simmons+simmons

Fraud in the time of COVID

Will the coronavirus recession prompt an upsurge in economic crime?

03 April 2020 Publication

+ Share Publication

It now appears inevitable that the global spread of COVID-19, and governments' responses to it, will cause a severe, if hopefully short-lived, recession. There is clear potential for it to morph into an all-singing, all-dancing financial crisis. All economic downturns prompt greater levels of, and reveal ongoing, economic crime putting huge burdens on companies, both in terms of direct cost to organisations in the midst of the crisis and as a result of enforcement action and parallel civil proceedings pursued in the years following its conclusion. As such, companies need to be on the lookout for warning signs of criminal activity and ensure that the undoubted pressures of the current crisis do not weaken their focus on compliance and proper risk management.

Recession and economic crime

Economic crime tends to surge during and following a recession. With respect to the 2008-2009 financial crisis, a study by the advisory firm BDO suggested that the amount of money lost through fraud jumped from an average of 4.57% of total spending in major developed economies from 1997-2007 to an average of 5.47% between 2007-2011. That equates to a 20% increase and a total cost of about £85 billion per year in the UK alone. The same study found similar spikes around previous recessions. These spikes occur for at least two reasons.

The first is that a collapse in markets and commodity prices, particularly following the build-up of a significant bubble prior to the crash, tends to flush out ongoing fraud that was hidden whilst times were good. The most famous example is the Madoff Ponzi scheme; despite numerous reports to US enforcement agencies it remained undetected until the crash. It's fair to say that law enforcement did not catch Madoff: the economy did.

Current circumstances are practically a perfect storm in this regard: the markets have dropped dramatically; price volatility is hitting all-time highs; commodity prices have crashed; and (unlike the 2008-2009 financial crisis) COVID-19 is truly global and will likely lead to a significant recession in every country around the world. Meanwhile, the reach of government, and the contact points between business and public officials, is expanding rapidly and into new areas.

Second, at times of financial difficulty and business disruption, the risk of fraud and corruption increases. Both tend to increase when there are greater incentives or pressures to engage in misconduct and greater opportunity to do so, where attitudes become more permissive towards 'borderline' conduct or where individuals find it easy to rationalise these behaviours. All such behavioural factors tend to be present in recessions. It is not difficult to understand why financial crime might surge in our current circumstances:

financial pressures and pressures on individual performance are greater in businesses under stress and where individuals' livelihoods are at stake. COVID-19 and government lock-downs of large sections of the economy will drive many companies to the wall. Many others will still face severe financial difficulties. In such circumstances there may be an increased temptation for individuals to engage in activity they would not normally countenance, for instance falsification of figures to meet sales targets. Likewise some companies will also face increasing incentives to falsify their reporting or to include statements in their market disclosures that may, in time, turn out to be misleading;

the disruption faced by businesses and, in particular, the bulk of employees working from home presents greater opportunities for potential fraudsters, both internal and external. Having staff working from home makes it more difficult for businesses to monitor those employees. This increases the opportunity for individuals to engage in behaviours that might amount to fraud or market abuse. Likewise, mass working from home is likely to weaken many organisations' data control processes, leaving them more vulnerable to cyber and other data loss incidents – including those prompted by fraud. Similarly, personal insecurity on the part of employees makes them more likely to fall for phishing scams and other fraudulent schemes. Interpol have published COVID-19 related guidance for law enforcement flagging increased fraud and cybercrime risks (here and here). We have published separate articles on market abuse and cyber-security risk linked to COVID-19;

financial crime governance and processes tend to come under strain. Compliance officers and the legal function are sometimes seen as constraining business and their

intervention in the future may suffer significantly from that perception; and

in difficult economic times the capacity for individuals to rationalise their actions increases. For instance, it is perfectly possible to envisage how individuals might consider that, given the extraordinary nature of the current crisis, they are entitled to 'bend the rules' – particularly those relating to financial crime - in order to ensure that their businesses can survive the crisis or so that targets can be met. Unsurprisingly, enforcement agencies and regulators are very unlikely to take a similar view.

Steps companies can take now

We are currently still at a very early stage of the COVID-19 crisis. However history suggests we should expect to see a wave of fraud and other economic crime arising from this period in the months and years to come. Indeed, at a low level, we have already seen the first enforcement action against a COVID-19 fraud (by the DOJ in relation to a seller of fake vaccines: see here). Companies should therefore be taking steps now to ensure they are best placed to prevent crime from occurring and in order to deal with it in the event that it does occur.

As such, if they have not already, companies must urgently review the risks associated with their current working arrangements and put in place measures to ensure the continuation of a strong control environment. That will reduce the risk of misconduct. In particular we would recommend:

reminding employees of existing company policies governing conduct and the acceptable use of company systems, devices and information. Remote training should also be issued where necessary;

for regulated companies (e.g. by the FCA), ensuring that regulatory compliance, including relating to systems and controls, is maintained;

where appropriate, putting in place measures to identify any unusual behavior such as enhanced monitoring or retrospective review of high-risk transactions; and

warning employees that cyber criminals may exploit the current turmoil to increase phishing attacks. In particular, we have seen attempted phishing attacks hidden in emails regarding medical updates or "important notices" for those working remotely.

Applicable law

UK

Services

Investigations

Dispute Resolution

Crime

Contact

Thomas Bowen
Supervising Associate

Stephen Gentle
Partner