COVID-19 Fraud & Economic Crime Webinar Recap

MAY 2020

Extreme crises—such as the Coronavirus (COVID-19) pandemic—present unique challenges and create conditions in which misconduct can thrive. On 6 May, Sarah Keeling, a former senior British government official and StoneTurn Senior Adviser, led a panel of anti-fraud and crime prevention experts to discuss the impact of the global pandemic on businesses, as well as the risk implications of the virus.

Panelists included:

MODERATOR
Sarah Keeling
Senior Adviser,
StoneTurn

Alex Rothwell
National Coordinator for Fraud and Economic Crime, City of London Police

Jeremy Summers
Partner,
Osborne Clarke

Annabel Kerley
Partner,
StoneTurn

Alex Moss
Senior Manager,
StoneTurn

StoneTurn

GeoPolitical Context of the Pandemic *(Sarah Keeling)*

Setting aside the increased risks of fraud and economic crime directly related to the pandemic, clients are considering their strategy in an era of increased division between domestic and international operations with the added risk of economic slowdown. Some international institutions (UN, WHO, NATO), which historically have had global influence and credibility are now being questioned and losing their impact. The result is potentially an increase in economic – and possibly military – confrontations and domestic political polarisation. The fragility of many international relationships (China/Russia/U.S./Iran) may lead to increased risk for supply chains, international shipping and global businesses. The continuing rise in cyber-attacks targeting operations and infrastructure and data/money theft remains a great threat. Environmental risks are causing concerns for multinationals, especially given the risk of climate change events and destruction of natural ecosystems.

On the Frontline of Fraud Prevention *(Alex Rothwell)*

After an initial period of adjustment for policing, capacity issues have normalised. In fact, sickness levels among the police are actually better than normal for this time of year. Demand for policing is also down, with fewer resources required for events, demonstrations and public gatherings.

Police capability however, has been affected by the pandemic. Prosecutions have largely stalled; there are challenges in performing traditional activities such as executing search warrants and arresting people because the benefit has to be balanced against health risks. As lockdown measures are relaxed, demand for policing will increase and, unfortunately, the ability to enforce social distancing compliance, for example, will be diminished. This will put more responsibility on businesses to manage those issues.

Fraud has not diminished during the crisis; we are seeing very consistent levels of crime today. What has changed is the type of fraudulent activity. There is an increase in online shopping fraud, particularly related to the sale of hand sanitizer, personal protective equipment (PPE) and/or COVID-19 testing or "treatment" kits. Criminals are exploiting business executives working from home and attempting to secure rushed transfers of cash. We are also seeing an uptick in phishing and smishing campaigns. PPE procurement is likely the biggest challenge for law enforcement going forward as we have already seen a number of multimillion dollar PPE frauds originating overseas.

A Looming Wave of Regulatory Enforcement *(Annabel Kerley)*

The economic crisis emanating from the COVID-19 pandemic will likely give rise to two sources of new cases for regulators. Firstly, we are seeing some similarities with conditions seen after the 2001 dot.com bubble and the 2008 financial crisis, whereby the ensuing economic downturn revealed historic large-scale frauds, particularly around serious accounting irregularities and industrial-sized Ponzi schemes. Second, the pandemic itself will give rise to new issues, from increased bribery and corruption by companies and individuals in "survival mode" and frauds relating to the PPE and pharmaceutical supply chains, for example. Regulatory agencies such as the Serious Fraud Office (SFO) and Financial Conduct Authority (FCA) will be vigilant about uncovering these types of misconduct. In fact, the FCA has vowed to "clamp down with all relevant force" on those who seek to exploit the current crisis.

To help minimise the impact of intentional or unintentional misconduct, organisations should:

- Prioritise culture, now more than ever: Continue to reinforce the importance of compliance culture in difficult times
- Reassess sales incentives: Ensure that employees are not implicitly encouraged to commit fraudulent acts
- Focus on and maintain segregation of duties as a means to prevent misconduct despite potential challenges to staff availability and physical locations
- Document any control workarounds put in place during the pandemic to ensure these may be fully reversed when conditions normalise

Consequences of the Pandemic

(Jeremy Summers)

An evolving range of fraud has been identified involving e-commerce (fake PPE etc.), identity theft and investment scams all seeking to leverage off current anxieties. There is already concern that the NHS tracking app will, when it comes online, present a clear data theft risk. The need to commit resources to monitoring these new risks is raising concern that other issues, for example insider trading, may not be detected as easily as would have been the case before the pandemic started.

The pandemic has created a host of new risks for businesses and individuals. Many organisations may be tempted to cut corners when onboarding new suppliers or customers and, in so doing, could inadvertently expose their businesses to money laundering risks.

As with previous crises, businesses will collapse and when the tide recedes, accounting practices adopted before the lockdown may come under scrutiny.

For those companies that may fall victim to fraud, they should consider swift and aggressive litigation. Civil courts are operating remotely. The familiar arsenal of freezing orders, prohibition orders, seizure orders and tracing orders are still available, and we have seen the courts respond to well-prepared cases granting orders efficiently and quickly. So, there is definitely hope for those who have seen their assets improperly diverted and seek recovery now.

Responding to the Increased Risk of Fraud Arising from COVID-19

(Alex Moss)

The sudden increase in business pressure caused by COVID-19 has resulted in otherwise effective policies, procedures and internal controls being relaxed or even ignored. While many businesses are still focused on survival, internal controls must not be overlooked, as fraudsters and criminals seek to exploit weaknesses exposed by the pandemic. For example, employees or third-party agents could resort to illicit activities, such as bribery, to expedite a government process or obtain goods from a supplier. As a result of 'social distancing,' isolation and travel restrictions, there is less effective on-site monitoring of activities and direct oversight of employees, which increases the risk of fraud and corruption. In addition, with a significant number of employees working remotely, any weaknesses in remote connections are susceptible to cyberattacks.

Organisations on the front line of combating the pandemic are most vulnerable. This includes government bodies, healthcare companies and the charitable sector. But all businesses can benefit from taking a holistic look at their response to the COVID-19 crisis. In particular:

1. Conduct a fraud risk assessment to ensure existing controls are operating effectively and look for new, unanticipated risks.

2. Use a lull in "normal" business activity to refresh employee antifraud training.

3. Utilise data analytics tools to ensure the integrity of organisational data (completeness and accuracy) and leverage technology to spot potential anomalies.

4. Enhance third-party due diligence efforts: Companies should not be tempted to cut corners when performing third-party due diligence or allow transactions prior to the successful completion of formal vetting. Key factors to consider include:

   - Are the vendors legitimate, established companies?
   - Can they manufacture, procure and/or deliver the specific product?
   - Is there any evidence that the vendor has successfully completed transactions with other customers or clients?
   - Are there any regulatory issues, sanctions, or other reported violations relating to the third party?
   - Are there reputational risks in dealing with the third party, such as indicators of fraudulent business activities?

5. Looking forward to recovery, businesses should strongly consider post-event assurance reviews. Most misconduct won't come to light until after the pandemic is over. Companies should assess their performance during the crisis, as soon as practicable, to understand any internal control deficiencies and plan any remediation measures.

Question and Answer Session

Q. Has fraud risk originating out of call centres been suppressed at all by the lockdown in India?

Alex Rothwell: Historically, there has been data theft from legitimate call centres in India. In terms of illicit call centres operating in the country, there is certainly resident expertise to set up—and labour to sustain—that type of operation while communicating with an outside jurisdiction. But earlier controls put in place to deter data theft from Indian call centres seem to be working. Reported frauds originating from call centres in India are down, which may be a positive result from lockdown orders.

Q. Mine is less of a question and more of comment:

A. I'm joining the call today from Switzerland, which is historically fairly complacent when it comes to fraud prevention. A large multinational organisation based here has just announced that interim remote work measures will become the new reality and its large headquarters in Switzerland will likely not be repopulated. Moves like these have enormous implications for increased fraud and economic crime risk. I've appreciated the helpful tips provided by the panelists today in terms of preventing fraud now and post-pandemic. But even in the best of times, resource-rich companies struggle to invest appropriately in effective antifraud measures. Post-pandemic, justifying this expense will be even

more challenging, particularly for small and medium-sized companies.

Q. What are the panel's predictions for regulatory responses to COVID-19-related frauds?

Annabel Kerley: When fraud is determined to be a direct result of efforts to exploit the circumstances created by the pandemic, I think regulators will clamp down extremely hard but there are challenges to that. I don't believe the level of post-pandemic enforcement will be as broad as what was seen after the financial crisis, for example. Instead, I think regulators will focus their efforts on highly impacted areas, such as healthcare. We also expect a spike in internal investigations amongst organisations where fraud prevention was not a priority.

Jeremy Summers: My view is that all regulators—not least because of resource constraints—will want to approach post-pandemic enquiries in a flexible way and this is a relatively new perspective. Where people or organisations are genuinely trying to navigate their way through the challenges created by the pandemic, there will be leniency. However, I'd echo that when intentional abuse is uncovered—regulators will come down very hard.

Q. Is there a role for independent agencies to oversee or steer the interplay between private and public agencies regarding pandemic-related intelligence?

Jeremy Summers: In these extraordinary times, I believe everyone is searching for solutions and intelligence is key. A more formal private-public partnership aimed at garnering intelligence—led by law enforcement, of course—could do much to benefit the greater good.

Alex Rothwell: In fact, sharing intelligence in this way is something we have started to discuss within law enforcement. A lot of beneficial information does exist in an open forum environment. The challenge is getting that data into one place in an easy-to-access way. There are a number of providers that are great doing that—including StoneTurn. We are just beginning to talk about how we harness the power of centralised data. I think there is a real opportunity to bring that discussion forward now but no immediate solution.

Q. What types of fraud schemes linked to COVID-19 is the panel seeing? How do you expect this to change over the coming months?

Alex Moss: Phishing and smishing—email and text scams—are on the rise. There has also been an increase in spear-phishing attacks where fraudsters impersonate senior business leaders and attempt to pressure employees into an urgent transfer of funds. Going forward, I think we will see more fraud related to the unprecedented amounts of money being pumped into the global economy from various government relief efforts.

Annabel Kerley: In fact, fraud related to the Paycheck Protection Program (PPP) in the United States is already coming to light. It's only a matter of time before similar schemes are uncovered in the UK and EU. I think we should also expect an increase in charity fraud as more fraudsters establish fake charities purporting to provide COVID-19 relief.

Q. What practical tips can you share for conducting effective investigations remotely?

Annabel Kerley: First, prioritise what must be

investigated and direct your resources to ongoing, high-profile or high-stakes matters. Given the current lockdown environment, focus on less contentious activities such as data gathering or data review and ensure you have the proper controls to secure evidence for future imaging and analysis. Interviews with uncooperative witnesses, which largely require building rapport in-person, should be delayed to the extent possible.

Alex Rothwell: Many of our investigations are involved, long-running enquiries and we continue to work to progress them. For example, police are going out as part of investigations but we have seized goods and interviewed witnesses in line with quarantine and social distancing protocols. In every instance, we are performing a comprehensive risk assessment beforehand based on specific circumstances to ensure that we are protecting employees and the public, as well the people with whom we are dealing.

Jeremy Summers: Only a very tough enforcement agency would penalise a business that failed to thoroughly investigate allegations of misconduct in this environment. Organisations that make an objective, well-documented decision about how to best proceed during the pandemic should be viewed positively. Also, be sure to take proper steps to ensure document and materials preservation and that should tick all the boxes for a regulator right now.

Q. Could private prosecutions help tackle the unexpected increase in COVID-19-related fraud?

Jeremy Summers: Private prosecutions have gained some momentum in recent years. However, in an environment where there is an enormous backlog within the criminal justice system as a result of the pandemic—will authorities be increasingly reluctant to dedicate scarce resources to private debt collection claims, for example? That remains to be seen but I believe that the number of private prosecutions could drop off coming out of this crisis.

Q. Do you think enforcement agencies should look at refining the process to ensure that investigations don't get mired in quicksand?

Jeremy Summers: Major fraud investigations, particularly those conducted by the SFO, regularly last a number of years, often causing serious stress-related illness. This is only going to heighten with COVID-19-related delays. I think there is a real case for looking at how the investigation process can be improved, and in particular, to really focus on the core issues rather than looking to upturn every stone.