

# Insurance Fraud in Times of Crisis

COVID-19 Pandemic–Related Risks in the P&C  
Insurance Industry

October 2020 | Fall Update



## Introduction

Historically, fraud comes to the front in times of widespread economic hardship and natural disaster. The COVID-19 pandemic presents both of these factors because it has caused economic malaise that rivals the disastrous effect it has had on the lives of the thousands who have contracted the virus. As if this were not enough, the insurance industry has an additional challenge to consider: an increased likelihood of insurance fraud.

In this update to the original report from May 2020, Insurance Bureau of Canada (IBC) takes stock of the insurance fraud landscape six months into the COVID-19 pandemic. The updated report provides an in-depth look at Canada's dismal economic performance across Q2-Q3 2020 and connects macro-level indicators to the factors that increase the likelihood of fraud, to suggest why insurers should be particularly concerned about fraud at this time.

In addition to retaining all relevant content from the original report, this update provides a deeper analysis of two pre-existing threats that have taken on greater importance in our new, remotely connected world: cyber-attacks and telemedicine fraud. The report also highlights auto theft/owner give-ups and real estate development fraud as threats requiring continued attention. The report concludes by highlighting some silver linings for property and casualty insurers that could come out of this crisis. Particularly, IBC believes that the industry could emerge from the COVID-19 pandemic with improved data sharing and towing regulations, notably in Ontario.

## Fraud in Recessionary Times: Canada's Economic Update

While consumer response to an economic downturn varies depending on the recession's characteristics – for example, what caused it and how long it lasts – previous downturns can shine light on how some may respond to the financial strain caused by this pandemic, and how we can expect them to behave should the economy fail to make a sharp, V-shaped recovery.

Historically, insurance crimes have increased when the economy is in decline. In fact, even with lower aggregate claims volumes, the proportion of cases being referred to internal special investigation units (SIUs) tend to noticeably increase during recessions. Insurance regulators also see increased referrals. During the Great Recession of 2008–09, the Florida Division of Insurance Fraud reported a 21% increase in referrals compared to the previous year. British regulators indicated that they also experienced a nearly 10% increase in all frauds throughout 2009, with false insurance claims acting as one of the primary drivers behind this increase. The preliminary evidence suggests that insurers are seeing the same pattern during the COVID-19 pandemic.

PwC found that while the incidence of economic crime during recessions varies by country, some industries, including insurance, tend to report higher levels of fraud than others. PwC's 2018 Economic Crime Survey found that "instances of fraud tend to rise in times of economic downturn" as a result of increases to the following three factors that make up the Fraud Triangle:

1. Incentives or pressure to commit fraud
2. Opportunities to commit fraud
3. An ability to rationalize one's decision to commit fraud.

As shown in Figure 1, most survey respondents indicated that a greater level of financial pressure drives up the risk that they will experience fraudulent activity during a recession. Losses from fraud, on top of decreased investment income and potential reductions in consumers' insurance needs resulting from new driving habits, could be financially impactful for insurers during the COVID-19 pandemic.

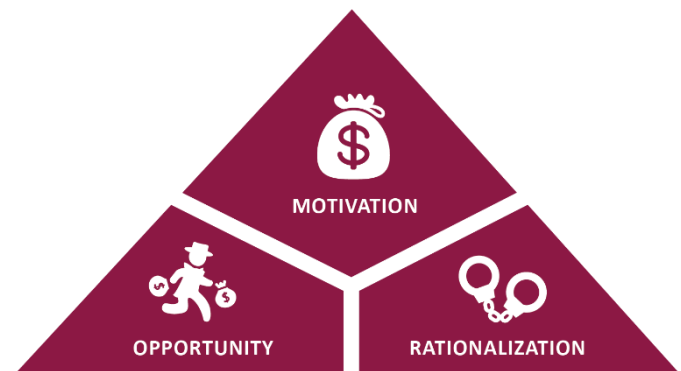


Figure 1 - Fraud Triangle

### Current Economic Overview

No country is immune to the economic toll the pandemic has taken. According to the International Monetary Fund, the global economy will contract by 4.9% in 2020. However, this contraction is unevenly distributed, with some national economies facing significantly more strain than others. Unfortunately, Canada is one such nation. According to Statistics Canada, real gross domestic product contracted at an

annualized rate of 38.7% in Q2 as the COVID-19 pandemic forced the closure of non-essential businesses and slowed the economy to a crawl, making it the steepest three-month decline on record.

While the correlation between the state of the economy and crime rates is not as clear in Canada as it is in Britain or the United States, research supports a consistent relationship between unemployment and increased property crime, particularly when high unemployment rates are sustained. As such, the pressure the pandemic places on crime rates will heavily depend on how quickly laid-off workers are called back to work or can find new employment. This could prove problematic; while Statistics Canada reported the country added 378,000 jobs in September, it remains approximately 720,000 jobs (-3.7%) short of pre-pandemic levels. Statistics Canada also noted that employee compensation fell a record 8.9% since the pandemic hit, as a result of job losses, layoffs and reductions in hours.

Considering that half of Canadians were reported by consulting firm MNP to be within \$200 of monthly insolvency, many Canadians are experiencing financial strain. While the full effects of this pressure have been palliated somewhat by governmental support schemes, such as the Canada Emergency Response Benefit (CERB) and Canada Emergency Commercial Rent Assistance (CECRA), it is unclear what might happen once these programs cease to be available. The CERB, for instance, paid over \$71 billion to nearly 8.67 million Canadians throughout the pandemic; however, this benefit was terminated on October 3, 2020.

## COVID-19: Opportunities for Fraud and Abuse

While the industry has dealt with many crises, the resulting scams were most often targeted at specific lines of insurance. The COVID-19 pandemic is different from past crises in that it crosses all lines of general insurance, including home, auto and commercial. This is in addition to the pressures that life and health insurers and the workers' compensation system are already facing.

As insurers are adapting to their new operational realities, fraudsters may presume decreased vigilance and view the crisis as an opportunity to profit. With limited resources to fight fraud, insurers should focus their attention on specific areas that are likely to produce scams.

As policyholders' financial situations deteriorate, the industry may see an increase in opportunistic fraud. Some of the scams that people have already been caught running and those that are likely to materialize in the near future include:

- Fraudulent auto thefts (known as owner give-ups) due to the inability of the owner to finance the vehicle; in particular, ride-sharing operators may report their vehicles as stolen because of a significant decrease in demand for their services
- Arson, particularly of detached garages or sheds, to generate an influx of cash



- Water damage claims, which (unlike arson) do not require investigation from first responders, draw significantly less attention from witnesses, and lack available forensic specialists to determine exact cause and origin.

Beyond opportunistic fraud, organized crime entities have already found ways to profit from the pandemic. IBC and industry investigators identified the following scams in the early days of the pandemic:

- Body shops, preying on consumers' fear of contracting COVID-19, charging exorbitant fees for cleaning vehicles and storing the vehicles for several days before commencing repairs (in the past, body shops in Western Canada have used a similar scam based on fears about synthetic opioids)
- Alleged hit and runs (i.e., no third-party information), where the damage is not consistent with the facts of loss
- Car rental agencies failing to accept returns, including drop-offs, thereby increasing rental costs
- Increased incidences of staged collisions, with policyholders citing the fear of contracting the virus as the reason they failed to remain at the scene, go to the hospital or promptly report the "accident"
- Additional "jump-ins" on collision claims, which is when people not in the vehicle at the time of the collision make a claim, as fraudsters may capitalize on others' anxieties and suggest a limited exchange of information, including passenger names.

IBC is urging insurers and commercial enterprises to exercise heightened vigilance regarding the threat of cargo theft. In its initial report, while this has yet to be borne out in the data, IBC noted that lockdown orders could drive up the rate of cargo theft, particularly of parked trailers in holding yards, given the inability to receive shipments. While this threat has somewhat abated as the economy has reopened, it remains a concern and will only grow more likely as major Canadian cities experience subsequent waves of COVID-19.

## **New Realities, New Opportunities for Fraud**

In its initial report, IBC warned insurers of what they could expect as we entered an unknown reality defined by COVID-19. Now that we have marked the six-month anniversary of the pandemic declaration, we have a clearer understanding of the avenues that fraudsters have been exploiting since March 2020. Two of the most prominent and novel are cyber scams and telemedicine.

### ***Cyber Threats***

As economies and communities locked down, fraudsters started, almost immediately, to capitalize on the fact that our personal and professional lives became even more dependent on the internet. Much like the coronavirus, cyber scams move quickly and can affect large geographic areas in a short time. Unfortunately, Canadians seem to be particularly vulnerable to cyber attacks. A report from technology company Dell noted that in the first quarter of 2020, an astounding 66% of all global phishing attacks were targeted at Canadians. The next closest country faced a mere 7% of total phishing attacks. And, according

to IBM, Canada's security breaches are the third most costly in the world, at over 1.2 times the global average cost.

While phishing attacks remain the most common form of cyber attack, Interpol has identified a full suite of cyber-related threats posed by the COVID-19 pandemic.

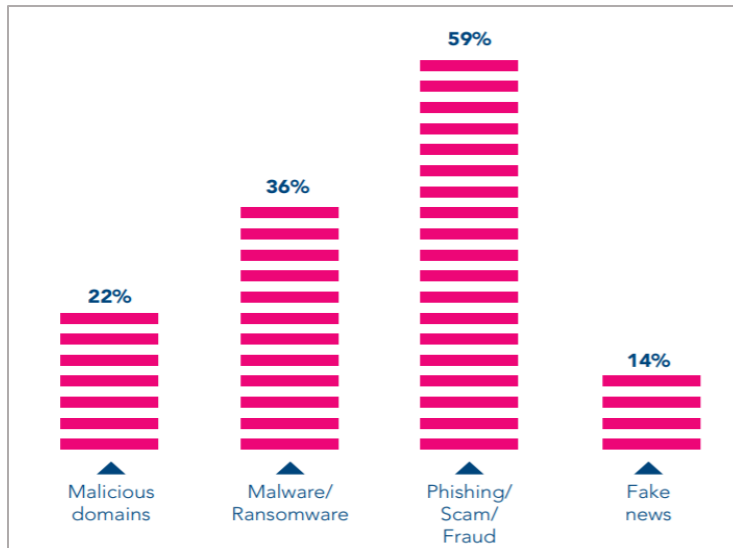


Figure 2 - Distribution of Cyber Threats Reported to Interpol

According to one U.S. study, ransomware attacks increased by 109% and totaled 121 million incidents during the first half of 2020. As shown in Figure 2, businesses have clearly taken note of this acceleration, and ransomware attacks are now identified as the main cyber threat by 36% of Interpol member countries. According to Beazley Breach Response, financial services and health care remain the two most heavily targeted industries for cyber attacks, and in late August the insurance industry was indirectly impacted by a ransomware attack. On August 19, ICS Courier, used by some insurers and brokerages, suffered a ransomware attack that interrupted mail

pick-up and delivery services which resulted in consumers' insurance coverage being at risk. Additionally, the insurance brokerage Arthur J. Gallagher suffered a ransomware attack on September 26. It is unclear whether any customer data was stolen.

While commercial operations are most at risk of a ransomware attack by virtue of their ability to secure the funds needed to pay the ransom, cyber criminals have not turned a blind eye to the vulnerability of ordinary citizens. In some European countries, Vodafone's internet usage has surged around 50%, meaning there are potentially more opportunities for the public to be susceptible to fraudsters. Unfortunately, [a recent Chubb cybersecurity survey](#) shows that only 46% of respondents were concerned about their cyber security while working remotely. Cyber criminals, however, are aware of this decreased vigilance as according to Bitdefender, the number of digital attacks in March was at least 475% higher than those in February. Moreover, other experts have noted that the attacks are taking new forms. For instance, there has been a 176% increase in attacks with malware disguised as Microsoft Office files.

And while it's a best practice to use a corporate VPN for work, it is no panacea. A cyber crook recently exploited a vulnerability and posted the IP addresses of over 900 corporate VPNs online. Anyone with access to the list could use the information to gain internal access to those networks.

Though harmful to a business of any size, cyber attacks can be particularly crippling to small and medium-sized enterprises (SMEs). IBC [surveyed](#) SMEs last fall, and 44% said they had no cyber crime defences,

while 37% estimated that incidents would cost them more than \$100,000. Nearly two-thirds of survey respondents said they had no cyber insurance coverage at all.

It is highly unlikely that the cyber threat will recede anytime soon. Interpol predicts that cyber crime will increase as COVID-19 persists, and that criminals searching for new revenue streams as a result of lockdown orders may view cybercrime as offering “easy entry” into new forms of criminality.

### ***Telemedicine***

As a health care crisis first and foremost, it is no surprise that COVID-19 would quickly generate an uptick in medical billing fraud and abuse. As early as April, Verisk claimed that its data showed a 14% increase in claims linked to providers with suspicious billing practices, suggesting that fraudsters were ready to capitalize on the commotion. There is a high risk that the pandemic is generating new opportunities for fraud that are a function of our new, physically distant reality. One such opportunity is in the increased uptake of telemedicine.

Telemedicine involves health care services provided via phone or video in lieu of in office visits. While it has proven to be an invaluable tool for doctors and patients during the pandemic, long thought-out regulations risk being relaxed, which could potentially usher in an era of remote medical fraud. According to the Coalition Against Insurance Fraud, the process has already begun in the United States. While telemedicine accounted for just under \$20 billion in health care charges last year, it is expected to grow to \$65 billion by 2025 due to COVID-19. This growth trajectory is troubling, as despite its modest size, telemedicine has already enabled some of the largest insurance scams in US history; in fact, two fraud cases have exceeded \$1 billion each.

Telemedicine fraud is more difficult to identify and investigate than traditional medical fraud, and it will eventually become tougher to litigate. This tends to be the result of the same factor: geography. Geographical factors pose challenges with respect to serving legal documents such as subpoenas, but they also have a more practical impact in that it is tougher to get boots on the ground to investigate a claim and interview the parties involved. Moreover, its virtual nature means an insurer cannot conduct surveillance on a telemedical operation as it would on a bricks and mortar clinic, which makes validating billing more challenging. As COVID-19 ushers in a new, increasingly digital reality, having an open line of communication with policyholders is more important than ever, as is having state-of-the-art analytical capabilities.



## Auto Theft Claims and Real Estate: Continue Monitoring

IBC warned members in its original report to look out for various types of fraud that were likely to materialize as the pandemic progressed. Six months into the pandemic, the evidence suggests that opportunistic actors have attempted to defraud insurers through some of these identified scams, most notably through vehicle-owner give-ups.

IBC is aware of at least two cases in which multiple vehicles were reported stolen from the same driveway on the same evening, and that have been the subject of SIU or law enforcement investigation, or both, as a result of substantial concerns regarding the veracity of the claims. Vehicle theft remains an area where IBC advises members to exercise additional caution. If you have access to the key fobs of the vehicle at issue, IBC's new KeyReads service could be of assistance in ascertaining whether a theft actually took place.

The original report also identified how recessions have previously impacted commercial lines specifically. While the data suggests that fraudulent activity spiked in the commercial sector after the 2008 recession, for this crisis IBC suggested focusing on food spoilage claims given the challenges COVID-19 posed to the food and hospitality industry. However, restaurants are not the only commercial enterprises under strain at this time. The manufacturing and construction industries have been among the hardest hit, the latter of which will now be discussed.

The COVID-19 pandemic has seen a record number of Canadian commercial bankruptcies. Under the creditor protection process, a record 12 companies began proceedings in June, which is significantly higher than the 10-year rolling average of three proceedings per month. In total, 27 major Canadian companies (those that owe over \$5 million) have been granted creditor protection since COVID-19 was declared a pandemic in March. Many proprietors do business with very low margins, and losing a client through bankruptcy caused by COVID-19 financial pressures could put them into dire straits, especially if they lack trade credit insurance.

Additionally, experts in insolvency predict that real estate development could be the next domino to fall. Of the 27 companies granted creditor protection since the beginning of the pandemic, nine are connected with the real estate development sector. In the absence of further government action, such as the extension of the CECRA program, it would not be surprising to see an uptick in fraudulent directors and officers (D&O) and errors and omissions (E&O) claims emanating from this sector in the near future.

It is important to remember that a denied claim does not mean that an individual is done with the insurance process. For instance, a client may submit a business interruption claim that is denied, but then quickly follow it with a suspicious water or fire claim, or some other type of loss that is covered by their policy. While the vast majority of policyholders are honest and trustworthy, verification is essential.

## Silver Linings?

While the pandemic has posed many challenges, IBC is optimistic that some positive changes will come out of the current crisis. While a number of COVID-19–induced shifts will be temporary, we suspect that other, more fundamental shifts are here to stay. The two positive changes that might be here to stay are wider data sharing between insurers and towing reform.

### Data Sharing

Even in privacy-conscious Western nations, people have seen the value in making a small sacrifice for the collective good. Canada’s “COVID Alert” app has been downloaded over 4.7 million times, and in Norway, 25% of the population downloaded the government’s COVID-19 app in just a few days. Apparently, many people are willing to play an active role to prevent the spread of the virus and to share some of their personal data because it provides substantial benefits. It proves that reciprocity helps solve the privacy issues that consumers have with sharing data. We at IBC certainly hope this could be indicative of consumer and government willingness for insurers to share data for the limited purposes of detecting, preventing and suppressing insurance fraud.

One potential avenue could be through the consultation [announced](#) by the Ontario government on August 13, 2020, regarding the modernization of the province’s privacy law regime. One of the matters to be considered in this consultation is whether Ontario should develop its own private sector privacy law, which would apply instead of the federal Personal Information Protection and Electronic Documents Act (PIPEDA) if the federal government were to be deemed substantially similar. Under the coordination of the Ontario Committee, IBC’s Privacy Working Group has crafted a submission that seeks to advance the industry’s work on anti-fraud data sharing, among other things. IBC is encouraged by the language being used by the government, particularly regarding the need for clarifying consent requirements (including exceptions to consent) and the importance of balancing privacy laws with the need to enhance innovative services for the public good. In our view, steps made to improve insurers’ fight against fraud are invariably in the public interest.

That said, IBC has made clear to the Ontario government that the private sector would prefer that the Ontario government, at the very least, wait to see the federal government’s long-awaited PIPEDA reforms before proceeding with any new provincial law. IBC has instead asked the government to raise its recommendations to help with fraud detection and prevention with the federal government at the appropriate time.

## Towing Reform

In early June, the Assistant Director of the FBI appeared before a U.S. Congressional committee to testify about the importance of public-private sector collaboration in the fight against insurance fraud. He applauded the important work being advanced by private industry, noting how “relationships with the private sector have allowed us to more efficiently and effectively address many of the fraud schemes that have emerged since the beginning of the COVID-19 pandemic.”

Law enforcement agencies in Canada are also being reminded of the value that a private industry perspective can bring to problems of public safety. Most recently, IBC and industry’s joint involvement in York Regional Police’s Project Platinum helped investigators refine their investigative plan, ultimately leading to the arrest of 20 people and the laying of nearly 200 charges related to a towing crime ring. The conservatively estimated insurer benefit of shutting down that towing crime ring is between \$1.2 million and \$4 million industry-wide.

As a result of the escalating violence and media attention associated with towing fraud, the Ontario government [announced](#) on June 29, 2020, the creation of a task force focused on improving the province’s towing industry. The cross-ministerial task force, jointly led by the Ministry of Transportation and the Ministry of the Solicitor General, will deliberate internally prior to conducting a public consultation. IBC has reconstituted its Towing and Storage Working Group, and the group has shared its submission with the government. The submission contains proposals organized around three key themes:

1. Ending “chasing,” including through provincial oversight
2. Strengthening consumer protections
3. Implementing stronger enforcement provisions.

Premier Doug Ford has publicly expressed his displeasure with the current state of affairs in the towing industry, and IBC is confident that legislation – including provincial oversight – will be in place by the end of 2020. It should be noted that this was one of the key recommendations IBC, at the direction of the Industry Insurance Crime Advisory Group (IICAG), presented to the Ontario government across various meetings last year.

## Conclusion

The COVID-19 pandemic threatens the physical and financial health of consumers and organizations alike. Unfortunately, it also represents an opportunity for fraudsters to profit at the expense of insurers and their honest policyholders.

As we continue to navigate the uncertainty that the pandemic brings in the months ahead, collaboration will become more important than ever. Sharing information and strategies, as this report does, is one of the sharpest tools we have in the fight against fraud. IBC will continue to monitor the pandemic's influence on fraud trends and inform members of any new schemes and best practices as it becomes aware of them.