Top ten UK frauds to be aware of during the COVID-19 pandemic

22 May 2020
By: Patrick Rappo | Katie O'Hara | Calum Ablett

This article was originally published on Thomson Reuters Regulatory Intelligence on 18 May 2020 and is reproduced with permission from the publisher.

The COVID-19 outbreak has had an unprecedented effect on the world economy. The UK government has quadrupled its borrowing plans over the next three months with HM Treasury seeking to raise GBP180 billion in order to meet its spending needs as tax revenues plunge. GDP is also predicted to slump by 35% and the number of people unemployed is predicted to increase to two million people by the end of 2020.

Millions of workers in the financial services industry and elsewhere are now working from home due to the government restrictions put in place. There has also been disruption to local and global supply chains, which has been exacerbated by lockdowns, travel bans and limitations on labour which have occurred as a result on the outbreak.

The result is a fertile ground for fraudulent activity. This article sets out the top ten frauds you should be aware of in the current climate and ways you can mitigate the risks.

Increased risk of cyberattacks

Current events are likely to have a negative impact on companies' cyber security position. The existence of significant financial and operational challenges may lead to the de-prioritisation of cyber security and planned IT security improvement programmes being put on hold. In addition, the increased use of remote access tools by employees while working from home increases the risk of cyberattacks.

Malicious cyber actors can take advantage of these changes in the following ways:

- Targeting remote access systems with denial of service attacks, seeking to disrupt business operations or to extort money.
- Increasing phishing attacks.
- Infiltrating home WiFi networks and accessing IT systems via VPNs.

Phishing, whaling and smishing attacks

“Phishing” is the use of fake emails or web links to obtain sensitive information about victims, such as passwords, usernames or bank account details. Phishing can also be used to deploy malware. “Whaling” is similar to phishing but is highly targeted and aimed at senior executive-level individuals. For example, a senior executive may receive a fraudulent email from what appears to be a trusted supplier, partner or employee within their organisation requesting a transfer of funds. This type of activity has seen huge returns for fraudsters. Finally, “Smishing” is a phishing-style fraud carried out

via SMS.

Regulators in the financial services industry have issued warnings about such schemes to individuals, however dangers to businesses and their investors are equally increased. Barracuda reported a recent spike in COVID-19-related phishing attacks since the end of February. 77% were scams, 22% were brand impersonation, 1% business email compromise.

Account takeover fraud

Account takeover fraud occurs when a fraudster accesses an individual's (e.g. an employee's) account and uses the account to carry out unauthorised transactions or gain access to confidential information. Fraudsters can obtain account details using various techniques, including phishing, smishing, data breaches and the use of malware.

CEO fraud / impersonation fraud / business email compromise fraud

CEO fraud and impersonation fraud exist where individuals inside an organisation receive emails purporting to be from a senior executive, instructing the transfer of money to a fraudsters account or requesting financial information. This may be carried out in one of two ways:

- Name spoofing – uses the name of the CEO but a different email address (which may be similar to the company's email address).
- Name and email spoofing – the CEO's email address is compromised and attacker uses the CEO's name and correct email address.

The current situation increases risk of both CEO and impersonation fraud as employees work remotely and this can be used as justification for unusual and non-routine payment requests. Alternatively emails or calls may purport to be from the company IT team and are designed to obtain passwords or enable malicious software to be downloaded onto a company's IT systems.

Invoice fraud

Invoice fraud occurs when fraudsters send communications purporting to be from company suppliers, asking for the supplier's bank details to be changed in order to re-route money to fraudster's bank account. Related to this is “invoice hijacking” where a fraudster serves a false invoice on a business after positioning itself in the middle of correspondence between the company and one of its suppliers. This is often achieved through email hacking and observing patterns of behavior and correspondence.

There is an increased risk of invoice fraud and hijacking in the current context due to:

- An increased number of employees working from home, and the resulting IT security weaknesses.
- The current situation making it easier to justify change in payment details.
- Employees already being distracted as a result of changes to working routines.

Investment fraud

With interest rates low and volatile stock markets, fraudsters can take advantage of companies seeking higher-return investments or financial safe havens. Fraudsters may attempt to induce businesses to buy or sell investment products on the basis of false information. For example:

- “Good cause” investments – fraudsters seek investment for good causes such as the production of sanitiser, manufacture of personal protection equipment or new drugs to treat the virus, with the promise of high returns.
- “Pump and dump” schemes - an attempt to boost the price of a stock via false coronavirus claims and later selling the stock at the inflated share price.
- Fraudulent investments offering hedging against stock market volatility.

Fraud in the supply chain

The COVID-19 outbreak has caused increased pressure on many companies' supply chains. For example: closed

borders in certain jurisdictions; suppliers invoking force majeure clauses; a shortage of components and raw materials, This increased pressure can increase the risk of fraud in a variety of ways, including:

- Reliance on alternative suppliers.
- By-passing of controls and due diligence.
- Risk of improper payments to “grease the wheels”.

Insider fraud

Insider fraud occurs when a current or former employee, contractor or any other party who had access to data (often confidential information) commits this fraud by misusing the aforementioned data. The insider may seek to profit from the stolen data, for example by selling the data or using the information to make investment decisions.

Recent events may mean that organisations within the financial services sector are forced to make elements of their workforce redundant, or reduce working hours. Disgruntled employees facing redundancy may look to remove intellectual property, gain financially or otherwise cause reputational or financial damage to their employers.

Advance fee fraud

When carrying out advance fee fraud, fraudsters usually pose as the government or the employee of a business. The fraudsters require businesses to pay a fee before receiving a product, service and/or money. After paying the fee, the victim does not receive the item they thought they were paying for. Examples include:

- Fraudsters may exploit short-term financial struggles caused by the current situation and ask for an upfront fee when applying for credit that the company never receives.
- Fraudsters may impersonate local authorities or government bodies and seek to take advantage of companies seeking assistance from government support schemes by requesting an advance fee in exchange for assistance.

Associated crimes

Fraudulent activities like those previously listed come with a number of associated risks, for example:

- Employees seeking to cover up internal fraud may commit offences relating to accounting misstatements or misleading auditors.
- Acts committed in the supply chain may expose companies to criminal liability under section 7 of the UK Bribery Act for “failure to prevent bribery” e.g. facilitation payments.
- Failure to conduct adequate due diligence on counterparties may create money laundering risks.
- The potential for reportable regulatory breaches which may result in increased regulatory supervision of your firm and/or regulatory enforcement action.

How to protect yourself against the top ten frauds

The frauds listed above exploit the remoteness of employees from the workplace and are carried out via technology; two elements which are unavoidable during the current pandemic. For example, they involve unauthorised access to a business's systems, or incorrect payments made to a fraudulent recipient, usually via or with the unintentional aid of an employee. Alternatively, they involve an employee's exploitation of the business either via supply chain fraud or insider fraud.

Consequently, it is essential for financial services companies to ensure that they monitor the activity of all employees while working from home, have systems checks in place to identify suspicious activity and that all employees are trained on the threats presented to the business during this unprecedented time. We set out below measures which will help to mitigate the risk of the fraudulent activity taking place in your business:

- Ensuring that remote access systems are patched and secure for employees working from home.
- Having adequate security controls which are able to withstand distributed denial-of-service attacks.
- Ensuring that the Cyber Security team are able to continue working effectively in the current circumstances.
- Providing employees with guidance and training on the potential fraudulent activity which may impact your business

such as how to avoid cyber security breaches and how to spot suspicious activity.
- Engaging audit committees at an early stage to ensure appropriate financial controls are in place.
- Documenting how and why financial decisions are made and make it clear what acceptable practice is.
- Ensuring employees use the Financial Services Register and Warning List to check who is being dealt with, even when contacted by phone.
- Implementing additional verification procedures before making payments.
- Ensuring an electronic invoice is genuine by:
  - contacting multiple contacts to validate invoice;
  - checking the email address you have received the email from; and
  - sending a new email to a known contact rather than replying to the email received.

- Ensuring the compliance function is fully operational and visible to employees.
- Ensuring compliance and monitoring tools are functional.
- Ensuring existing policies and procedures are adequate.
- Providing employee training.
- Focussing on due diligence.
- Monitoring financial controls and ensuring that they are effective.
- Increasing scrutiny and transparency (internal and external).
- Engaging with management.

AUTHORS

Patrick Rappo
London | T: +44 (0)20 7349 0296 [UK Switchboard]
Patrick.rappo@dlapiper.com

Katie O'Hara
Senior Associate
London | T: +44 (0)20 7349 0296 [UK Switchboard]
katie.ohara@dlapiper.com

Calum Ablett
Associate
London | T: +44 (0)20 7349 0296 [UK Switchboard]
calum.ablett@dlapiper.com