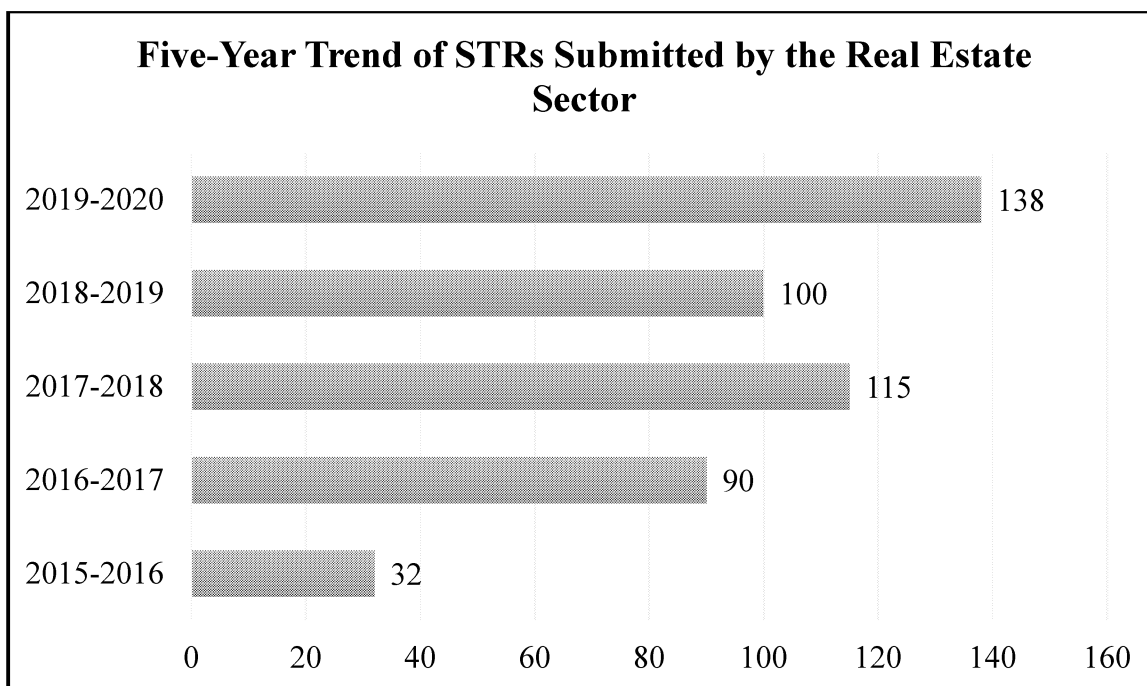


Figure 1: A five-year comparison on the number of suspicious transactions reports submitted by the real estate sector prior to 2019-2020.

FINTRAC's 146 examinations of REs in the real estate sector represented 37% of the overall examination plan. Of the 146 examinations, the outcomes were as follows: 7 were recommended for enforcement actions (5%); 59 recommended for a follow-up activity (40%); and 80 required no further activity (55%).

When compared to the average of all examinations conducted by FINTRAC, the real estate numbers represent a slightly higher level of non-compliance. The comparison between follow-up and enforcement activities required as part of real estate examinations and the overall average is as follows:

- Enforcement action: 5% for real estate vs. 3% for total average of all examinations
- Follow-up activity: 40% for real estate vs. 34% for total average of all examinations
- No further activity: 55% for real estate vs. 63% for total average of all examinations

Areas in the sector where the Centre identified the highest level of non-compliance were in the implementation of adequate risk assessments, incomplete or generic policies and procedures, as well as gaps in client information records, and receipt of funds records. To address the non-compliance in this sector, the Centre conducted 35 follow-up examinations to assess the level of enhancement in compliance with the Act and Regulations with three of these being recommended for a penalty. Lastly, one AMP was issued to a real estate entity in 2019–20.

FINTRAC faces a number of compliance challenges in the real estate sector. Primarily, there remains a misunderstanding among several REs across this sector as to how ML/TF can occur during a real estate transaction. To address this lack of awareness of ML/TF risks, and in addition to guidance on FINTRAC's website, examinations now include an outreach component on how to complete an STR and how to recognize indicators of ML/TF. This new approach is in place and appears to have had an impact on STR reporting levels, as described above.

Another challenge faced by FINTRAC is the very high population of real estate entities in the sector. The number of real estate examinations within the yearly examination plan is significant, however it covers a small portion of the overall RE population when considering the several thousands of real estate REs that exist across Canada. FINTRAC dedicated resources in 2018–19 to identify new REs across activity sectors, including in the real estate sector, and as previously mentioned, the Real Estate Council of British Columbia's (RECBC) provided a reliable list of registered entities in British Columbia. Some of these newly identified entities were added to the examination plan for 2019–20.

As per FINTRAC's risk-based approach, examinations in this sector continued to focus on large brokerages in Vancouver and the Lower Mainland, as well as those from the Greater Toronto Area and Montréal. Such large REs represent a greater share of the market, and some adopt several dozens, if not hundreds, of agents. Therefore, the focus on larger entities offers the Centre with impactful opportunities to assist and assesses compliance with the PCMLTFA and its regulations in this sector.

The real estate sector exhibits high vulnerabilities, as identified in the Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada⁸ (also known as the National Risk Assessment). As such, FINTRAC will continue to invest a significant number of resources to this sector, specifically in British Columbia, to focus on specific areas of risk, such as high value and high volume sales.

3. Results of Follow-up Examinations in All Sectors

In 2019–20, FINTRAC conducted 44 follow-up examinations. Of these, four resulted in enforcement actions (9%), 13 were considered for a follow-up activity (30%) and 27 required no further activity (61%).

The four examinations that resulted in an enforcement action were recommended for AMP consideration (three real estate and one DPMS). The 13 entities where a follow-up activity was considered resulted in actions as follows:

⁸ *Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada*
<https://www.canada.ca/en/department-finance/services/publications/assessment-inherent-risks-money-laundering-terrorist-financing.html>

Of the 27 where no further activity is required,

- two REs were credit unions;
- three REs were MSBs; and
- 22 REs were in the real estate sector.

s.16(1)(c)

Out of the 44 follow-up examinations conducted, 35 were carried out in the real estate sector alone. The outcomes of these examinations were as follows:

- Three were recommended for an enforcement action (9%)
- 10 were recommended for a follow-up activity (29%)
- 22 required no further activities (63%)

4. Third Party Analysis of Suspicious Transaction Reports (STRs)

Summary of STR Third-Party Assessment

During the 2019–20 fiscal year, FINTRAC completed 21 third-party STR analyses. This internal product allows FINTRAC

The third-party analysis allows FINTRAC to examine the larger reporting environment of the RE being examined and to test the effectiveness of its risk-based approach in identifying suspicious transactions. With this approach, FINTRAC

The approach helps FINTRAC identify potentially suspicious transactions and verify whether the examined entity should have submitted STRs.

While initially envisioned as a tool for real estate examinations (), the third-party analysis was expanded to many other sectors, ranging from major banks to dealers in precious metals and stones (DPMS) and to casinos. FINTRAC regional officers also played a key role in providing input to adapt this product to the different challenges posed by the various sectors and to meet the needs of each specific examination.

RC6

s.16(1)(c)

This approach is proven to be very effective particularly for sectors where there is low reporting. The third party analysis approach is used to identify lines of questioning for the REs that are to be examined and that do not submit many reports. This approach is particularly effective for sectors like [REDACTED]

D) Enforcement Activities

1. Update on AMPs Review and AMPs Activity

The Centre completed the final stage of the AMP program review in August 2019. This resulted in the publication of seven harm done assessment guides⁹ that describe FINTRAC's approach to assessing the harm done by the 200 violations prescribed in the *PCMLTF Administrative Monetary Penalties Regulations*, and FINTRAC's rationale in determining the corresponding penalty amounts. In addition to the AMPs policy, these guides and penalty calculation examples are published and readily available on FINTRAC's website. As such, REs and the public can find specific information on expectations when FINTRAC proceeds with an enforcement action and they can see how the Centre calculates an AMP.

With this publication, the Centre further strengthened FINTRAC's Enhanced Transparency Initiative introduced last fiscal year. It is worth re-stating that FINTRAC received recognition from the CFR for excellence in regulatory openness and transparency.

With the AMPs review complete and REs fully aware of FINTRAC's new methodology, the AMP program has resumed its issuing of penalties to non-compliant REs under the new AMP policy and penalty calculation methodology. In 2019–20, FINTRAC issued two additional notices of violation under the new AMP policy and penalty calculation methodology. One case is closed with the penalty being imposed and the other was reviewed as of July 2020, and it is awaiting closure.

A number of AMP files are in progress as of March 2020. FINTRAC is in the process of considering possible enforcement action for a number of additional examinations.

2. Public Naming – Legislative Requirement

In support of efforts to enhance regulatory transparency, the PCMLTFA was amended on June 20, 2019, requiring FINTRAC to make public all AMPs imposed. Going forward, all AMPs imposed by the Centre must be made public as soon as feasible.

3. Non-compliance Disclosures to Law Enforcement

In addition to communicating seven non-compliance disclosures (NCDs) to law enforcement this fiscal, the Centre substantially increased its outreach and awareness efforts with respect to non-compliance offences of the PCMLTFA. The result is an exponential increase in interest

⁹ Harm done assessment guides, <https://www.fintrac-canafe.gc.ca/pen/1-eng>

to consider non-compliance investigations and charges. As part of efforts to bring awareness to law enforcement and Crown prosecutors, FINTRAC delivered 13 outreach events; responded to 43 enquiries on compliance requirements from federal, provincial and municipal law enforcement bodies; and assessed 163 voluntary information records for non-compliance. In 2019–20, FINTRAC became aware of one case where individuals and entities were charged with offences under the PCMLTFA including the failure to register as an MSB and failure to report transactions. Generally, FINTRAC maintains awareness of non-compliance charges laid through monitoring of open-source information, as well as through relationships fostered with law enforcement bodies.

4. Voluntary Self-declaration of Non-compliance (VSDONC)

FINTRAC published its VSDONC policy in February 2019. In 2019–20, the Centre received 134 VSDONCs, which represents a 97% increase in such declarations from the previous fiscal year where 68 VSDONCs were completed. This is mainly explained by the increased awareness of reporting entities of this tool, since the publication of the policy, allowing them to proactively rectify non-compliance as soon as they detect it. The majority of VSDONCs involved transaction reports that had not been reported (large cash transaction reports, electronic funds transfer reports and STRs), mainly due to RE systems error. The majority of VSDONCs received came from financial entities. Subsequently, Compliance HQ and the regions worked closely with the REs that communicated the VSDONCs to the Centre to ensure that all related reports were submitted accurately to FINTRAC.

VSDONCs are an important tool for FINTRAC to ensure that REs comply fully with the PCMLTFA and submit previously unreported reports that they detect via different methods (e.g., due to a periodic review of their program; conducting ongoing risk assessments or quality control activities, etc.). Not only do VSDONCs encourage compliance from REs [REDACTED] the resulting reports become potential actionable financial intelligence that the Centre can disclose to law enforcement and national security partners when legislative disclosure thresholds are met.

s.16(1)(c)

RC6

IV. FINTRAC'S CONTRIBUTION TO IMPROVING THE EFFECTIVENESS OF CANADA'S AML/ATF EFFORTS

A) Development and Implementation of Regulatory Amendments

In addition to working closely with the Department of Finance Canada and the Department of Justice Canada to complete the development of PCMLTFA regulatory amendments published in July 2019, FINTRAC also supported the drafting of an additional set of regulatory amendments that were pre-published for consultation in Part 1 of the Canada Gazette on February 15, 2020.

During the first year of implementation of the July 2019 regulatory amendments, FINTRAC successfully made IT systems changes and provided guidance to REs in November 2019 and

March 2020, which allowed the pre-registration of VC and FMSBs in advance of the coming into force on June 1, 2020 of new obligations for these REs. The remainder of the regulatory amendments, which are set to come into force on June 2021, represent substantial implementation work, including the introduction of new large virtual currency transaction reporting obligations and additional customer due diligence and record keeping requirements. This work and other competing priorities have added significant pressures on current FINTRAC resources.

FINTRAC remains committed to executing the necessary infrastructure to allow for the implementation of new requirements, but it will not be without additional and unexpected challenges. At the fiscal year end, it was clear that the pandemic restrictions on both FINTRAC and REs operations would affect the implementation project's critical paths and contribute to delays in key system infrastructure updates to allow for new reporting requirements. The Centre will work with the Department of Finance Canada to explore ways in which FINTRAC can demonstrate flexibility in developing systems, as well as applying and enforcing the new regulations.

B) Update on 2018 Parliamentary Review

Following the 2018 Parliamentary Review of the PCMLTFA by the House of Commons Standing Committee on Finance (FINA), FINTRAC received funding through the 2019 Budget to strengthen FINTRAC's compliance activities in the real estate and casino sectors in British Columbia to support the implementation of new regulations, and to expand FINTRAC's public-private partnership projects. FINTRAC also participated in new initiatives such as the Canada Border Services Agency's (CBSA) Trade Fraud and Trade-Based Money Laundering Centre of Expertise, and Public Safety Canada's AML Action Coordination and Enforcement (ACE) Team, both of which support further collaboration among AML/ATF Regime members through the sharing of resources and information.

In addition, FINTRAC continued to work with the Department of Finance Canada to research and develop policy options on issues that the FINA Report identified. FINTRAC assisted in developing policy on the following subjects in 2019–20:

- analysis regarding new disclosure recipients and new reporting entity sectors;
- options to implement geographic advisories;
- transition to becoming the sole supervisor of FRFIs;
- electronic submission and reception of cross-border currency and cross border seizure reports from CBSA; and
- increasing public awareness of FINTRAC and its mandate.

C) Contribution to Canada's National Inherent ML/TF Risk Assessment

In 2019–20, FINTRAC continued to play a leadership role in advancing the Regime's understanding of ML/TF vulnerabilities by contributing knowledge and data towards the

update of Canada's 2015 National Inherent ML/TF Risk Assessment. More specifically, FINTRAC conducted research and analysis on RE sectors covered by the PCMLTFA, as well as on other relevant and ancillary sectors that are not currently REs under the Act to better understand risks and vulnerabilities that may be exploited by criminals to generate proceeds of crime, launder money, or finance terrorism.

D) Strategic Analysis of Canada-Linked Illicit Finance Dynamics

FINTRAC financial intelligence assessments have highlighted areas of vulnerability to global illicit finance networks in the Canadian financial system

s.15(1)

s.16(1)(c)

These networks have been observed to simultaneously engage in major money laundering on behalf of transnational organized crime groups while facilitating remittances, capital flight, and trade payments on behalf of third parties, using the formal financial system, informal value transfer systems and trade-based money laundering.

Global illicit finance network often operate through multi-level compensation schemes that leverage global cash pools. Illicit cash is a commodity for which there is an offer and a demand. The formal financial system is critical to the settlement of compensation schemes.

RC6

RC3

Key illicit finance network "streams" linked to Canada include the following:

RC3

s.15(1)
s.16(1)(c)

RC6

E) Engagements with the Department of Finance Canada and Other Government of Canada initiatives

FINTRAC provided insight into the development of the proposed *Retail Payments Act*, specifically the registration component of this, because of Centre's experience with the MSB registration obligations and its public registry of MSBs.

FINTRAC also participated in the Federal-Provincial/Territorial (FPT) Working Group on Beneficial Ownership. As a member of the FPT Working Group on Increasing Beneficial Ownership Transparency, FINTRAC provided its expertise in detecting, deterring and preventing ML and TF by contributing input on a consultation paper prepared by Innovation Science and Economic Development Canada and the Department of Finance Canada to inform the development of measures to increase beneficial ownership transparency in this country. FINTRAC also provided its expertise to the province of British Columbia as it begins work to develop a public beneficial ownership registry.

F) Engagement with Financial Action task Force (FATF)

Supporting the Head of Delegation to the FATF at the Department of Finance Canada, FINTRAC regularly reviewed documentation from FATF, and provided compliance/supervisory perspectives to key FATF papers and initiatives. Such input heavily involved FINTRAC subject matter expertise insight into the FATF's Risk-based Approach Guidance, international surveys and other FATF papers. FINTRAC also contributed to Canada's third year follow-up report, as well as to the preparation for the fifth year follow-up one. FINTRAC was a part of the Canadian delegation at international FATF meetings related to virtual currency providers and supervisory roles.

G) FINTRAC Contributions to the Commission of Inquiry into Money Laundering in British Columbia

FINTRAC has been an active participant in the ongoing provincial Cullen Commission, and has dedicated significant resources to responding to the Commission's requests for the Centre's data, documentation, and interviews with FINTRAC subject matter experts.

FINTRAC has produced briefing materials for use by witnesses at hearings and interviews, including issue sheets on specific hearing topics. These documents aim to help witnesses explain FINTRAC's mandate and the evolution of the Centre's Compliance and Intelligence programs, and highlight ongoing and upcoming work to address issues relevant to the Commission.

FINTRAC is also working closely with Regime partners to respond efficiently and appropriately to requests for documentation by the Commission. This effort is coordinated through a Cullen Commission Joint Policy Committee headed by the Department of Justice, that aims to administer production deadlines and strategies for Government of Canada witness testimony.

Going forward, FINTRAC will continue to respond to requests for information made by the Commission and it will continue to develop messaging that properly positions its role and demonstrates its results in British Columbia.

V. Upcoming Compliance Priorities

FINTRAC will continue to work with REs and their industry representatives to implement the amendments to the PCMLTFA's associated Regulations. For example, the Centre will continue to draft and publish over 60 pieces of guidance for REs relating to the amendments coming into force on June 1, 2021. In addition, FINTRAC's Compliance sector will continue to provide timely PIs to REs, industry associations, and other regulators.

The Centre will continue to provide its operational perspectives on policy proposals currently under consideration. To this end, the Centre remains dedicated to supporting the Department of Finance Canada as the Canadian AML/ATF regime's policy lead.

From an assessment perspective, the focus in 2020–21 will be on the continued transition for AML/ATF supervision of FRFIs from OSFI to FINTRAC. As the Centre takes full responsibility for AML/ATF supervision of FRFIs, FINTRAC will focus on acquiring resources to better assess FRFIs, including staffing and training. FINTRAC will also continue to ensure compliance with the PCMLTFA and its associated Regulations among all sectors, with special attention to the casino and real estate sectors across the country, and especially in British Columbia.

FINTRAC will also seek to build capacity in understanding and assessing ML/TF risks in the virtual currency sector. This includes the acquisition of technology and the development of expertise for supervision of this new activity within the MSB sector. Considering that this newly regulated sub-segment of the MSB sector is very different from traditional REs covered under the PCMLTFA, FINTRAC remains dedicated to developing and fostering subject matter expertise to ensure the compliance of these new REs.

On enforcement, FINTRAC will continue to focus on administering the newly revised AMP policy and continue to address the enhanced interest from law enforcement on NCDs. FINTRAC will continue to invest in its people. Virtual training will continue to be enhanced and continuous learning will be promoted, especially in areas related to new and emerging trends in AML/TF.

VI. SUPPORT FOR REPORTING ENTITIES DURING the COVID-19 PANDEMIC

The onset of the COVID-19 pandemic lockdown measures in March 2020 led to significant changes in the way FINTRAC and REs conducted their business. The business of AML/ATF compliance was not immune to the pandemic. As the seriousness of the COVID-19 pandemic increased, FINTRAC's Compliance sector immediately took action and worked swiftly and diligently to respond to the challenges faced by REs in their ongoing compliance with the requirements of the Act and associated Regulations.

As early as March 25, 2020, FINTRAC was able to demonstrate administrative flexibility by releasing a message to all REs regarding reporting requirements, and identity verification, including the status of compliance assessments and enforcement during the COVID-19 pandemic. This guidance acknowledged challenges faced by REs and indicated that no new examinations would start until further notice. It also provided guidance for REs that may have believed that the pandemic would affect their ability to meet their obligations. The message asked REs to prioritize submissions of STRs and encouraged REs to submit VSDONCs if they feared they would not be able to meet their obligations for reasons outside of their control. The guidance also included direction on acceptable flexibility in verifying the identities of individuals. FINTRAC released an additional three messages to REs after March 25. In addition to providing guidance related to RE obligations and proactively posting information on FINTRAC's public website, FINTRAC also contacted industry associations and conducted extensive virtual outreach to REs across the country.

The effects of the pandemic took hold only toward the final weeks of fiscal year 2019–20. As such, its true effects will be much more apparent in the following year and ongoing. Potential outcomes of the global pandemic on fiscal year 2020–21 may include fewer opportunities for in-person engagement events, fewer on-site compliance examinations, an increase in VSDONCs, and other unforeseen consequences.

As for enforcement activities, the current COVID environment has affected FINTRAC's interpretation of reasonable timeframes given the working conditions of some REs and their respective representatives in court. In light of measures taken throughout sectors, given the pandemic (less staff, shorter work hours, work from home, etc.), FINTRAC decided to continue issuing penalties, but has exercised flexibility in increasing the appeal period from 30 to 90 days to ensure that REs seeking review of their penalty have ample time to prepare their case. This approach is in line with Federal Court extensions of time granted amidst the COVID-19 pandemic.

FINTRAC will work closely with regime partners and stakeholders, and will continue to assess the situation in relation to COVID-19 to ensure that the Centre can continue to ensure compliance with the PCMLTFA and protect Canadians and Canada's financial system, while respecting and supporting reporting entities in these challenging times.

VII. CONCLUSION

FINTRAC took significant steps to further strengthen its Compliance Program in 2019–20. The Centre continued to demonstrate its commitment to enhance the transparency of its program and finalized FINTRAC's AMP Review through the publication of the harm guides, and continued its work toward the updating of the Assessment Manual.

In 2019–20, FINTRAC's Compliance Five-Year Engagement strategy was launched. It had already made significant progress in its engagement efforts on the implementation of regulatory amendments; its engagement with sectors with high ML/TF risks; its development and revision of MOUs with relevant stakeholders; and its broad engagements with many different business sectors and across all levels of government.

For assessments, this year marked the beginning of the transition of AML/ATF supervisory responsibilities of FRFIs from OSFI to FINTRAC. Fiscal year 2020–21 will be the second and final year of this transition. Additionally, compliance examinations continue to show positive results relating to the implementation of the new assessment approach.

In 2020–21, FINTRAC will continue to focus on strengthening its relationships with REs through its various engagement activities as the Centre enters year two of its five-year engagement strategy. FINTRAC will also continue to apply its new enforcement tools, such as the new AMPs policy and VSDONC policy, to ensure that non-compliance is effectively deterred, thereby allowing valuable intelligence to successfully reach the Centre.

In summary, as FINTRAC looks to the future, and in its 20th anniversary of service, it will be important to take stock of the agency's progress and evolution, while continuing to build on the momentum created by the significant changes to regulatory transparency that have taken place in 2019–20. FINTRAC will continue to close regulatory gaps; draw insights from our analysis; and use our regulatory authorities to mitigate existing and emerging risks and in responding to threats to the safety of Canadians and to our economy.