Fraud Trends Stemming from the COVID-19 Pandemic

Cameron Pyper, CPA, CA, CFE

nagel + associates
FORENSIC AND INVESTIGATIVE ACCOUNTANTS

In a memorable scene from the esteemed HBO crime drama *The Sopranos*, mob boss Tony Soprano is angry with his captains about their dwindling earnings, claiming that the recession is no excuse for poor financial results in their line of work. He rhetorically asks his consigliere, Silvio Dante, "…what two businesses have traditionally been recession-proof since time immemorial?". Silvio responds, "Certain aspects of show business, and our thing[1]".

While the developments of the last several months – a global pandemic, government-ordered closures, mass unemployment, civil unrest – have presented problems far more formidable than those of a typical recession for enterprises both criminal and legitimate, they have also provided fertile ground for fraud and other wrongdoing. Despite some underworld revenue streams being disrupted or completely drying up[2], such as sports gambling (due to professional leagues suspending their seasons), protection rackets (due to mandated business closures), and the drug trade (due to border restrictions), other opportunities have presented themselves for those willing and able to exploit them, suggesting that Silvio's argument holds true even in these extraordinary times.

This article addresses some of the recent fraud trends that have emerged over the past several months in Canada as well as in other parts of the world, because of COVID-19.

A Confluence of Circumstances

The coronavirus pandemic has created waves that have touched virtually all corners of the globe, giving rise to a convergence of many, often mutually exacerbating, developments, including:

Death and illness of loved ones	Stock market volatility
Widespread layoffs	Mandated business and school closures
Physical distancing requirements	Closed borders / other travel restrictions
Remote work arrangements	Critical shortages of certain goods

Collectively, these circumstances have created widespread uncertainty, fear, anxiety, instability, isolation, and desperation – precisely the sorts of conditions that opportunistic 'bad actors' can readily exploit[3].

[1] "For All Debts Public and Private." The Sopranos. (Season 4, Episode 1). HBO. Television.
[2] https://www.cbc.ca/news/canada/organized-crime-covid-1.5584645
[3] https://www.cbc.ca/news/politics/covid-scams-fraud-crime-1.5551294

According to the Canadian Anti-Fraud Centre (CAFC), Canadians reported losing $1.8 million to frauds related to COVID-19 between March 6 and May 25, 2020[4]. Like many attempts to quantify the pervasiveness of fraud, this figure is almost certainly understated, as frauds often go undetected, and even those that are detected often go unreported. Indeed, the CAFC acknowledges that what gets reported to them is "typically the tip of the iceberg"[5]. Notwithstanding, the extent and variety of frauds reported to date to the CAFC (and to other authorities) suggest a pervasive problem. In general, many of these frauds fall into one of five categories: product scams, investment scams, cybercrime scams, impersonation scams, and government scams.

Product Scams

Product scams include the sale of test kits, medicines, medical supplies, and other goods/services that are fake, substandard, exorbitantly priced, and/or never delivered. Organized crime groups are believed to be heavily involved in these types of scams[6].

According to the CAFC, reported frauds of this nature have included fraudsters posing as cleaning or heating companies selling decontamination services, duct cleaning, or air filters that purportedly protect against the coronavirus. The CAFC has also received reports of questionable testing kits or remedies that in many cases are ineffective[7].

In British Columbia, an investigation by the RCMP and Health Canada resulted in over 1,500 illegal COVID-19 testing kits being seized[8], while Toronto Police made an arrest following an investigation conducted alongside American authorities, in connection with prohibited COVID-19 testing kits being shipped across the Canada-U.S. border[9].

Product scams appear to be a worldwide concern amid the pandemic. For example, a Europol report on how COVID-19 will affect European crime trends cites "…the trade in counterfeit and substandard goods" as one of the most prominent developments that they have observed[10]. Moreover, it is a trend that they anticipate to continue in the medium term (with an expected proliferation of counterfeit vaccines) as well as the long term (with an expected recession-spurred increase in demand for cheaper products)[11].

---

[4] https://www.antifraudcentre-centreantifraude.ca/index-eng.htm
[5] https://www.cbc.ca/news/canada/organized-crime-covid-1.5584645
[6] Ibid.
[7] https://antifraudcentre-centreantifraude.ca/features-vedette/2020/covid-19-eng.htm
[8] https://www.citynews1130.com/2020/04/30/1500-unauthorized-covid-19-test-kits-seized/
[9] https://torontosun.com/news/local-news/toronto-man-charged-with-fraud-over-covid-19-test-kits
[10] https://www.europol.europa.eu/publications-documents/beyond-pandemic-how-covid-19-will-shape-serious-and-organised-crime-landscape-in-eu
[11] Ibid.

Mitigating the Risk of Product Scams:

- **Purchase only from reliable sources**
- **Assess price against the prices of comparable goods or services**
- **Be skeptical of claims about products that seem too good to be true**
- **Perform online searches for customer reviews of companies and products before making purchases**

Investment Scams

Investment fraud and other financial services schemes have also been a widespread problem during the current crisis.

In April, the Ontario Securities Commission (OSC) and the RCMP's Integrated Market Enforcement Team (IMET) issued a joint warning about pandemic-related investment scams, including cases in which investors have been approached by companies claiming to offer methods of preventing, detecting, or curing COVID-19. They also warned about aggressive stock promotions and 'pump and dump' schemes in which false or misleading information (including about potential cures, remedies, or tests) may be disseminated to artificially inflate stock prices[12].

Similarly, the CAFC has issued a warning about fraudsters posing as financial services companies or financial advisors and offering loans or debt consolidation or promoting certain investments[13].

According to Torys LLP, both Canadian and American securities regulators are actively pursuing companies that have made inaccurate disclosures relating to COVID-19-related goods/services such as therapeutics, vaccines, or personal protective equipment, as well as companies that have attempted to hide existing financial problems by falsely representing them to be related to the pandemic[14].

[12] https://www.osc.gov.on.ca/en/NewsEvents_nr_20200423_osc-rcmp-issue-joint-warning-on-coronavirus-investment-scams.htm
[13] https://antifraudcentre-centreantifraude.ca/features-vedette/2020/covid-19-eng.htm
[14] https://www.torys.com/insights/publications/2020/05/cracking-down-on-covid-19-fraud-us-and-canadian-securities-regulatory-enforcement-update

Mitigating the Risk of Investment Scams:

- **Perform due diligence before making investment decisions**
- **Make sure the business you are dealing with is regulated and/or licensed**
- **Be wary of businesses based overseas**
- **Be skeptical of those who aggressively promote certain investments**

Cybercrime Scams

Cybercrime is another area that has been – and is expected to continue to be – an area of focus for the criminal element looking to take advantage of the pandemic. Cybercrime can be carried out through various means, including emails, text messages, and illegitimate websites, usually for the purpose of obtaining money, personal information, or both[15].

Victims of such schemes have been induced to open email attachments, click on links in text messages, visit websites, or perform other similar actions by fraudulent communications relating to the pandemic. These include 'phishing' emails and other messages indicating that recipients have been exposed to a person who tested positive or instructing them to click on a link or provide personal information in order to collect government benefits[16].

Mitigating the Risk of Cybercrime Scams:

- **Do not open attachments or click on links from texts or emails unless you are certain that they are from a trusted source**
- **Check the sender's email address**
- **Check email content for spelling and grammar errors**
- **Be leery of any requests for personal information – do not respond unless there is a legitimate reason why the information is required AND you trust the entity to which you are providing the information**

[15] https://www.cbc.ca/news/canada/organized-crime-covid-1.5584645
[16] https://www.cbc.ca/news/politics/covid-scams-fraud-crime-1.5551294

Impersonation Scams

There have also been numerous reports of fraudsters pretending to be charities, government agencies, or other authorities, in order to obtain funds and/or personal information from unsuspecting victims. Such impersonations may be part of the types of cybercrime-related schemes described above, or they may be a unique category of schemes altogether.

The CAFC has received reports[17] of fraudsters posing as:

- public health authorities offering fake information relating to infections in a given neighbourhood or personal test results, and then soliciting personal information;
- charities seeking donations under false pretenses;
- utility companies threatening to disconnect services if payments are not made; and
- government departments asking for personal information.

In addition to the above, there have been reports of 'job scams' in which criminals pose as employers offering work-from-home employment – an enticing proposition for many, given the prevalent unemployment and stay-at-home orders – and request money or personal information as part of the purported job application[18].

The OSC has also warned about similar types of impersonation schemes, including ones in which fraudsters are posing as banks, financial advisors, prospective employers, or government departments/agencies, in an attempt to obtain financial or personal details[19].

Mitigating the Risk of Impersonation Scams:

- **Verify the identity of parties representing themselves to be agents of the government or other authorities, and corroborate claims that they make**
- **Be skeptical of any requests for personal information or payments**

[17] https://antifraudcentre-centreantifraude.ca/features-vedette/2020/covid-19-eng.htm
[18] https://www.cbc.ca/news/canada/organized-crime-covid-1.5584645
[19] https://www.osc.gov.on.ca/en/NewsEvents_nr_20200423_osc-rcmp-issue-joint-warning-on-coronavirus-investment-scams.htm

Government Scams

In the wake of the pandemic, governments have been hurrying to provide financial support to people and businesses, as well as trying to procure the necessary testing kits, medical supplies, and personal protective equipment. While both measures are much-needed, they also create areas that crooks can abuse, including by claiming financial relief or other benefits to which they are not entitled, and by setting up companies to source and re-sell needed supplies and equipment at excessive mark-ups. For example, a Virginia man was recently charged with submitting fraudulent loan applications to take advantage of emergency financial relief provided by the CARES Act[20].

In response to concerns about support programs being abused, the Canada Revenue Agency recently opened up a 'snitch line', which provides a mechanism for people to report information relating to individuals who are receiving the CERB or CESB despite not being eligible, or businesses that are misusing the wage subsidy program[21].

Possible Future Trends

As governments continue to ease restrictions and businesses and institutions begin to open up again, many of the aforementioned problems will persist, and several others will likely present themselves.

Financial difficulties are likely to continue for many individuals and businesses, as continued mandatory closures, concerns about subsequent 'waves' of the coronavirus, strained financial resources, and other factors will cause some employers to be slow to rehire and reopen. Many customers and tenants that have been able to defer or reduce credit card, loan or rent payments temporarily, or that have only been able to meet such obligations with funds from government support programs, will find it difficult to make ends meet when such concessions or support programs are phased out. These problems will only be exacerbated when landlords begin to evict and lenders begin to call loans with greater frequency and zeal than they have in the last few months. All of which is to say that financially speaking, the worst of this crisis may not be behind us.

[20] https://www.justice.gov/usao-edva/pr/man-indicted-covid-19-related-loan-fraud
[21] https://www.canada.ca/en/revenue-agency/programs/about-canada-revenue-agency-cra/suspected-tax-cheating-in-canada-overview.html

Such ongoing financial difficulties may give rise to a number of conditions that criminals and other unscrupulous opportunists can take advantage of. For example, struggling companies may feel compelled to scale back or eliminate certain 'non-revenue-generating' activities, such as internal audit, control, and compliance functions, thereby leaving themselves vulnerable to fraud at a time when bad actors, both internal and external, may be looking to defraud them.

These types of cost-cutting measures can lead to shortcuts being taken, standard procedures being bypassed, and financial information being misrepresented[22], all of which create risks for the organization. The trend of working from home, which is expected to continue for many office workers, may also make some of these negative outcomes more likely.

Recent economic conditions may also lead to more risk aversion, both for individual investors as well as financial institutions[23]. This may make it more difficult for businesses to obtain financing through traditional avenues, which may lead them to turn to other financing sources, including those looking to exploit them. Such sources include criminal groups, which may be looking to buy or lend money to struggling businesses[24], given that legitimate businesses offer organized crime groups a means of laundering proceeds of crime, demonstrating legitimate earnings, and carrying out further criminal activity.

In fact, Italian police recently arrested 91 suspected mobsters who were allegedly involved in laundering proceeds of their extortion and drug trafficking operations by purchasing failing businesses affected by the COVID-19 lockdown[25].

Desperation may also lead otherwise honest employees and businesses to carry out fraud against their employers, vendors, customers, or insurers, which could lead to increases in payroll fraud, procurement fraud, expense report fraud, benefits fraud, financial reporting fraud, and insurance fraud.

[22] https://www.corporatecomplianceinsights.com/fraud-covid-19-targeted-response/
[23] https://www.cbc.ca/news/business/pittis-risk-covid19-new-era-1.5544090
[24] https://www.cbc.ca/news/canada/organized-crime-covid-1.5584645
[25] https://www.cbc.ca/news/world/italy-coronavirus-covid-mafia-arrests-1.5565793

Another trend that is expected to continue in the near future is ongoing growth in online retail transactions, contactless purchases, and digital wallets. Stores and restaurants that were a short time ago primarily or exclusively physical businesses are rapidly adapting to offer online ordering[26]. These changes in how consumers are making purchases are expected to give rise to upticks in chargeback fraud (in which customers claim goods were not received and request refunds through their credit card company) and account takeover (in which a customer's online account is taken over by someone else)[27].

While nobody can be sure what the future holds, past experience and current trends would appear to suggest that crooks will continue to look for ways to use worldwide uncertainty and instability to their advantage.

About Our Firm

nagel + associates is a Toronto-based boutique forensic accounting firm that focuses exclusively on Forensic Accounting, Investigations and Disputes, Anti-Fraud Training, Anti-Fraud Consulting and Crypto Advisory. For more information about our services, please visit nagel-forensics.com.

[26] https://www.oliverwyman.com/our-expertise/insights/2020/apr/payments-shifts-with-covid-19.html
[27] https://www.forbes.com/sites/louiscolumbus/2020/05/18/how-e-commerces-explosive-growth-is-attracting-fraud/#aa691466c4b9