COVINGTON

Surge in COVID-19 Related Fraud

April 9, 2020

White Collar

The COVID-19 crisis has led to a sharp rise in fraud and cybercrime in the UK. Although many of the scams we have seen so far have targeted individuals, there is a growing concern that fraudsters are setting their sights on businesses who may now be more vulnerable to fraudulent schemes as a result of the crisis. The UK government's imposition of stringent lockdown measures on 23 March 2020 forced many companies to shut their offices and instruct staff to work remotely—a transition that has made it harder for some organisations to maintain adequate anti-fraud systems and controls.

Fraud on the Rise

Action Fraud, the UK's national reporting body for fraud and cybercrime, revealed a 400 per cent increase in reported cases of COVID-19 related fraud in March—an upward trend that is expected to continue in the coming weeks and months. Action Fraud has reported a large number of scams involving websites purporting to sell testing kits, face masks, and other medical supplies currently in short supply. The authority has also observed a marked increase in phishing scams, including messages purporting to be from HMRC that promise tax refunds or financial support but request the disclosure of sensitive information, including payment card numbers.

Meanwhile, the FCA has highlighted the heightened risk of finance related phishing scams in the midst of COVID-19. In an announcement on 26 March, the FCA said that the UK would likely see an increase in fraudulent activity, and set out a number of frauds that customers should be especially vigilant for. These included schemes exploiting the financial concerns of customers by purporting to offer loans in exchange for an upfront fee. Fraudsters may also masquerade as insurers or claim managers and offer customers assistance in recovering losses flowing from COVID-19 and the economic fallout. Other schemes highlighted by the FCA include scammers sending messages to customers warning that their bank is facing difficulties due to the crisis and encouraging them to move money to a new bank on an urgent basis. Although the FCA's warning was designed primarily for individuals, it is easy to see fraudsters adapting these schemes to target businesses.

The Risk to Business

There are reports that cybercriminals are already targeting companies in push payment scams, where the fraudster—who will often masquerade as an existing supplier—sends an email to the company instructing them to transfer money to a new account. These frauds can be sophisticated and difficult to detect. The email will usually relate to a recent purchase made by the company and appear as though it has been sent by a supplier representative with wh om the

company is familiar. Consequently, recipients often fail to treat such emails with sufficient caution and will approve payment without verifying the request with the supplier.

A significant number of UK businesses have been hit hard by the government's lockdown measures and many are likely to need financial support from creditors in the coming months. Fraudsters often take advantage of economic downturns and may commence phishing campaigns offering businesses credit facilities in return for upfront payments. Fraudsters may also masquerade as landlords or existing creditors and offer their target company a reduction on an overdue or upcoming payment in return for a fee to be paid into a new bank account.

The lockdown will no doubt present challenges to companies in detecting and preventing fraud. Good communication—both internal and external—lies at the heart of all effective anti-fraud procedures. For example, suspicious emails should be flagged internally to raise awareness throughout the business, and unusual requests for payments from suppliers or creditors should generally be verified by phone with the relevant party prior to payment. Ensuring that employees are familiar with and adhere to anti-fraud procedures is also fundamental in protecting companies from cybercriminals.

However, the recent transition to remote working for a significant number of businesses—which took place quickly and gave companies scant time to prepare—threatens to jeopardise communication protocols and adherence to anti-fraud procedures. For example, a phone call to a supplier to query a payment may not happen because an employee does not have a remote contact number for the supplier. Further, remote working may cause employees to feel more distant from their organisation and colleagues, which can lead to a less stringent approach in following policies and procedures.

Will the Authorities Cope?

The sharp rise in fraud against individuals and the clear risks to businesses—many of which are already struggling in the challenging economic conditions—will be a cause for great concern for the UK government and law enforcement authorities. So far, they have been eager to convey that they are well-prepared to handle the rise in COVID-19 related fraud. The Minister for Security, James Brokenshire, has stated that "the government is committed to working with the NCA and all law enforcement partners to tackle [the issue of fraud] and protect the public." Meanwhile, Andrew Penhale, the Head of the Specialist Fraud Division at the Crown Prosecution Service (CPS), said that CPS prosecutors are "prepared for any potential increase in fraud-related files."

Notwithstanding this show of strength, the current crisis has the potential to constrain the ability of the government and law enforcement authorities to counter the rise in fraud. The government will no doubt be preoccupied with responding to the health threat posed by the virus and containing the economic fallout emanating from the lockdown—a problem that will become more acute and require greater attention as time goes on. The lockdown will also likely make it more difficult for enforcement authorities to respond quickly and effectively to new reports of fraud. For example, SFO staff are now working from home and Action Fraud has reported that its contact centre is operating a reduced service and has only a "small number of advisors on hand to help."

Responding to the Heightened Threat

With fraudulent activity on the rise and law enforcement capacity likely to be stretched, it is fundamental that businesses are alive to the risks and take appropriate measures to protect themselves. Companies should emphasise to their employees the importance of communication in detecting and preventing fraud, particularly while working from home, and remind employees of the company's anti-fraud policies and procedures. These may need adapting to reflect the realities of remote working.

If a company falls victim to fraud, it is vital to take action immediately. The earlier a business is able to identify the fraud, the greater the chance of it being able to claw back its funds. Although it will generally be appropriate to notify law enforcement, in the first instance companies should reach out to a law firm, who will be able to take urgent steps to recover the misappropriated funds, including taking injunctive action against the banks to prevent funds being withdrawn.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our firm:

Ian Hargreaves	+44 20 7067 2128	ihargreaves@cov.com
Matthew Beech	+44 20 7067 2310	mbeech@cov.com