COLLAS CRILL

COVID-19 and financial crime

APRIL 2020

Collas Crill Compliance's Executive Director, Sandra Lawrence, discusses the rise in financial crime during the COVID-19 pandemic and what businesses can do to protect themselves in the latest Compliance Matters. Compliance Matters is a source of international news and analysis on the latest regulatory initiatives within the private banking and wealth management industries.

Alas, in my opinion many of the most successful criminals are often better strategists than some of the most powerful business executives in the world. If only some of them had decided to channel their skills into legitimate enterprises, their destiny may have been considerably different and their positive impact on society insurmountable.

The COVID-19 pandemic has presented criminals with new opportunities to exploit vulnerabilities, while we all focus on adjusting to our own unique and, at times, challenging situations; whether that's a combination of working from home, home schooling, caring for a vulnerable friend or relative, dealing with grief, isolation, mental health challenges, the list goes on.

A high demand for specific goods, an increase in remote working, a decrease in travel and increased anxiety, coupled with the tactical innovation and ability of organised crime groups to adapt quickly has presented them with new opportunities and it took almost no time at all for text messages purporting to be from banks and emails offering counterfeit hand sanitiser to start flooding into our inboxes and mobile phones.

Cyber crime

With the vast amount of us working from home, criminals occupying the cyberspace arena have upped their ante and the National Cyber Security Centre (NCSC) has reported a significant spike in the number of scam emails being sent out, resulting in the launch of their Suspicious Email Reporting Service (SERS). The SERS received in excess of 5,000 reports of suspicious emails within the first day of its launch, and these reports led to 83 scams being removed from the web.

In an example of a recent large-scale attack, the Chartered Institute for Securities and Investments (CISI) announced this month that they were victim of a cyber attack on their online payments process on or around 14 February, which is believed to have compromised in excess of 1,000 members' financial information. Investigations are ongoing, but the CISI have reported that malware was installed into a vulnerable part of their software, resulting in members' payment details being stolen.

The NCSC has published helpful and user-friendly guidance to assist businesses and employees with working from home. By regularly raising knowledge and awareness internally with employees, sharing relevant examples and offering tips on what to look out for to identify malicious emails, companies can help to support staff and ensure that the business follows best practice, mitigating the exposure or impact of a data and cyber security attack.

Fraud

Fraudsters will always look to exploit financial services when there is a distraction and focus elsewhere; they are more likely to be able to rush something through with a weak explanation or bypass usual security controls, while a business is focused on trying to deal with a crisis. This is a well-known risk, and COVID-19 is no exception. While employees juggle the challenges and distractions of working from home, remote schooling, looking after infants and generally just trying to function during a particularly stressful and anxious time, fraudsters are waiting in the wings for their opportunity to pounce.

The National Fraud & Cyber Crime Reporting Centre reported a 400% increase in COVID-19 fraud reports in just March 2020 alone.

On 14 April, Interpol reported how the German health authorities fell victim to fraud when trying to procure protective face masks for their frontline healthcare workers. An upfront payment of €1.5m was made and, days before the delivery was due, the German authorities were notified that the payment had not been received, and that an urgent payment of €880k must be sent directly to the supplier immediately, to secure the order. Suffice to say, the masks did not arrive and it transpired that a legitimate face mask supplier's website had been cloned by a fraudster.

In response, Interpol warned the public to remain vigilant 'as organised crime groups continue to adapt their activities to benefit from the global health crisis'.

Europol reported on 6 April that an individual had been arrested for defrauding an EU pharmaceutical company of €6.64 million for face masks and hand sanitisers. After the payment had been sent to a bank account in Singapore, the items never arrived and the supplier disappeared.

The FBI published a warning to all health care professionals on the increased risk, offering four helpful hints on what to look out for, as they may indicate suspicious activity: unusual payment terms; last-minute price changes; last-minute excuses for delays in shipment; and unexplained source of bulk supply.

Regularly reminding staff to stay focused, and enhancing security controls can help to protect organisations from falling victim to frauds, or inadvertently processing fraudulent payments. If a payment is outside of the normal activity expected for a client, or employees feel like they are being pressured to make a payment quickly, reassure staff that it's ok to stop momentarily, take stock of the situation and, if appropriate, consider suspicious activity reporting. Assure them that they will not be penalised for being prudent and flagging genuine concerns, in particular during the crisis. Clients will understand, particularly when it is explained to them that additional controls have been implemented to protect them and their assets from falling victim to financial crime.

On the flip side, in times of crises and where staff are dealing with their own personal financial worries and other external pressures, there may be a temptation for an otherwise exemplary employee to turn rogue. Ensure that you regularly check in with employees and show your support during these difficult times. Look for signs of stress or changes in behaviour which give cause for concern.

Validating internal policies, procedures and controls, and providing assurance of their effectiveness to boards has never been more important. The last thing that a business would want to be dealing with during a worldwide pandemic is a critical

failure of internal controls and internal fraud.

Counterfeit goods

Counterfeiters have been equally adaptable in shifting their production and distribution of goods to exploit the pandemic, which has resulted in a global shortage of products and an opportunity for crime. Counterfeiters have capitalised on the anxiety of individuals and the urgency in which products are required, with Europol reporting the production of fake blood screening tests, substandard face masks and many other inadequate products flooding the market, jeopardising public safety. This activity is inevitably expected to generate significant profits for the criminals, and they will need to launder the funds somewhere.

Law enforcement

Worldwide law enforcement authorities are working hard, and the stoic collaboration between authorities to track down individuals behind the above type of criminal activity (and more), while faced with travel bans and their own staff challenges, is truly humbling.

My inbox has been flooded daily with emails from Europol reporting on successful arrests, retrieval of funds and complex investigations, involving international co-operation between multiple cross-border law enforcement authorities, all working together in the international fight against financial crime.

The National Cyber Security Centre (NCSC) is proactively dealing with the increased data and cyber security threat, and financial regulators are relaxing certain requirements in a sympathetic response to the current challenges being faced by the finance sector. It is important to keep abreast of these regulatory changes, and ensure that you regularly monitor developments.

Proceeds of crime

With this exponential increase in criminal activity generating significant proceeds of crime, the money needs to be laundered and this places great responsibility on all Money Laundering Reporting Officers to protect their organisations from the threat.

The threat exposure is made even more complicated by the very public nature in which hints and tips on how to protect you and your organisation are communicated. Much as it can be considered suspicious if a new business relationship is fully prepared with pristine due diligence packs, the fraudsters, spammers, counterfeiters and organised crime gangs trying to take your money also have access to those hints and tips, and are able to prepare themselves fully to answer your questions, or evade suspicion in the first place.

Staff are distracted or anxious, and so humility and soft skills are required more than ever in showing support, guidance and leadership to navigate these unprecedented times, while boards continue to demonstrate oversight of the effectiveness and resilience of their internal policies, procedures and controls.

The crisis does offer GRC and AML/CFT practitioners an opportunity to demonstrate the personal value that they add to an organisation, and while they have the board's complete attention and respect, ensure that other uncertainties within the business, which might not been taken so seriously in the past, are addressed.

I'm certain that once a COVID-19 vaccine has been developed, counterfeiters and fraudsters will be nimble in changing their schemes to offer fake or non-existent vaccines, and so the C-19 impact on Financial Crime will be around for some time to come. We must remain vigilant.

COLLAS CRILL

For more information please contact:

Sandra Lawrence

Head of Compliance | Guernsey

t: +44 (0) 1481 734808 | **e:** sandra.lawrence@collascrill.com