ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Fraud’s Perfect Storm: Mitigating Risk in a Global Pandemic

Compliance and Ethics

In times of economic stress, corporations face heightened fraud risk, both within and outside their organization. To protect their bottom line, it is critical that organizations have in place a robust anti-fraud strategy, effective monitoring and controls, and a meaningful fraud response plan.

History shows that times of crisis trigger an increase in corporate fraud incidents across a range of categories, including:

- Internal frauds perpetrated by rogue employees, including senior management;
- External frauds perpetrated on corporates through phishing and malware attacks directed at their employees; and
- Supply chain fraud.

Additionally, due to the increased attention to and scrutiny of corporations' costs, profits, and accounting practices during a crisis, previously undetected frauds often come to light.

During the Great Recession, for example, the UK courts in 2008 tried individuals for fraud amounting to some US$450 million in losses at affected organizations — roughly three times the amount of fraud prosecuted the prior year. During this same period, Ponzi schemes perpetrated on investors, such as the Madoff case, came to light.

Moreover, the Federal Bureau of Investigations (FBI) reported at the end of 2008, 545 corporate fraud cases were being pursued by field offices throughout the United States, several of which involved losses to public investors individually exceeding US$1 billion. These are just some examples that point to the depth and breadth of fraud that can occur during times of economic uncertainty.

Identifying different types of fraud on the rise

As of May 2020, 68 percent of antifraud professionals responding to an Association of Certified Fraud Examiners (AFCE) survey had already experienced or observed an increase in fraud levels in the wake of COVID-19, with a quarter saying the observed increase has been significant.

Preying on cyber vulnerabilities

In particular, according to the ACFE, the threat that has risen most during COVID-19 is cyber fraud, such as hacking, ransomware, and malware. This can include CEO fraud, also known as business email compromise (BEC), a major fraud risk that targets people within an organization who regularly perform legitimate fund transfers.

In April 2020, the FBI warned that cyber criminals are targeting organizations that use popular cloud-based email services to conduct BEC scams. The FBI also noted that between January 2014 and October 2019, the Internet Crime Complaint Center received complaints totaling more than US$2.1 billion in actual losses from BEC scams using two popular cloud-based email services.

Supply chain fraud

The COVID-19 pandemic has caused huge supply chain issues across multiple sectors. Problems in the supply chain will both create fraud risk and may mask fraud incidents.

For example, suppliers may attempt to overcharge for or underdeliver on goods, while employees may collude with suppliers for kickbacks. Corporations may suffer as their competitors engage in murky practices to maintain or increase market share.

Financial statement fraud

During the COVID-19 pandemic, we have seen companies uncover potential fraud in their financial accounting, with severe consequences. For example, in April 2020 the Chinese startup Luckin Coffee disclosed that an internal investigation had uncovered US$310 million in fabricated transactions.

Separately, in times of crisis, companies may make a tactical decision to go into administration or liquidate, which could trigger fraud by senior management (e.g., regarding transfer of assets), resulting in an adverse outcome for suppliers, banks, and other creditors.

Insider fraud

Indeed, senior management within an organization can pose the biggest internal fraud risk since their seniority can enable them to bypass controls. They may succumb to pressure to commit fraud in an attempt to keep an organization afloat during turbulent times, for instance by fictitiously inflating revenues.

According to the 2020 Report to the Nations issued by the ACFE, schemes committed by owners/executives resulted in a median loss of US$600,000, which was nearly four times larger than the median loss caused by managers, and 10 times larger than the median loss caused by average employees.

For companies with a global footprint, there may be a heightened risk of fraud by local management in certain locations because staff from head office are unable to travel and do regular site visits.

Employees across the spectrum will be concerned about job and financial security, given the huge jump in redundancy and unemployment rates. Employees could succumb to the pressure to “deliver” — in particular, those in customer-focused and commission-based roles will be keen to hit their targets.

As a result, they may misappropriate assets, or engage in potentially fraudulent practices that erode profit margin, such as granting volume discounts to customers to hit sales targets, then subsequently giving credit notes.

Investment fraud

Companies that are struggling for cash may fall victim to scams perpetrated by fraudsters pretending to be potential investors. Fraud risks for investors are also heightened as investors look to withdraw assets from funds, for some of those funds may be revealed to be Ponzi schemes. Investors will need a smart legal and investigative strategy in order to recover their invested funds.

Mitigation strategies

Given the current squeeze on revenues and focus on cost management, organizations that can root out and protect against fraud will bolster their bottom line. Without question, a multifaceted approach works best.

Identification and swift investigation of fraud incidents

The ACFE’s 2020 Report to the Nations estimated that, for a typical business, fraud losses total five percent of revenues each year. An organization may already have a concern about a particular

location, division, employee or, supplier — perhaps triggered by a fraud risk assessment, complaint, or whistleblowing report, or even through data analytics.

The longer it is left unaddressed, the higher the potential losses. A swift and effective investigation will establish whether there was any misconduct, determine the amount of fraud losses incurred, and provide a critical path for both loss recovery and control improvements to prevent further losses.

Fraud response plan

Organizations need to have in place a meaningful fraud response plan, since speed is of the essence in minimizing fraud losses. The plan should include governance, the path of escalation to senior management and other stakeholders, respective roles and responsibilities, data preservation and retrieval, and use of third parties with specialist expertise such as investigative firms and legal counsel. The plan may require updating considering current challenges relating to travel restrictions and access to evidence.

Identification of fraud risk

Entities need to identify where their fraud risk lies. For instance, an organization may be overly reliant on a small number of suppliers or on third-party intermediaries for sales, which presents a risk of fraud, as well as bribery and corruption. Or it may need to revisit its existing fraud risk assessment in light of COVID-19 and scrutinize its supply chain. Any concerns regarding suppliers need to be addressed now, before the problem worsens.

Monitoring for fraud

AFCE's 2020 report found that when fraud is detected proactively — such as through document examination, surveillance, or monitoring — it tends to be detected more quickly and thus cause lower losses. Conversely, passive detection — for example, through accident or a confession — results in lengthier schemes and increased financial harm to the corporate victim.

It is key for organizations to implement proactive monitoring, and to regularly undertake a fraud health check to identify potential anomalies pointing to possible fraud based on data analytics.

Prevention through effective antifraud controls

A fraud risk assessment may reveal fraud control weaknesses as a result of the pandemic. For example, given the shift to remote working, the pandemic may have lessened the impact and effectiveness of some antifraud controls, such as "four-eye checks" through a two-person review process.

Business practices will have also adapted; communications with customers and suppliers will have moved mainly online, presenting additional fraud risk factors around verification, which in turn require controls to be adapted. Risks may arise in respect to recently departed staff who still retain access to systems.

A fraud health check may also reveal situations where fraud controls have been bypassed, for example, by senior management pressured to make speedy decisions.

Deterrence factor

Employees may be deterred from engaging in fraudulent acts and collusion if they are aware that the company undertakes fraud monitoring. This can be messaged to employees, including recent joiners, through training. Training can also remind employees of the importance of adhering to antifraud controls. This messaging is particularly important in times of crisis, when employees may perceive that the control environment is weakened due to management focus on business fundamentals.

Whistleblowing

Employees may be aware of, or suspicious of, potentially fraudulent actions by a colleague, manager, or supplier. ACFE's 2020 report found that 43 percent of fraud schemes were detected by tips, and half those tips came from employees. Further, organizations with a hotline detected fraud more quickly than those without a hotline.

The current pandemic may prompt employees to speak up about such concerns, particularly where they perceive that their organization is in financial difficulty or their job might be at risk. In order to encourage employees to report such concerns, organizations must have in place an effective whistleblowing framework and strategy, whereby employees trust they can speak up without fear of retaliation, and reported concerns are investigated in an effective manner.

Conclusion

Companies often spend energy and resources on maximizing revenues; however, increased focus on stemming fraud losses can make a significant difference to an organization's overall profitability. To sum up with a tried-and-true axiom, an ounce of prevention is worth a pound of cure.

For more advice and resources on the coronavirus pandemic, visit the ACC Coronavirus Resource Center.

Joanne Taylor

Managing Director

K2 Intelligence Financial Integrity Network

She has 20 years of legal, investigations, and financial crime compliance experience, which includes fraud risk management, anti-bribery and corruption, regulatory enforcement, and fraud investigations experience working within the financial and legal services industries.