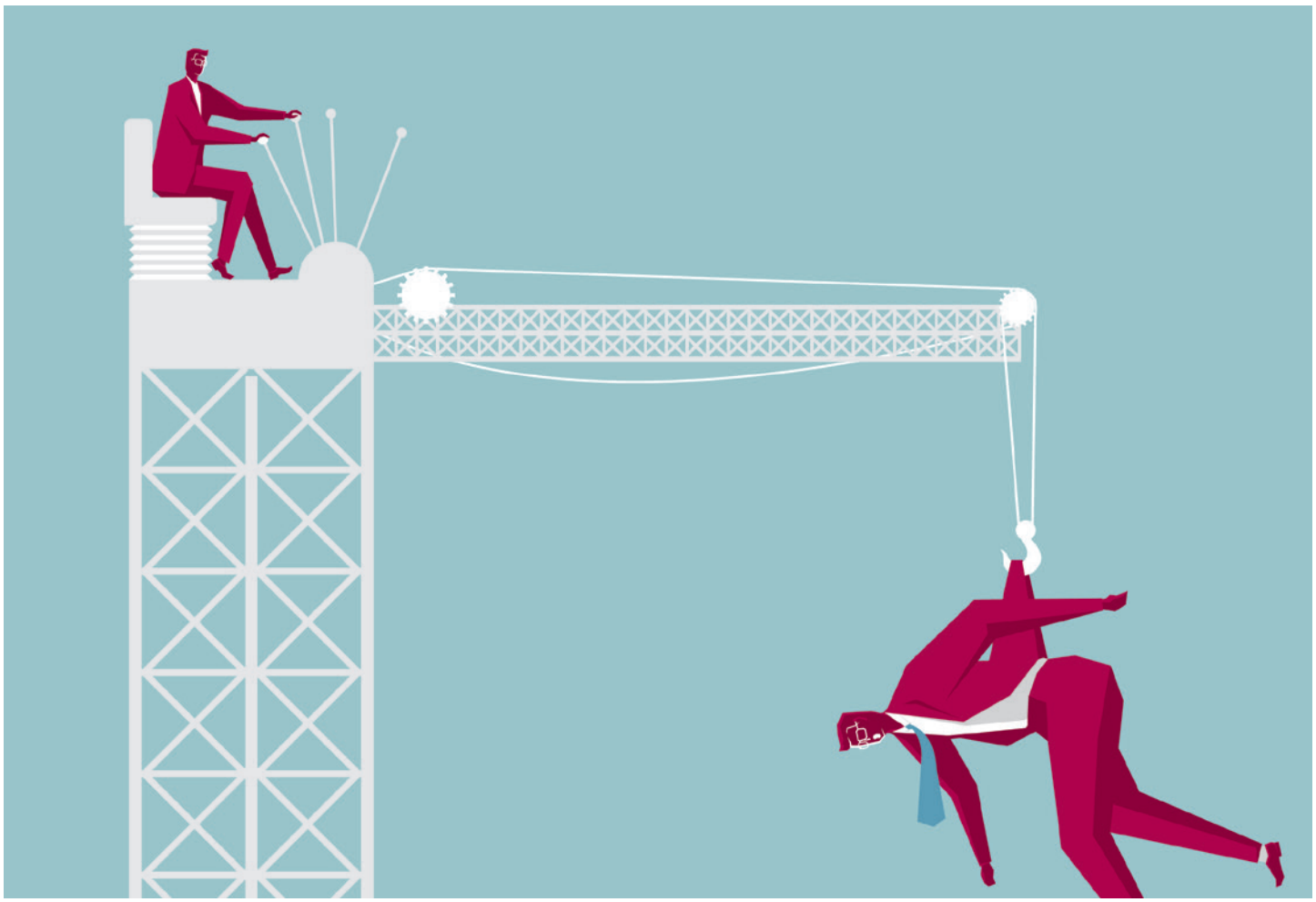
SHOOSMITHS

SPECIAL REPORT Q&A July 2020

Fraud risk and enforcement in the UK

FW discusses fraud risk and enforcement in the UK with Alma Angotti at Guidehouse and John Hartley at Shoosmiths LLP

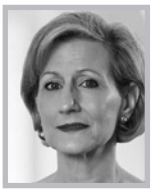


Q&A:

Fraud risk and enforcement in the UK

FW discusses fraud risk and enforcement in the UK with Alma Angotti at Guidehouse and John Hartley at Shoosmiths LLP

THE PANELLISTS



Alma Angotti
Partner
Guidehouse
T: +1 (202) 481 8398
E: alma.angotti@guidehouse.com

Alma Angotti is a partner and co-head of the global investigations and compliance practice. With over 25 years of regulatory practice, she has held senior enforcement positions at the US Securities and Exchange Commission (SEC), Treasury's Financial Crimes Enforcement Network (FinCEN) and Financial Industry Regulatory Authority (FINRA). She is currently on secondment in London. In these positions, Ms Angotti was responsible for conducting investigations involving securities fraud, insider trading, financial fraud, anti-money laundering and counter terrorist financing, market manipulation, investor and market protection, and other regulatory violations.

John Hartley
Partner
Shoosmiths LLP
T: +44 (0)20 7282 4068
E: john.hartley@shoosmiths.co.uk

John Hartley specialises in advising individuals and corporates through the challenges of criminal and regulatory investigations. Mr Hartley is regularly instructed in matters relating to fraud, bribery & corruption, proceeds of crime and financial services related investigations. He has also recently advised on alleged breaches of EU economic sanctions. Additionally, he is well-placed to provide pre-action advice and assistance on regulatory and compliance issues, including anti-bribery policies, business bribery risk assessment and staff training.

FW: How would you describe the current level of fraud risk, and common types of fraud, facing companies in the UK? How has the nature of this risk changed as a result of the COVID-19 pandemic?

Angotti: The level of fraud risk in the UK is high and we expect it will continue to increase. Data from UK Finance shows that fraudsters stole an estimated £1.2bn in 2019 alone. The Crime Survey for England & Wales stated that between 2018 and 2019 there were more than 3.86 million fraud offences against adults. We have seen an increase in authorised push payment (APP) frauds in the UK, where criminals use platforms to trick victims into authorising payments from their account to an account held by the criminal. The recent COVID-19 outbreak has helped fraudsters capitalise on APP schemes. There have been many reports of criminals using social media platforms to advertise fake personal protective equipment deals, for example. As early as 10 April 2020, Action Fraud, a UK fraud-reporting centre, reported almost £2m in COVID-19-related fraud schemes, but we believe this number to be much higher.

Hartley: We all know that the majority of fraud itself follows a pattern and that it is the subject matter or target of the fraud that changes periodically – not necessarily the fraud mechanism itself. I would say though that the level of fraud risk right now has never been higher. Statistics over the last few years have consistently shown that fraud is massively underreported and the true costs have never been fully revealed. More people are at home and online than ever – possibly without the protections that come in an office environment – thus increasing the exposure to cyber attacks and phishing scams. It is also sadly true that should there be a long-term economic downturn this will lead inevitably to an increase in organised crime.

FW: Could you highlight some of the key legal or regulatory developments in the UK designed to tackle fraud risk? What compliance challenges does this raise for companies?

Hartley: UK regulators are constantly looking at ways that consumers and business can be better protected, and so too are the legislators. While some regulators have been easing deadlines and protocols during the COVID-19 crisis to allow business continuity, others have been looking at the gaps that might emerge. For example, the Competition & Markets Authority (CMA) has set up a task force to take action against businesses using the crisis as an excuse to breach consumer protection laws. Likewise, there are teams set up to observe pricing structures and to ensure there are no unfair practices or cartels emerging.

Angotti: The Fraud Act 2006 was the first comprehensive attempt to consolidate the UK's anti-fraud legal and regulatory framework since the Theft Act 1968 and 1978. The Fraud Act simplified UK law in relation to fraud and provided a comprehensive legal framework to fight against technology-fuelled fraud schemes by simplifying the overly prescriptive conditions that defined fraud under the Theft Act, allowing for easier and swifter prosecutions. More recently, new EU-led legislation, such as the Payment Services Directive 2 (PSD2) has been enacted to attempt to provide a stronger anti-fraud framework to electronic payment services. Companies face two main compliance challenges. First, UK case law shows that savvy criminals continue to defraud UK businesses, taking advantage of a general lack of awareness by employees. Thus, training employees to be aware of phishing and other fraud schemes is critical. Second, many companies are struggling to deploy some requirements of PSD2 by the deadline of the end of 2020, mostly around the three prongs of strong customer authentication (SCA) and building additional authentication into checkout flows.

FW: In your experience, what are the key principles of effective fraud risk management, especially monitoring and detection processes that can identify red flags? How important is it for companies to tailor their processes for the specific risks they face?

Angotti: Every organisation should perform an anti-fraud risk assessment that provides an ongoing evaluation of the fraud risk faced by the business. The risk assessment should change as the

business risks change. Firms should draft a comprehensive anti-fraud policy and code of conduct that clearly communicates the firm's zero-tolerance toward fraud. These should be distributed to all employees and set the tone for the organisation's anti-fraud culture and commitment to ethics and integrity. Anti-fraud training, tailored to employees' job functions, should raise levels of fraud awareness in the organisation. Forensic data analysis is an essential part of a strong fraud detection strategy. Forensic analytics tools can digest whole populations of structured and unstructured data, meaning that these tools can give firms the opportunity to monitor all transactions, rather than examining only unusual transactions or those identified from sampling, resulting in a greater chance of identifying potentially fraudulent activity. A centralised data repository of anti-fraud controls, including interdiction lists, SAR customers, investigation results and fraud typology statistics will help the organisation mitigate consumer fraud losses and implement future process improvements. A consumer fraud hotline allows customers to report instances of fraud directly to the financial crime department. Finally, companies should continuously monitor their fraud detection techniques and make improvements to enhance overall programme effectiveness on an ongoing basis.

Hartley: We all know that fraud is an opportunistic beast and will attack any vulnerabilities. The key principle in my view is to admit to your failings or vulnerabilities. No one can afford these days to take the stance that it can never happen to you or your business. For this to happen you need to know what your areas of weakness are. If you know what your exposure is then you can plan and mitigate. Once you have identified your vulnerabilities, you can then focus on those and see what gaps may appear in your control system. This process needs to be regular and systematic to be effective. Of course, all will be for nothing if there is no effective leadership or governance from the top of an organisation. A lack of corporate governance undermines most things but fraud risk especially so. Whilst a risk assessment may not be necessary for each and every business model, it should be recognised that each industry, sector and sub-division will have different risks associated with it. Careful consideration should therefore be given to having a bespoke set of processes in place.

FW: When it comes to investigating actual or potential cases of fraud or corruption, how important are forensics and expert insights? What fraud investigation techniques and procedures are typically deployed to gather evidence from technology to prove wrongdoing, particularly in cases where data has seemingly been erased, corrupted or destroyed?

Hartley: Expert witnesses of course have their place, but you need to be able to access the data in full for them to be able to conduct the task from start to finish. An expert witness in court carries significant weight when the data and subject material is subject to interpretation. Technology-enabled investigations are now indispensable and typically most investigations will commence with electronic data review before speaking with a subject. Any corporate body will have access to digital material in house whilst law enforcement agencies will have the power to seize computers, servers, mobile phones and anything else that has storage capability. In criminal investigations I have seen a dramatic increase in the use and interpretation of metadata as this digital footprint on a document can reveal so much information. This has revolutionised the way in which cases of false invoicing and forgery are investigated. An act of destroying data itself may well be indicative of a certain type of behaviour and if there is evidence that material has been deliberately destroyed any prosecutor would seek to try and have that admitted as a standalone piece of evidence. Many governments have in place legislation to try and avoid those who are the subject of an investigation from becoming aware of the fact in an effort to preserve material. In the UK, the offence of 'tipping off' under the Proceeds of Crime Act carries a potential maximum sentence of two years imprisonment. In the digital age it is of course almost impossible to delete data completely. Data is constantly backed up, more often than not in more than once place.

Angotti: It is common for criminals to try to hide their illegal activity by destroying digital evidence that would shed light on their actions. Fortunately for fraud investigators, it is actually very hard to complete this task. A document or email is not gone just because you click on the delete button. Electronic documents create

> "AN INCREASING NUMBER OF COMPANIES ARE ABLE TO ACCESS MACHINE LEARNING SYSTEMS (MLS) AND AI TO DETECT FRAUD. THE COSTS OF THESE SYSTEMS ARE COMING DOWN AND IT IS A QUICK SOLUTION."
>
> JOHN HARTLEY
> Shoosmiths LLP

'trace evidence', which leads to a trail of details regarding the history and contents of the document. It takes a sophisticated effort to remove trace evidence. Forensic tools are often used to analyse trace evidence and these analyses can identify if documents have been deleted, who deleted the documents and when the documents were deleted. In addition, it is also possible to recover the contents of documents that were deleted. Audit trails from access logs and IP addresses can be triangulated against other systems, such as building security systems and phone records, to identify when data has been tampered with or removed. Cyber tools can identify brute force password hacking attempts, for example. The findings from these analyses have been used as the primary evidence to generate leads and prove illegal activity.

> ELECTRONIC DOCUMENTS CREATE 'TRACE EVIDENCE', WHICH LEADS TO A TRAIL OF DETAILS REGARDING THE HISTORY AND CONTENTS OF THE DOCUMENT. IT TAKES A SOPHISTICATED EFFORT TO REMOVE TRACE EVIDENCE.
>
> ALMA ANGOTTI
> Guidehouse

FW: What advances are you seeing in efforts to track, trace and recover the proceeds of fraud?

Angotti: The Fraud Act 2006 shifted the UK anti-fraud legal framework's focus away from victims to perpetrators. Almost 15 years later, we do not have a comprehensive victim-centred strategy to track, trace and recover the proceeds of fraud. Industry-led initiatives have tried to bridge these gaps. The Dedicated Card and Payment Crime Unit brings together police, financial institutions and the public and has been an innovator in the fight against fraudulent schemes that use new technologies, such as social media. Since 2016, the Banking Protocol has also played a crucial role in protecting vulnerable people from fraud. In 2019 alone, the Banking Protocol prevented around £49m in fraud and led to 253 arrests. The Protocol will become even more important as societies recover from COVID-19. However, we need to do more to help vulnerable communities with APP fraud. COVID-19 is changing the fabric of social interaction as we know it; less tech-savvy individuals will, unfortunately, be primary targets for fraud.

Hartley: The UK is one of the leading countries for asset recovery work in both civil and criminal courts. Almost every case that results in a conviction in the Crown Court can now lead to some form of financial investigation if the prosecutor considers it appropriate. The primary legislation in the UK is the Proceeds of Crime Act and under the rules there are essentially two figures placed before the court – benefit and realisable. The former is the amount that was made as part of criminality and the latter is what the defendant has available. There need not be a direct link between the criminal act and the available asset. Therefore, if the defendant inherited a property that was unconnected to the criminal act, for example, it can still be taken into account as an available amount and dealt with accordingly. While it is therefore a powerful tool for a prosecutor, the victims remain largely powerless.

FW: To what extent is technology helping to both detect fraud and aid asset recovery? Will anti-fraud technology only continue to become more integral to company systems and processes?

Hartley: An increasing number of companies are able to access machine learning systems (MLS) and AI to detect fraud. The costs of these systems are coming down and it is a quick solution. MLS use computer algorithms that 'learn' patterns in databases so that they can adapt and improve automatically to detect potential fraudulent scenarios. When implemented by an organisation, MLS can detect fraud by finding hidden and implicit correlations in data in real time. There are two types of MLS: supervised and unsupervised. Supervised MLS can be used when the company knows which data is fraudulent and the MLS then attempts to learn the patterns in this data. Unsupervised MLS are different and are used when the company does not know what data is fraudulent. Unsupervised MLS are asked to learn the data structure on their own. MLS are presented with the data so that they can attempt to understand the underlying structure and dimensions of that data and therefore detect whether it is fraudulent. Companies that use MLS to detect fraud usually use a combination of supervised and unsupervised systems.

Angotti: Fraud technology tools can help detect and deter fraud, and many companies use these tools in all aspects of their operations, including in the accounting, vendor management and procurement departments. These tools can be calibrated, based on the business's activity, to identify red flags of potential fraud that will provide fraud investigators with valuable information to further investigate the anomalies. The presence of these tools is also a strong deterrent for criminals. In terms of asset recovery, technology tools can quickly ingest and

analyse financial records to determine where and when funds were sent and received. Technology can also be used to identify patterns of transactions, and maybe more importantly, to identify behavioural patterns and networks of transactions that can more easily identify fraud. This has become much less of a manual process and allows professionals to quickly focus on the key areas in a recovery effort. These tools will also catalogue evidence and maintain a proper chain of custody for litigation purposes.

FW: How do you envisage the nature of fraud risk in the UK developing in the years ahead? Are there any specific trends you expect to emerge?

Angotti: Financial crime across the globe is expected to rise in response to the uncertainty resulting from the COVID-19 pandemic. We have recently seen fraudsters using the internet to exploit victims' natural anxieties around COVID-19 to steal both their money and personal information. The City of London Police reported a 400 percent increase in COVID-19 related fraud in April 2020 and Action Fraud recorded a total of nearly £970,000 due to COVID-19 related fraud since February 2020. In nearly all cases, criminals used cyber fraud to target their victims. For example, Cifas reported that some individuals using Microsoft's Office 365 platform were targeted by a phishing campaign that featured COVID-19 information as a lure to convince them to provide personal credentials. Users received an automated message that purported to be from DocuSign carrying a link to a COVID-related document. The malicious link to the document employs a page that looks like a DocuSign login page that steals their credentials. Companies must adapt their processes and controls to support their customers and meet regulatory requirements.

Hartley: The risk of fraud will always be present. I doubt that it will ever be eliminated as it is driven by people who are dedicated to finding novel ways of making money. Greed is a trait that will always be there and so with it risk. As technology and governance advances, so too will the tools used to circumvent them. Likely targets will be new and emerging areas, such as the continued development of virtual reality, machine learning and artificial intelligence technology. Unfortunately, as organisations invest in the emerging technology used to detect and combat fraud, fraudsters will also be using it too. As we are living in an increasingly cashless society, there needs to be a focus on protecting those card not present transactions. The introduction of SCA will no doubt assist in protecting the consumer at the point of transaction. However, this may in turn lead to an increase in the number of cyber attacks on businesses that hold account details. ■