COVID-19 and financial crime: Fraud expert warns of heightened risk of fraud and cybercrime

Sapere Forensic Director and Head of Investigations, Gary Gill, warns businesses of the increased risk of phishing emails, payment diversion and other financial crimes, due to the COVID-19 pandemic.

The COVID-19 pandemic has seen significant changes in the way in which many businesses operate. More employees are working from home and many are facing financial hardship, customers are increasingly transacting online, suppliers are faced with changes in demand for products and services, as well as different ways of delivering them, and the government has announced a range of measures to combat the economic fallout from the pandemic.

My previous experience with economic upheavals, such as the Global Financial Crisis (GFC), shows that financial crime spikes during this type of crisis. The response to COVID-19 is resulting in major economic upheaval, and we should expect the risk of crimes such as fraud and cyber-attacks to be heightened. We must do everything possible to ensure the controls that prevent, detect and deter these crimes are operating as effectively as possible.

What are the threats and what can be done to combat them?

Working from home (WFH)

While we are all adjusting to WFH, its business-as-usual for hackers and other organized criminals, and there are already reports of increases in the following types of scams:

- **Phishing emails:** Clicking on dodgy links can compromise sensitive, confidential or personal information and lead to fraud and theft of personal information. Remind your employees about the heightened risks related to phishing emails during the pandemic and not to click on suspicious links.
- **IT Scams:** A call or email from someone claiming to be an employee in the IT department, asking for a password or providing instructions on how to download software to gain unauthorized access to your systems. Make sure your employees are aware of these types of requests and don't respond to them.

Procure-to-pay channel fraud

The procure-to-pay channel is where the money is, and naturally attracts more than its fair share of fraud. The pandemic only heightens the risk. Be particularly aware of the following:

- **Unusual procurement practices:** A recent publication by the NSW Independent Commission Against Corruption (ICAC)[1] discusses increased pressure to engage in emergency procurement; agreeing to contract variations; using direct negotiations and other exemptions to competitive procurement processes; and paying suppliers more quickly, especially small businesses. These practices heighten the risk of corruption and fraud. Businesses should apply their normal procurement controls as far as practically possible.
- **Theft of stock and other assets:** Unfortunately, some individuals will take advantage of workplace disruption during the pandemic to steal business assets. Check your security measures are up to scratch.
- **Business email scams:** The now infamous "CEO email" scam is even more of a risk during the pandemic, because it gives rise to a range of unusual transactions and emergency requests in the procure-to-pay function. An urgent request for a large payment into a bank account from someone purporting to be a senior officer of a company or a change in a supplier's bank account details that would have been questioned in the past might not be questioned now, and WFH makes it more difficult to verify this type of request. Make sure your employees in payment functions have a heightened awareness for this type of request.

Risks particular to specific industries

The pandemic and response to it may affect specific industries in different ways.

- **Healthcare**: This sector may be subject to increased threats of ransomware attacks during the pandemic. Cyber security defences in this sector should be alert to an increased level of attack.
- **Superannuation**: The Australian Institute of Superannuation Trustees (AIST) has warned that "unscrupulous operators have already begun targeting super fund members and offering to assist them in taking up the new early release super measures". Superannuation funds and their members should take extra care in dealing with early withdrawals.

Fraud related to economic support programs

The ICAC publication referred to above provides a useful summary of the risks associated with stimulus funding and new programs. Well-intentioned programs announced during the GFC were targeted by fraudsters (remember the home insulation program!) and it will only be a matter of time before they target some of the COVID-19 economic support measures.

Watch this space …

[1] NSW Independent Commission Against Corruption. (2020). *Managing corrupt conduct during the COVID-19 outbreak*. Sydney, Australia. ICAC NSW. Retrieved from: https://www.icac.nsw.gov.au/prevention/corruption-prevention-publications/latest-corruption-prevention-publications

About the author

Gary Gill is a director and Head of Investigations at Sapere Forensic. He has extensive experience in the prevention, detection and investigation of financial crime, and has led numerous investigations into matters involving fraud, bribery, corruption, money laundering, cyber-crime and other related misconduct for corporates, financial institutions and government.
He also advises his clients in effectively managing risks relating to fraud and other financial crime.

Read more about Gary and his expertise here: http://www.srgexpert.com/our-people/gary-gill/

Find out more about Sapere's fraud risk management services here:
Sapere Investigations & Financial Crime Risk: http://www.srgexpert.com/our-services/investigations-financial-crime-risk/
Sapere Forensic: http://www.srgexpert.com/our-services/forensic-accounting-damages/