Andrew Howard, BDO

Andrew Howard is a Partner in the forensic services division of BDO. He helps clients navigate complex fraud and litigation matters by offering practical advice and solutions.

Adam Simms, BDO

Adam Simms is a Partner in the forensic services division of BDO. He provides investigation, risk management and advisory services, specialising in financial crimes and other misconduct.

Financial crime

Is your organisation at risk in a post-COVID-19 world?

Andrew Howard and Adam Simms, BDO

The conditions around the COVID-19 pandemic—economic uncertainty and lack of internal controls in a new digital workplace—have created the perfect ecosystem for financial crime. Leaders who fail to take the right precautions and preventions now could find themselves and their organisations in an irremediable situation.

In this paper, BDO Forensics Partners delve into the murky world of financial crime—what's driving it today, the impact of the pandemic, and how executives, directors and boards can protect themselves and their organisations. They also share key strategies to prevent, detect and respond to these risks in the post-COVID-19 world.

What is financial crime?

When we think of financial crime, white-collar crimes such as executive-level fraud and corruption are the top things that come to mind. And that's not surprising given some of the more notable historical United States cases such as Enron, WorldCom and, more recently, Theranos in the United States and Australian Wheat Board and Securency in Australia.

Yet, as the world continues to change, the idea of what constitutes 'financial crime' has broadened. Many people are familiar with financial crimes relating to the abovementioned examples—fraud, corruption, ponzi schemes and insider trading. However, financial crime also includes money laundering, terrorism financing, modern slavery, breach of whistleblowing laws, tax evasion, phoenix, workplace misconduct, competition/anti-trust activity and certain electronic/cybercrimes, which are on the rise with cryptocurrencies becoming the tool of choice of cybercriminals.

This definition of financial crime is not the only thing that is expanding—board and director responsibilities and liabilities are too.

Today, boards, directors and executives are more accountable for how their organisations are run than ever before. For these leaders, failure to control and prevent these financial crimes from occurring in their organisation can result in significant reputational and financial loss for both the organisation and the individual, and even time behind bars.

However, as history shows and recent events highlight, changing conditions pose a risk for a similar financial crisis to occur as a result of the COVID-19 pandemic, due to increased uncertainty and lack of internal controls in a new working environment. While emphasis by corporate executives, directors and board members is on the pandemic and business survival, they must remain aware of their obligations and accountability regarding financial crime by understanding the factors that drive it, especially during COVID-19, and strategies to prevent, detect and respond to risks appropriately in the new world.

The regulatory environment

The collapse of financial markets during the 2008 global financial crisis (GFC) brought to light the problems of criminal and fraudulent behaviour in the financial services industry. Since then, there has been a global push for directors and executives to play an active and more accountable role in setting the appropriate standards for behaviour and conduct within companies and organisations.

As such, there have been fundamental shifts in accountability with new regulations being implemented and increasing pressure within organisations to ensure adequate procedures are being put in place and communicated to relevant personnel who need to be aware of their legal obligations and defences to crimes committed within their organisation.

We are seeing:

- increased funding to federal regulators, courts and the Australian Federal Police (AFP) to undertake and process criminal investigations
- whistleblowing laws involving criminal prosecution
- increasing pecuniary penalties in the *Corporations Act 2001*
- the notion of deferred prosecution agreements.

On 2 December 2019, the Australian Government introduced the Combatting Corporate Crime Bill into Parliament (the *Crimes Legislation Amendment (Combatting Corporate Crime) Bill 2019*).

The Bill introduced amendments to the *Criminal Code Act 1995* which, among other things, established a new corporate offence for failing to prevent an associate of the corporate from committing foreign bribery offences by having (a lack of) adequate procedures.

Changes to legislation/guidance regarding director/executive responsibility and the adequate procedures defence will likely mirror the *Bribery Act 2010* present in the United Kingdom.

What is changing today?

Directors and executives today operate in an absolute spotlight of transparency. With the advancement of investigative technology and the rapid rate at which information can be acquired and distributed via social media, criminal and fraudulent corporate behaviour can no longer be swept under the carpet; the truth of the situation will be uncovered soon enough. And what will follow will be damaging to a corporate's reputation.

With directors and executives already facing pressure concerning existing obligations and responsibilities, the COVID-19 pandemic and the financial uncertainty it has created has produced serious challenges. Traditionally strong companies are now struggling and facing potential business failure, and directors/executives need to figure out what to do now while also keeping an eye on the long-term implications of their decisions and how they can navigate these uncertain times moving forward.

With this pressure and uncertainty, the COVID-19 pandemic has formed the perfect storm for corporate criminal activity to flourish. To explain this further, it is important to relate this situation to a foundational model of corporate crime: the fraud triangle.

The 'fraud triangle'

Why do people commit financial crime?

The fraud triangle model, developed by Dr Donald R. Cressey, aims to explain how and why fraud occurs in organisations through explaining three key elements that are usually present in instances of corporate crime:

- opportunity
- incentive/pressure
- rationalisation.

The COVID-19 pandemic has created a range of new opportunities and incentives for individuals to perpetrate corporate crime and we have seen quite a few instances of this, even in the early stages of the pandemic.

Element 1: Opportunity

The first element relates to the belief that there is an opening for an individual to perpetrate fraud and get away with it. Weak internal controls and a lack of enforcement/oversight can provide an individual with the opportunity to commit fraud.

For example, an employee might identify that timesheets are not being reviewed and subsequently submit fraudulent timesheets. This is the only element of the model that can be completely controlled, and thus completely prevented, by the organisation.

When the COVID-19 pandemic hit, businesses, and society in general, had to rapidly transition to a new way of life. Employees working remotely and organisations shifting their immediate focus to business survival and having less of an emphasis on maintaining and improving internal controls have created a whole new range of risks and opportunities.

We are seeing that internal controls have been eroded due to a lack of direct supervision, breakdowns in verification processes and the use of procedural workarounds to bypass controls that would be considered as safe and robust in a traditional in-office/on-site setting.

Element 2: Incentive/pressure

Incentive/pressure in this regard relates to the motivation behind the perpetration of fraud. Personal factors, such as financial hardship arising due to gambling habits, drug addiction and unsustainable extravagant spending, are all examples of motivations behind fraudulent acts. Unfortunately, in many instances, these pressures are seen by the individual as unsolvable issues that they cannot get past.

Therefore, they see financial crime as the only way to ease that pressure rather than seeking assistance to try to relieve their personal burdens. The more incentive/pressure behind the perpetration of fraud, the easier it is for an individual to justify their actions.

COVID-19 has created significant distress for individ-

The quote

As the world continues to change, the idea of what constitutes 'financial crime' has broadened.

The quote

The pandemic has created a range of new opportunities and incentives for individuals to perpetrate corporate crime.

uals and households; be it personal or financial. A large number of people are losing their jobs, or at least living on a reduced income and this uncertainty around the security of their job and their livelihood may pressure individuals into seeing corporate crime as the only way to stay afloat.

The economic response to the COVID pandemic has delayed the 'pressure' for now, but an expectation that the JobKeeper payment will end will be further incentive/pressure.

Element 3: Rationalisation

Rationalisation explains the thought process of the individual committing fraud. They must believe that in their current situation the gain they will receive from committing the fraud will outweigh the possibility of detection. This relates to the pressure faced by an individual who believes that there is no other way around their hardship, and thus they might conclude that they have nothing to lose and everything to gain.

The second aspect of this element relates to the individual's justification or reasoning behind why they committed the fraud. Those who perpetrate a corporate crime may not see themselves as a criminal, but rather a victim of circumstance.

Examples of justification might include job dissatisfaction after being overlooked for a promotion, or personal circumstances such as the need to look after one's family if their partner loses their job or becomes ill.

The distress surrounding the uncertainty of one's job and financial stability arising as a result of COVID-19 might make it easier for an individual to rationalise perpetrating fraud. One may feel that they are already close to losing their job, or that they are entitled to more than what they are getting from their employer. Alternatively, an individual might justify their fraudulent actions through the belief that they need this money to protect their family and their livelihood during these uncertain times.

Mitigating financial crime

The crime risk response needs to be adaptive and versatile, which might not be so different from what many are already doing. The prevention, detection and response approach to corporate crime is as important now in response to COVID-19 than it has ever been.

Risk assessments

An organisation's approach to preventing corporate crime needs to have a COVID lens. Fraud and misconduct risk assessments, employee and third-party due diligence checks and organisational culture and training (among other things) are all critical preventative methods that need to be adapted to the COVID landscape. While staff are working remotely and supervision is minimal, it is important to ensure that there is adequate segregation between duties.

Further, data analytics has proven a useful proactive tool to identify anomalies which can be immediately followed up and investigated if necessary.

Avenues for detection

It is also important to set a tone from the top of the organisation that misconduct is not to be tolerated and should be brought up if identified. This can be done through employee inductions and regular awareness training throughout their time with the organisation.

Additionally, data analysis is useful to detect outliers among a large field of data, such as an employee having a duplicate bank account. These anomalies can be identified quickly and investigated if necessary, and this will be increasingly important in the new remote environment in which many businesses now operate.

Response more important than ever

An organisation's ability to respond to issues that arise is vital and especially during these times. Dealing with issues effectively and investigating them thoroughly should be the focus by having a robust process in place. Such a process will allow the investigation outcomes to be managed correctly.

We are seeing spending curtailed in risk assessments and investigations, with this work being deferred, or worse, not undertaken.

Yet the opposite should be happening, as issues not resolved or investigated can be bleeding your business of funds, revenue or future earning capacity. Aside from that, the reputational issues that can arise from not managing this process correctly can be severe. This was one of the major deficiencies highlighted during the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry.

Responding with technology

In the wake of COVID-19, the response and investigations into claims of corporate crime need to be able to be successfully undertaken with lesser resources and physical interaction. This is where the augmentation of technology and technology-lead investigations is becoming increasingly important, and is becoming the new norm when responding to claims of corporate crime.

If an organisation isn't looking into alternative technologies and applications to adapt their response to corporate crime, especially in the current environment, they will fall behind in their investigative effectiveness and will risk missing out on cost efficiencies. Technology that drives effective remote investigation capability is key.

Looking ahead

It is expected that corporate crime will rise as the pressures of the pandemic impact businesses and employees, especially when stimulus packages begin to be turned off.

With this, the main takeaway for organisations is to build awareness and be informed about the crime risks to the business. It is critical moving forward to be aware of any potential opportunities for fraud and to be proactive in the response to identifying and responding to criminal behaviour. **FS**