



Department of Finance Canada
Ministère des Finances Canada

MEMORANDUM NOTE DE SERVICE

TO À  Minister of Finance

FROM DE Paul Rochon

SUBJECT OBJET **COVID-19-Related Money Laundering Risks and Challenges**

Security classification Classification de sécurité
PROTECTED B
Originator Auteur
Tamara Trotman
Our file Notre référence
Your file Votre référence
2020FIN498914
Date

For Information. This note provides background information on the unexpected global increase in money laundering related to COVID-19, as well as proposed next steps.

Summary

- Criminals have profited from the COVID-19 pandemic resulting in an unexpected increase in global financial crime. Criminal networks have exploited government pandemic supports; weaknesses in compliance, supervision and enforcement; and digital technologies.
- The global response to COVID-19 has highlighted the importance of robust and adaptable business continuity plans on the part of governments and reporting entities.
- Active communication and partnerships among domestic and international financial intelligence units (FIUs), law enforcement and reporting entities is essential to fighting COVID-19-related financial crime. This should include regular sharing of typologies and guidance to the private sector so it is equipped to prioritize operations based on risks.
- It is important for countries to assess and communicate risks on a continuous basis, and advance policies, legislation and regulations to respond to emerging risks and strengthen regimes.

Background

The Financial Action Task Force (FATF) has taken a leadership role in trying to understand global money laundering (ML) and terrorist financing (TF) risks and vulnerabilities associated with COVID-19. In May it published a paper, which identified challenges, good practices and policy responses to new ML and TF threats and vulnerabilities arising from the COVID-19 crisis. Since the publication of the paper, COVID-19-related financial crime has evolved and expanded. Given the evolving situation, the FATF solicited in July updated information from its

ADM: Leah Anderson (613-369-3620)
Director General: Lynn Hemmings (613-369-3865)



- 2 -

global network and hosted a number of workshops to facilitate information sharing. Canada's most recent submission to the FATF (see Annex A) includes input from the Canada Revenue Agency, the Financial Transactions and Reports Analysis Centre (FINTRAC) and the Royal Canadian Mounted Police (RCMP). The risks and increase in financial crimes identified by Canada's operational partners are consistent with those identified by other jurisdictions. However, responses to these crimes vary by jurisdiction.

On July 30 and 31, the FATF hosted a webinar on ML/TF risks in relation to COVID-19. Participating experts represented Europol, Interpol, FIUs, anti-money laundering (AML) supervisors, global financial institutions, treasury departments and the FATF. The experts were unanimous in their findings. Financial crime is on the rise at levels not expected at the start of the pandemic; however, it is too early to pronounce on TF activity. Interestingly, non-financial crime such as illicit drug use and violence remains steady at pre-pandemic levels while financial crime has "exploded" according to experts.

As businesses closed, individuals remained in their homes and governments issued supports, criminals moved quickly to take advantage of the situation. Governments around the globe have reported fraud associated with COVID-19-related government procurement. For example, the German government was duped into procuring €15 million worth of face masks which did not exist by a network of fraudsters in Ireland, the Netherlands, the United Kingdom and Nigeria.

In addition, governments have reported fraud associated with COVID-19-related government supports to individuals and businesses. As subsidies rolled out quickly, it was easy for criminals who had been holding stolen or fake ID for a long period of time to access government loans and direct payments. Major banks have become unwitting recipients of fraudulent payments that end up in mule accounts. This is exacerbated by financial institutions' existing verification methods, which have become ineffective.

As businesses closed and staff worked from home without access to the tools required to fulfill their duties, criminal networks preyed on vulnerable businesses with debt or low revenues by taking over these struggling businesses in order to clean their illicit funds. They also took over IT infrastructure of companies whose at-home IT staff were unable to maintain security protections and monitor systems, making e-mails and business transactions appear legitimate.

Criminals have also been scamming lonely individuals isolated at home looking for companionship by purchasing a pet. Fraudsters have required large deposits without delivering.

Additional COVID-19-related financial crime activities include:

- Social media and donation fraud.
- Child sex exploitation.
- Significant increase in the use of cryptocurrencies for the illicit transfer of funds.
- Electronic ransom and extortion, almost exclusively via Bitcoin. *Note that at the July 31 G7 Deputy Ministers of Finance meeting there was a decision to study this issue.*
- Stock exchange fraud.
- Taking advantage of real estate market price fluctuations for investments.
- Stockpiling cash as it has become riskier to smuggle cash across borders via mules.
- Illicit production of tobacco as criminal organizations expect governments to increase excise taxes.
- Taking advantage of gaps in legislation and regulations in different jurisdictions and in gaps among financial institutions by moving cash from one bank to another knowing that in many jurisdictions privacy/data protection legislation does not permit banks to communicate.
- Taking advantage of circumstances in developing countries where the population relies on mobile payments.

Considerations

How are Jurisdictions Responding?

The crisis exposed poor business continuity planning and outdated technology infrastructure in private sector and government systems and institutions. Most jurisdictions have since overhauled their business continuity plans and ordered secure and encrypted laptops to facilitate work from home. To bolster their response to the increase in financial crime, most jurisdictions are re-orienting their existing public-private partnerships with financial institutions to COVID-specific risks. In addition, some jurisdictions are permitting information sharing among large financial institutions in order to detect when criminals are using multiple banks to spread their risks.

In most countries, law enforcement has been diverted to support pandemic-related responses such as enforcing quarantines. By contrast, Australia has a dedicated economic crime centre and its law enforcement agents only cover financial crimes; they cannot be reassigned.

Understanding risks and evolving typologies allows resource deployment where it will be most effective. This includes real time assessments of customer behaviour. Governments are revising national risk assessments or creating COVID-19-specific risk assessments. FIUs from most advanced economies have been engaged in regular (weekly) communications with their reporting entities sending out newsletters, typologies and guidance on risk-based approaches. Some governments are obligating their banks to take on new responsibilities to address new crimes. For example, AUSTRAC (Australia's FIU) has required Australian banks to produce daily real-time intelligence related to COVID-19 issues.

Financial institutions have discovered that their existing customer due diligence and transaction monitoring protocols are no longer effective as they reflect pre-COVID profiles and behaviours

- 4 -

of customers and retail clients. Now that client patterns have shifted, existing profiles are ineffective at detecting suspicious activity. Moreover, client-facing staff have traditionally been critical to financial crime detection (e.g., the smell test) and were in the past responsible for 50% of suspicious transaction reports (STRs). Those staff are no longer engaging with customers in the same way. In response, some jurisdictions are supporting their financial institutions in deploying machine learning to detect unusual behaviour and track behavioural indicators in order to assess whether a customer's transaction is legitimate. In addition, some financial institutions are bringing together their fraud, financial crime compliance and cyber teams to take a big picture approach.

The impacts on individuals has been especially troubling. To educate the public, some jurisdictions and organizations are focussing on public awareness so citizens know what steps to take should they fall victim to a financial crime. To support awareness, Interpol has published information for the public concerning identity theft. In addition, Interpol has provided FIUs access to its database, and will be rolling out database access to financial institutions next year.

Given the level of cash stockpiling and risks that criminals are taking to move that cash, there have been a significant number of cash seizures by law enforcement globally. For example, on July 27, the RCMP made a significant cash and drug seizure near Windsor laying charges under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*.

Finally, from a global coordination perspective, one of the priorities for the 2020 to 2021 term of the German presidency of the FATF is digital transformation. This work should help make the case for reporting entities and FIUs to embrace the use of new technology in order to catch up to criminal organizations. Assessments of use cases may lead to a corresponding call for jurisdictions to change policies and legislation to facilitate more effective financial crime detection.

What Does This Mean for Canada?

The rise in financial crime, particularly through the use of cryptocurrencies, reinforces the need for Canada to stay the course in implementing its virtual currency regulations, which are expected to come into force fully in 2021. Given the importance of understanding one's own risk context, Canada's anti-money laundering/anti-terrorist financing (AML/ATF) regime should aim to complete its update of the national inherent risk assessment in the near term.

Communication between governments and their reporting entities and reporting entities' compliance with AML legislation and regulations has been critical for all parties to understand risks and take appropriate measures to combat the rise in money laundering. We should continue to encourage FINTRAC to increase the frequency of its outreach to reporting entities, particularly around evolving risks. Moreover, throughout the crisis, other jurisdictions maintained desk-based examinations of their reporting entities and are now moving back to on-site examinations. FINTRAC deferred desk-based and on-site examinations from the start of the pandemic; on July 27, FINTRAC issued an advisory indicating that desk-based examinations would resume in the coming weeks.

- 5 -

Finance will need to conduct research and engage operational partners on appropriate supports to combat the increase in money laundering, including resources, legislation and regulations.

[Redacted]

[Redacted]

Most other advanced economies have adapted to remote work by purchasing encrypted laptops and providing necessary tools.

[Redacted]

Next Steps

[Redacted]

[Redacted]

As work led by TBS on the government's digital strategy advances, Finance will communicate relevant developments to reporting entities. Finally, Finance will maintain its engagement with the FATF, G7 and Five Eyes on these issues.

s.18(d)

s.21(1)(a)

s.21(1)(b)

s.21(1)(c)

Annex A

Canada's Submission to Financial Action Task Force

COVID-19 ML/TF Risk Landscape and Corresponding Operational Responses

1) Since the last call for delegation input in March 2020, how have the ML threats and vulnerabilities associated with the COVID-19 pandemic developed? In particular:

- Have you detected any new ML threats or vulnerabilities in your jurisdiction?
- To what extent has ML activity been affected by changes in the ways that predicate offences are being committed? Are certain predicate offences leading to new ML typologies?
- Are there any informative case studies that you would be able to share? [If you are providing a case study please inform the Secretariat whether or not it is provided on a confidential basis, and if so, which parts of the case study are confidential]
- Are there any medium to long-term risks you see as emerging issues related to COVID-19?

Although it is still too early to determine if/how this pandemic will alter the money laundering landscape in the long run, the COVID-19 pandemic has important implications for organized crime by creating new or expanded opportunities for perpetrating fraud. For example, COVID-19 has led to an increase in specific categories of fraud and criminals have adapted from existing schemes, including phishing scams, identity fraud, and merchandise scams. Numerous law enforcement authorities also identified purchase order scams that involved the ordering of Personal Protective Equipment (PPE) supplies where payment is conducted via funds transfer (<https://www.edmontonpolice.ca/News/MediaReleases/ppeonlinescam>).

Rather than new ML typologies, general trends will likely continue for the laundering of COVID-19 fraud proceeds. This includes an increased use of virtual currencies, leveraging of mules (often the victims themselves) and the use of traditional product and services offered by financial institutions (for example, credit card payments, e-Transfers and wire transfers).

The COVID-19 pandemic, and associated closures and physical distancing measures, have disrupted some money laundering methods—particularly those that rely on placing illicit cash into cash-intensive businesses—and may expose criminal actors seeking alternate venues to integrate illicit proceeds into the financial system.

Canada Revenue Agency (CRA), which is responsible for administering tax laws in Canada, is facing a new threat of identity theft and the claiming of fraudulent government benefits pertaining to COVID-19. It may be very difficult to trace fraudulent benefits obtained through identity theft. CRA also has to cooperate closely with the police so that the latter can investigate fraud related to the Canada Emergency Response Benefit (CERB), which is a benefits program that was launched in response to COVID-19.

In the medium-term, CRA faces the risk of tax evasion pertaining to government's aid created to assist those affected by COVID-19, such as CERB and other government benefits. There could be money laundering with regards to tax evaded on this unreported income and it is very unlikely that those who obtain these benefits through identity theft will report this income. CRA will be able to investigate tax evasion and money laundering if the recipients do not report their income.

Recently, CRA has encountered rings of professional money-launderers who earn their income from money laundering but who do not report or pay taxes on this income. In the medium to long term, CRA faces the risk of having to deal with more of this type of organization as the COVID-19 lockdowns have given criminals an opportunity to pursue new avenues of crime, to learn more about cybercrime, and to better organize their activities.

Canada's federal police, the Royal Canadian Mounted Police (RCMP), also indicates that the closure of casinos in Canada has seen increased reporting of underground illicit gaming activities and related money laundering activities. Reporting indicates that the price of methamphetamine and cocaine have increased across Canada. Cash stockpiling is believed to be occurring in Canada. Some organised crime groups also continue to conduct trade-based money laundering through grocery stores.

2) Has COVID-19 had any impact on the threats or vulnerabilities associated with TF?

- While it is relatively early to determine the extent to which COVID-19 has had an impact on the threats or vulnerabilities associated with TF, open source information indicates the following:
- Several reports have indicated an increase in fraudulent activities related to COVID-19. Hence, terrorist financiers can use the crisis to raise funds by moving into COVID-19 linked criminal activity.
- Extremists groups are known to organize online and adapt to a crisis. This adaptive behaviour can extend to their fund-raising activities amidst the pandemic. Therefore, going forward, there may be an increase in online criminal activity, charitable donations, crowdfunding through social media, or electronic payments for TF purposes, considering that these activities were already occurring online even before the pandemic. While analysing the online fund-raising landscape, special attention should be paid to right-wing extremist content, which has resulted

in hate speech against minorities during this pandemic, along with a distrust of government authorities.

- Terrorist groups, such as ISIS and Al-Qaeda (along with their affiliates), have continued attacks in weak states such as Iraq, Nigeria and Burkina Faso. They are taking advantage of these governments' preoccupation with the COVID-19 pandemic, and continue to engage in extortion activities locally. On the other hand, groups like Hezbollah are dealing with a financial crisis because they do not have enough funds to compensate their fighters who are now also involved in providing health-care services.
- [REDACTED]
- All the cases being worked by the Criminal Investigations Division (CID) of CRA, which may involve cases linked to TF, have been impacted in some way by the COVID-19 restrictions. [REDACTED]

3) Has COVID-19 impacted on the capacity of FIUs and reporting entities to detect ML/TF activity? What steps has your jurisdiction taken to respond to these challenges?

FINTRAC has continued to produce tactical and strategic intelligence since the beginning of the pandemic, [REDACTED]

[REDACTED] The average daily number of suspicious transaction reports (STRs) reported by reporting entities (REs) has remained relatively consistent and the COVID-19 pandemic does not appear to have had a significant impact on the overall volume of STRs received.

While COVID-19 has not had a significant impact on the overall volume of STRs, REs have experienced challenges associated with verifying client information, with clients citing COVID-19 as the reason for not being able to comply with the RE's requests for further information.

Recognizing that REs may face challenges in meeting their obligations due to COVID-19, FINTRAC, who is also the AML/CFT supervisory authority, has issued guidance to REs. The guidance highlights that REs should prioritize submitting STRs. FINTRAC is also offering additional support to REs by providing flexibility in verifying the identity of an individual, or confirming the existence of a corporation or entity other than a corporation (<https://www.fintrac-canafe.gc.ca/covid19/covid19-eng>). In addition to this guidance, FINTRAC will also issue a special bulletin on COVID-19, which highlights areas that may pose an increased money laundering risk associated with the exploitation of the pandemic

s.16(1)(c)

s.21(1)(a)

situation.

FINTRAC will also continue to work closely with AML/CFT regime partners and stakeholders, and is constantly assessing the situation in relation to COVID-19 to ensure that it can continue to protect Canadians and Canada's financial system, while respecting and supporting REs in these challenging times.

4) Has COVID-19 impacted on the capacity of competent authorities to investigate or prosecute ML/TF or impacted on judicial processes? What steps has your jurisdiction taken to respond to these challenges?

Judicial processes in Canada have been significantly delayed due to public closures.

Investigations continue, [REDACTED]

[REDACTED] Resumption of these activities is staggered across the country, but the overall negative impacts should be low.

Every jurisdiction in Canada has brought in measures to govern how the courts will function under the COVID-19 restrictions. These measures vary across the country; however, it is still possible to obtain judicial authorizations to obtain information. Active hearings have been adjourned to later dates, but judges have still rendered decisions, verdicts and sentences across the country, sometimes by telephone.

CRA has adapted its approach in each region, to comply with the rules put in place by that jurisdiction. The CRA's ability to investigate offences has been impacted by the COVID-19 restrictions. [REDACTED]

[REDACTED] CRA Officers will still accompany the police when they are executing search warrants on Joint Force Operations, but must first assess the safety of the situation, and will be sending fewer staff than in pre-COVID times.

CRA has also decided not to conduct in-person interviews with witnesses, unless appropriate safety measures can be put in place. Therefore, CRA developed a strategy to conduct video interviews.

CRA continues to obtain judicial authorizations for banking information, but has arranged to receive this information electronically and not by hard copy, as was done in the past.

In the past, some requests for information from third parties were sent by hard-copy letters with written signatures. CRA has adapted to send requests electronically, with digital signatures.

5) Has COVID-19 had any impact on operational level international cooperation (eg. mutual legal assistance, extradition and informal cooperation between FIUs and LEAs)? What steps has your jurisdiction taken to respond to these challenges?

COVID-19 has created challenges in the areas of extradition and mutual legal assistance in criminal matters (MLA). Canada's central authority for MLA and extradition (Central Authority), has taken steps to respond to these challenges and mitigate negative outcomes.

s.16(2)

s.16(1)(c)

Travel restrictions, both domestically and abroad, have impacted both extraditions and MLA matters.

The execution of MLA requests to serve persons in Canada with a summons or subpoena to attend court as a witness in a foreign proceeding are being postponed in light of existing travel advisories and restrictions. As an alternative to executing such MLA requests, the Central Authority has offered foreign partners the option of facilitating testimony via remote video link and, where that is not feasible, the Central Authority has encouraged foreign partners to reschedule proceedings until travel restrictions and other protective measures are lifted.

With respect to extraditions, the travel restrictions have caused delays in both incoming and outgoing surrenders. Physical distancing, as well as concerns about the health of those sought for extradition, have also played a role. We have been able to work with our treaty partners in delaying matters or extending deadlines so no cases have been terminated due to these circumstances.

Restrictions on access to the courts, both domestically and abroad, have also impacted both extraditions and MLA requests. However, this situation is improving as courts begin to ease restrictions on access and broaden operations to include a broader spectrum of cases, including non-urgent matters.

The process of commissioning affidavits and obtaining certifications, either in support of MLA court applications or to certify records produced on behalf of requesting states or in support of extradition requests, is currently challenging given social distancing protocols and the prevalence of remote work situations. Efforts are being made to develop solutions such as virtual commissioning of affidavits or certifications; however, it is unclear if these solutions will result in admissibility issues later on. We have experienced some delays in obtaining Internet Service Provider data from other countries due to office closures and lockdowns in foreign states.

The imposition of physical distancing requirements in domestic jurisdictions has caused delays in executing some types of MLA requests. For instance, the execution of incoming MLA requests that seek voluntary witness statements or testimony, or otherwise require contact with witnesses, suspects, etc. have experienced some delays because this generally requires Canadian law enforcement authorities to meet with the proposed witness in person in order to take a statement or have them sign documents provided by a foreign partner. This is also the case for incoming MLA requests that involve the service of documents on a party or involving the execution of search warrants.

At an operational level, FINTRAC has maintained strong relationships with international partners and continued to work effectively with other financial intelligence units (FIUs) regarding the prevention, detection, and deterrence of money laundering and terrorist financing activities despite the ongoing COVID-19 pandemic.

Since March 16, 2020 (the date of on-set COVID-19-related emergency orders in Ontario, the location of FINTRAC's national headquarters), FINTRAC has continued to provide

- 11 -

timely and actionable disclosures of financial intelligence to other FIUs in response to queries submitted to FINTRAC. In multiple instances, these disclosures were made in support of urgent law enforcement investigations that are ongoing in the recipients' jurisdiction.

Within the same time period, FINTRAC has maintained disclosures of financial intelligence to FIUs on a proactive basis at a level consistent with the pre-pandemic period when it was determined that transaction reports in the FINTRAC database would be relevant to the investigation or prosecution of a money laundering and/or terrorist financing offence or substantially similar offence in their jurisdiction. Furthermore, during this period of time, FINTRAC has regularly continued to send queries.

Informally, FINTRAC has also maintained direct contact with several FIUs during the pandemic period to discuss ongoing operational issues of concern for money laundering and terrorist financing activities between their respective jurisdictions and Canada.

CRA finds that COVID-19 has had some impact on international cooperation, but the impact appears to be minimal. CRA's CID investigators are still able to make Exchange of Information Requests through CRA's Competent Authority, and make MLA requests through the International Assistance Group at the Department of Justice. As most staff in all areas are working from home, both in Canada and in other countries, there may be some small delays in these international requests. However, requests have gone out to other countries since the COVID-19 restrictions have been put in place, and responses have been received. All staff have remote connections to the CRA's network and mainframe computers, so disruption has been minimal.

There is an outstanding MLA request where CRA asked a foreign government to conduct witness interviews. These interviews are on hold while the foreign government determines how to conduct these interviews safely.

The RCMP is a member on the Cross Border Market Fraud Initiative (CBMFI) which is an international task force dedicated to the identification and combatting of market fraud through cooperative enforcement and policy / legislative amendments. Since COVID-19, members within the initiative have been sharing information to enhance international cooperation surrounding Financial Crime related to COVID-19. Members of the CBMFI currently include Canadian Securities regulators and RCMP, as well as the SEC, FINRA, FBI, German Securities Regulator (BaFin), City of London Police, Australian Securities Commission (ASIC) and the Investment Industry Regulatory Organization of Canada (IIROC). This initiative has been in place for several years, however, given the recent activity, it has migrated to a bi-weekly call focussed on fraud-related market activity and COVID-19.

In British Columbia, the RCMP set up a COVID-19 Fraud Responses Team. The team focussed on identifying and addressing market / investment COVID-19 related scams / frauds as well as other COVID-19 related scams/fraud.

In Ontario, the RCMP set up a COVID-19 Joint Intelligence Group (JIG) with partner

agencies to identify and monitor COVID-19 related financial crimes / scams.

At National Headquarters, the RCMP Federal Policing set up a COVID-19 Strategic Task Force to address emerging threats and trends from COVID-19 and to manage and coordinate strategic analytical discussion and implementation efforts in support of identifying a way forward for RCMP Federal Policing during the COVID-19 crisis. The Task Force provides high-level coordination and guidance.

RCMP Federal Policing has been working collaboratively with Service Canada, CRA and Canadian banking institutions and other key partners regarding the alleged frauds surrounding the COVID-19 Canada Emergency Relief Benefit (CERB). The RCMP and the Canadian Anti-Fraud Centre (CAFC) are working with our partners and stakeholders on the analysis and alignment of our mitigation and disruption efforts to tackle this current threat.

6) Has COVID-19 impacted AML/CFT supervision or monitoring of compliance in your jurisdiction? What steps has your jurisdiction taken to respond to these challenges?

The COVID-19 pandemic has had a significant impact on the assessment activities undertaken by FINTRAC's AML/CFT supervisory function. [REDACTED]. All on-going assessments continued but had to move from the on-site model to the desk assessment model [REDACTED]. While any new on-site examinations were deferred, FINTRAC is currently working on a plan to resume activities, including on-site examinations.

7) Has COVID-19 impacted on asset confiscation and restraint processes? Has there been an impact on asset management? What steps has your jurisdiction taken to respond to these challenges?

Canada's asset management directorate has continued to be able to service Canadian law enforcement during COVID. From CRA's perspective, COVID-19 has had no impact on asset confiscation and restraint processes and asset management. There have been some delays in moving these cases forward.

s.16(1)(c)

s.21(1)(a)