April 18, 2020

Combatting Civil Fraud Against Businesses in the Age of COVID-19

Fraud is a fact of business life. Most businesses are only partially prepared to address fraud. Even fewer are ready for what is necessary to seize and recover assets from perpetrators of fraud. These gaps often cause serious business losses. The trend over the past decade toward increasing fraud and money laundering has been accelerated by the COVID-19 pandemic. The focus all businesses must now put on managing the crisis will lead to significant vulnerabilities and increased losses due to fraudulent activity.

While most business fraud goes unreported, the federal government's Canadian Anti-Fraud Centre reports that about 20,000 Canadians were victims of fraud in 2019 with losses in the range of $100 million. These consumer-fraud statistics are the tip of the iceberg and do not include the significant and massive frauds suffered by public and private companies.

The numbers for business are staggering. According to PWC's 2020 report into global fraud (the "PWC Report"), businesses reported US$42 billion in total fraud losses globally (Fighting fraud: A never-ending battle (PwC's Global Economic Crime and Fraud Survey). Nearly half of companies surveyed suffered at least one fraud. The average number of frauds were six per company. Despite this, according to the PWC Report, only 56% of businesses conducted an investigation into their worst fraud incident.

Businesses with anti-fraud strategies drastically increase the chances of controlling and uncovering fraud. Businesses with strong due diligence, governance, and compliance programs dramatically increase their chances of asset recovery. These strategies have become imperative for business survival in the pandemic era.

Fraud Trends During COVID-19

Traditionally, internal employee, supplier, and vendor fraud often corresponds with a personal or business crisis, such as a significant financial loss or personal medical issue. These issues often lead to asset misappropriation, which is one of the leading types of fraud across all business sectors. These traditional triggers for fraud have been exacerbated by COVID-19.

Customer fraud is also on the rise as businesses move toward direct-to-consumer strategies. COVID-19 has given this trend a shot of adrenaline.

In addition to traditional cybercrime attacks, phishing attacks, and related scams, all of which are on the rise, the Canadian Anti-Fraud Centre has reported the following COVID-19 related scams:

- Loan and financial service companies
    - offering loans, debt consolidation and other financial assistance services
- Cleaning or heating companies
    - offering duct cleaning services or air filters to protect from COVID-19
- Local and provincial hydro/electrical power companies
    - threatening to disconnect your power for non-payment
- Centers for Disease Control and Prevention or the World Health Organization
    - offering fake lists for sale of COVID-19 infected people in your neighbourhood

- Public Health Agency of Canada
    - giving false results saying you have been tested positive for COVID-19
    - tricking you into confirming your health card and credit card numbers for a prescription
- Red Cross and other known charities
    - offering free medical products (e.g. masks) for a donation
- Government departments
    - sending out coronavirus-themed phishing emails
    - tricking you into opening malicious attachments
    - tricking you to reveal sensitive personal and financial details
- Financial advisors
    - pressuring people to invest in hot new stocks related to the disease
    - offering financial aid and/or loans to help you get through the shut downs
- Door-to-door sales people
    - selling household decontamination services
- Private companies
    - offering fast COVID-19 tests for sale
        - Only health care providers can perform the tests
        - No other tests are genuine or guaranteed to provide accurate results

- selling fraudulent products that claim to treat or prevent the disease
    - Unapproved drugs threaten public health and violate federal laws (Canadian Anti-Fraud Centre: COVID-19 fraud)

The Economist recently recognized the significantly increase risk of financial misrepresentation by companies and boards during the COVID-19 crisis. The alteration or presentation of company accounts so that they do not reflect the true value or financial activities of the company is inevitable during this time, and companies thus face significant civil and securities regulatory risk as a result (*The business of survival: How covid-19 will reshape global commerce*, *The Economist*, April 11, 2020).

With the increasing politicization of business during COVID-19, there are also increased risks of bribery and corruption. While the risks are lower in Canada than many other jurisdictions, supply chain issues will present significant bribery and corruption challenges for Canadian businesses who are required to comply with the *Corruption of Foreign Public Officials Act*. In fact, according to the PWC Report bribery and corruption is the number one fraud risk for Energy, Utilities and Resource firms, and the number three fraud risk for Industrial Products & Manufacturing businesses.

In short, the COVID-19 crisis will place significant pressure on the traditional triggers for fraud as businesses and individuals respond to mass layoffs, collapsing markets, and lost consumer confidence. Crises are opportunities for fraudsters as businesses scramble to respond, losing sight of traditional due diligence and compliance protocols.

Preparation To Maximize Asset Recovery

Each of the above types of fraud requires a specialized response. Of particular interest for the purposes of this article, are tactics and processes companies can use to maximize asset recovery in civil litigation given the legal framework for freezing and recovering assets. Often, after the fraud has taken place it can be a challenge

for an unprepared business to develop the necessary evidence to recover their losses. Proper forethought can mitigate these issues.

The first hurdle for businesses in civil asset recovery actions is tracing assets to relevant jurisdictions with proper enforcement mechanisms. Investigations can be costly if companies do not have sufficient and up-to-date information about a fraudster's activities and business operations (e.g. for suppliers, vendors, and customers - bank account information, payments history, location of operations, etc.). Financial controls ideally should anticipate these issues ahead of time to reduce investigation costs and it is imperative to keep this information current.

Assuming assets are located, freezing and civil search warrant applications are the essential next step. These types of applications are fraught with challenges. Applications for orders to freeze and secure assets that are brought without notice to the defendant require applicants to provide the court with "full and frank" disclosure. The standard is extremely high. Moreover, applicants must make an undertaking to the court that they will be responsible for any damages arising out of an improperly obtained injunction.

These legal standards mean that the quality of evidence collected by businesses seeking to recover assets misappropriated by fraud must be high. Most fraud succeeds as a result of failed or limited financial controls, incomplete records, and inefficient systems that make it extremely costly to trace and prove a fraud. If an applicant presents the court with an incomplete or misleading set of evidence, a business can quickly find itself on its heels defending an application to set aside an injunction freezing assets. If an injunction is set aside, businesses can quickly find assets dissipated and may also face an unwanted damage award payable to the alleged fraudster.

Given these challenges, businesses should proactively develop protocols that enable maximal recovery in a civil action. These protocols include a robust due diligence process that collects and compiles records for all transactions and key details of customers, suppliers, vendors, and employees, all while complying with relevant privacy legislation. As businesses increasingly outsource non-core competencies to contain costs, they increase the risk of fraud.

Effective outsourcing requires significant anti-fraud controls backed by a robust audit capability (whether that is internal or external). Internal audit procedures should be linked to the standard controls to ensure consistency and completeness. External auditors must be effectively on-boarded for clear systems mapping and careful understanding of day-to-day operations. Companies that do not have internal audit capabilities, should nevertheless develop protocols to enable more efficient external audits in order to reduce costs and increase effectiveness. Separate audit teams can often misunderstand the everyday use of systems and the data generated from them. Given this, there is a significant incentive to coordinate audit teams with on the ground personnel.

Analytics capabilities are now a mandatory dimension in most fraud cases. Data prove fraud. All data are not made equal. Data integrity, quality, and compatibility between systems is a crucial aspect of most modern business fraud cases. If firms do not have internal data analytics capabilities, they should engage outside firms to audit their data warehouses, reporting capabilities, and related systems to ensure that needed information is sufficiently robust and accurate to support more complex analytics conducted later. All of this work greatly assists ensuring that a company's data can meet evidentiary standards of proof. Sloppy or incomplete data management significantly reduces the chances of recovery.

Legacy systems can also present serious challenges, particularly in the case of frauds conducted over long periods of time. Modernizing legacy systems is thus not only a matter of efficiency in business operations but is a fundamental part of fraud detection and prevention.

In the end, effective anti-fraud programs marry well trained people with technological solutions and careful processes that identify and rank risks, develop effective governance and monitoring, and quickly deploy resources to address problems.

The above is only a sampling of the types of issues that arise when anti-fraud controls are incomplete and some examples of how to improve them. What is certain is that such controls must continuously evolve as fraudsters also hone and advance their

techniques. The losses to businesses can be massive, including direct financial loss, damage to brands, lost market position, loss of internal cohesion and motivation, and lost business. Even worse, internal fraud can lead to regulatory and criminal enforcement actions, which have the potential to cause existential crises for businesses.

Conclusion

The ability to effectively respond to fraud is a signal of company health. While business challenges during the COVID-19 pandemic are many and complex, neglecting anti-fraud controls is a serious mistake for any business. In this era, a serious incident of fraud could make the difference between a company's success or failure. At the same time, improving fraud controls can result in improved organizational efficiency and thus profitability. Effective civil asset recovery actions against fraudsters also pay reputational dividends that can ward off future problems. Addressing fraud risk thus also means organizational opportunity and will strengthen businesses as they pivot to address a new world.

by Shea Coulson

For more information on this topic, please contact:

Vancouver	Shea Coulson	604.691.7467	shea.coulson@mcmillan.ca