Financial Transactions and Reports Analysis Centre of Canada | Centre d'analyse des opérations et déclarations financières du Canada

SAFE CANADIANS, SECURE ECONOMY | CANADIENS EN SÉCURITÉ, ÉCONOMIE SÛRE

Reference number: 20/21-SIRA-006

July 2020

Special Bulletin on COVID-19: Trends in Money Laundering and Fraud

The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) is committed to supporting reporting entities in managing their money laundering and terrorism financing risks during these unprecedented times. In addition to the guidance and temporary flexibility communicated by FINTRAC since March 25, 2020 (https://www.fintrac-canafe.gc.ca/covid19/covid19-eng), reporting entities should be aware of COVID-19 related money laundering trends and observations.

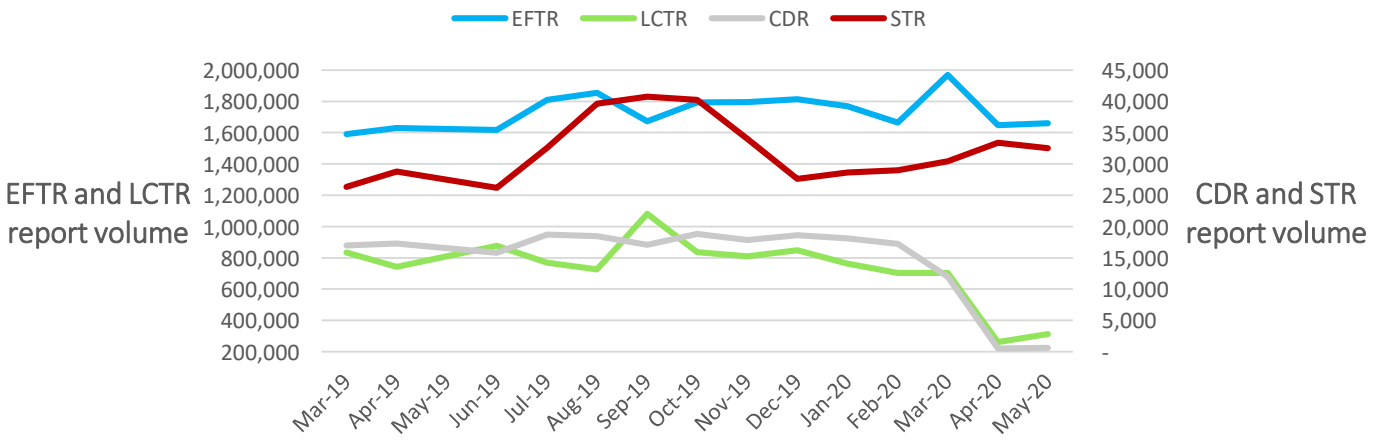
This special bulletin is based primarily on FINTRAC's analysis of COVID-19-related transaction reporting and the Canadian Anti-Fraud Centre's (CAFC) analysis of fraud reporting, and it highlights areas that may pose an increased money laundering risk associated with the exploitation of the pandemic situation.

TRENDS IN COVID-19 TRANSACTION REPORTING

Volume of Reporting

While the COVID-19 pandemic has not had a significant impact on the overall volume of suspicious transaction reporting (STR) and electronic funds transfer reports (EFTRs) received by FINTRAC, the volume of casino disbursement reports (CDR) and large cash transaction reports (LCTR) has significantly decreased beginning in March 2020.

Figure 1: Report volume by month (March 2019 to May 2020)



Document Number: 747029

Reference number: 20/21-SIRA-006
July 2020

The overall decrease in large cash transaction reporting is likely a result of the physical distancing and public health measures implemented in response to the COVID-19 pandemic, which has resulted in a general decline in cash transactions and business closures. While large cash transaction reporting in most activity sectors decreased, there was an increase (86%) associated with reporting from dealers in precious metals and stones in March 2020, when compared to the average volume over the last 12 months.

Given the closures of casinos and community gaming centres across Canada, there has been a very significant decrease in casino disbursement reports submitted to the Centre from March until the end of May 2020.

Observations in Suspicious Transaction Reporting

FINTRAC's analysis of suspicious transaction reports containing a reference to COVID-19 primarily highlights general suspicions of money laundering based on the nature of transactions conducted, as well as suspicions of the laundering of fraud proceeds. Financial intelligence units in other jurisdictions have reported similar findings.

The COVID-19 pandemic represents an unprecedented situation that may lead to unusual transaction activities. While many atypical patterns may reflect legitimate needs to access financial services during this challenging time, some individuals may attempt to profit from the current situation to undertake or facilitate money laundering. The COVID-19 pandemic, and associated closures and physical distancing measures, has disrupted some money laundering methods—particularly those that rely on the placement of illicit cash into cash-intensive businesses—and may expose criminal actors seeking alternate venues to integrate illicit proceeds into the financial system.

The characteristics of suspicious transaction reports related to COVID-19 highlighted below may not necessarily be indicative of money laundering, and must be examined in conjunction with additional risk indicators.

- The impact of COVID-19 provided as an explanation for:
  - Transaction activity that is atypical or not in-line with the client's financial profile.
  - Being unable to comply with reporting entity requests for further information regarding client financial activity.

- Individuals conducting transactions that appear at odds with the pandemic situation:
  - Large currency exchanges for unclear purpose, or for the purpose of travel that is not plausible given the COVID-19 pandemic.
  - Large cash deposits where the source of funds is unclear, or not plausible given the current pandemic situation.

- Transactions involving business accounts which appear at odds with the pandemic situation:

- Explanations for transactions deemed unlikely given the business profile and the anticipated impact of the COVID-19 pandemic on the operating model (e.g., restaurants, bars, gyms, travel industry, etc.).
- Unusual large cash deposits to business accounts, particularly in sectors most impacted by the COVID-19 pandemic or outside the norm for any business types.

➢ Activities which could be indicative of the laundering of proceeds from fraudulent activities or of an illegal attempt to profit from the pandemic:
- Unusual or suspicious transactions involving the sale or procurement of personal protective equipment or other medical or hygiene supplies that are in high demand due to the COVID-19 pandemic. Transactions may involve individuals seeking to purchase small quantities or large-scale procurement by institutions.
- Transactions that may be related to COVID-19 variations of existing mass marketing fraud schemes.
- Large cash withdrawals by individuals may be indicative of fraud victimization or the laundering of proceeds of fraud activities, often using mules who may have previously been victimized.

COVID-19 FRAUD TRENDS

FINTRAC's analysis of COVID-19 related transaction reporting and fraud reporting to the CAFC has revealed general COVID-19 related trends in money laundering and fraud, which are consistent with those identified as prevalent by international bodies and financial intelligence units in other jurisdictions.

The COVID-19 pandemic is having a significant impact on the global economy. Although it is still too early to determine if (or how) this pandemic will alter the money laundering landscape, the COVID-19 crisis has important implications for organized crime by creating significant new or expanded opportunities for the perpetration of fraud.

For example, it has created new opportunities for criminals in the virtual currency space in Canada and internationally. Counterfeiters have focused on selling fake COVID-19 home test kits and pharmaceuticals, and offering unconfirmed and often false advice on the treatment of COVID-19 on the Internet and the darknet, with transactions conducted using virtual currencies.

The increased use of online services during the pandemic also enhances the risk of cybercrime. Cyber criminals are exploiting the current situation to target individuals, businesses and entities with COVID-19 variants of popular phishing and blackmail scams, which are increasingly directing victims to send virtual currency for donations and ransom payments.

General trends observed in money laundering and fraud—including the increasing use of virtual currencies, the leveraging of mules (often the victims themselves) and the use of product and services offered by financial institutions—will likely continue for the laundering of COVID-19 fraud proceeds.

Financial Transactions and Reports Analysis Centre of Canada | Centre d'analyse des opérations et déclarations financières du Canada

SAFE CANADIANS, SECURE ECONOMY | CANADIENS EN SÉCURITÉ, ÉCONOMIE SÛRE

Reference number: 20/21-SIRA-006

July 2020

Summary of COVID-19 Fraud Reporting

COVID-19 has led to an increase in specific categories of fraud, which criminals have adapted from existing schemes. Reporting to the CAFC indicates an increased reliance on virtual currencies and traditional payment methods offered by financial institutions (i.e., credit card payments, eTransfers and wire transfers). Reports related to phishing schemes, identity fraud and merchandise scams, which account for 80% of the COVID-19 related fraud reported to the CAFC, are described below.

COVID-19 Merchandise Scams include offers for the supply of facemasks and other personal protective equipment (PPE) and COVID-19 test kits, unproven cures and treatments. Of the merchandise scams reported by victims to the CAFC, 62% relate to individuals buying facemasks and not receiving the product or receiving an inferior or counterfeit product; 18% relate to vendors selling all types of personal protective equipment (e.g., gowns, masks, gloves, sanitizers, etc.) and people not receiving anything at all or receiving inferior or counterfeit goods.

Indicators of COVID-19 Merchandise Fraud

- Merchants selling COVID-19 test kits, cures and treatments, and household decontamination services.
- Transactions involving the sale or procurement of personal protective equipment or other medical or hygiene supplies that are in high demand due to the COVID-19 pandemic, at significantly discounted prices.
- Customers providing payment through virtual currencies, or directing funds to an unrelated third party, especially those in a high-risk jurisdiction.
- Sudden onset and high volume of eTransfers into bank accounts of clients claiming to be involved in ecommerce (also known as electronic commerce or internet commerce). Funds are immediately depleted or forwarded to another account upon receipt.
- The use of personal bank accounts for business purposes, particularly those tied to ecommerce platforms.

Phishing scams include phone calls, emails and text messages from criminals pretending to be linked to Employment Insurance benefits, Canada Emergency Response Benefit (CERB), the Public Health Agency of Canada or other businesses. Victims are directed to click on a link or open an attachment, which may contain malware or may direct them to spoofed websites soliciting personal and financial information. The majority of the reports submitted to the CAFC tied to the identity fraud category relates to the victim's personal information being used to apply for the CERB payments.

Financial Transactions and Reports Analysis Centre of Canada | Centre d'analyse des opérations et déclarations financières du Canada

SAFE CANADIANS, SECURE ECONOMY | CANADIENS EN SÉCURITÉ, ÉCONOMIE SÛRE

Reference number: 20/21-SIRA-006

July 2020

Indicators of COVID-19 Identity and Emergency Benefits Fraud

- Sudden increase in large transactions involving customer accounts, where there was low balance and/or limited prior financial activity, or that direct payment to a beneficiary with whom the customer has no payment history or business relationship, may indicate fraud victimization or the laundering of proceeds from fraud activities.
- Recently opened CERB recipient accounts that lack the usual commercial transactions associated with daily living expenses.
- Bank accounts opened during the pandemic at a location that is not the customer's place of residence.
- The customer withdraws in full CERB payments deposited to the account or forwards the benefits to another account, immediately upon receipt of the benefits or after a period of inactivity.

As the pandemic continues, the CAFC expects that it is likely that the financial hardship faced by Canadian citizens and businesses will result in more victimization. Loan scams, debt consolidation frauds, and investment fraud will likely increase. Additionally, cyber dependent frauds such as spear phishing, ransomware and phishing campaigns that are taking advantage of the increased online activities (e.g. working from home) of Canadians, are also likely to increase.

Reporting to FINTRAC

For guidance on submitting suspicious transaction reports to FINTRAC, see Reporting suspicious transactions to FINTRAC.

Reporting to the Canadian Anti-Fraud Centre

www.antifraudcentre-centreantifraude.ca

Contact FINTRAC

- **Email:** guidelines-lignesdirectrices@fintrac-canafe.gc.ca (include Special Bulletin 20/21-SIRA-006 in the subject line)
- **Telephone:** 1-866-346-8722 (toll free)
- **Facsimile:** 613-943-7931
- **Mail:** FINTRAC, 24th Floor, 234 Laurier Avenue West, Ottawa ON, K1P 1H7, Canada

Cat. No. FD4-23/2020E-PDF
ISBN 978-0-660-35515-3

FINTRAC Special Bulletins provide information related to new, emerging and particularly topical methods of money laundering and terrorist activity financing. However, these Bulletins should not be considered legal advice. Please refer to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and its associated Regulations for the full description of the reporting entities' obligations.

Document Number: 747029