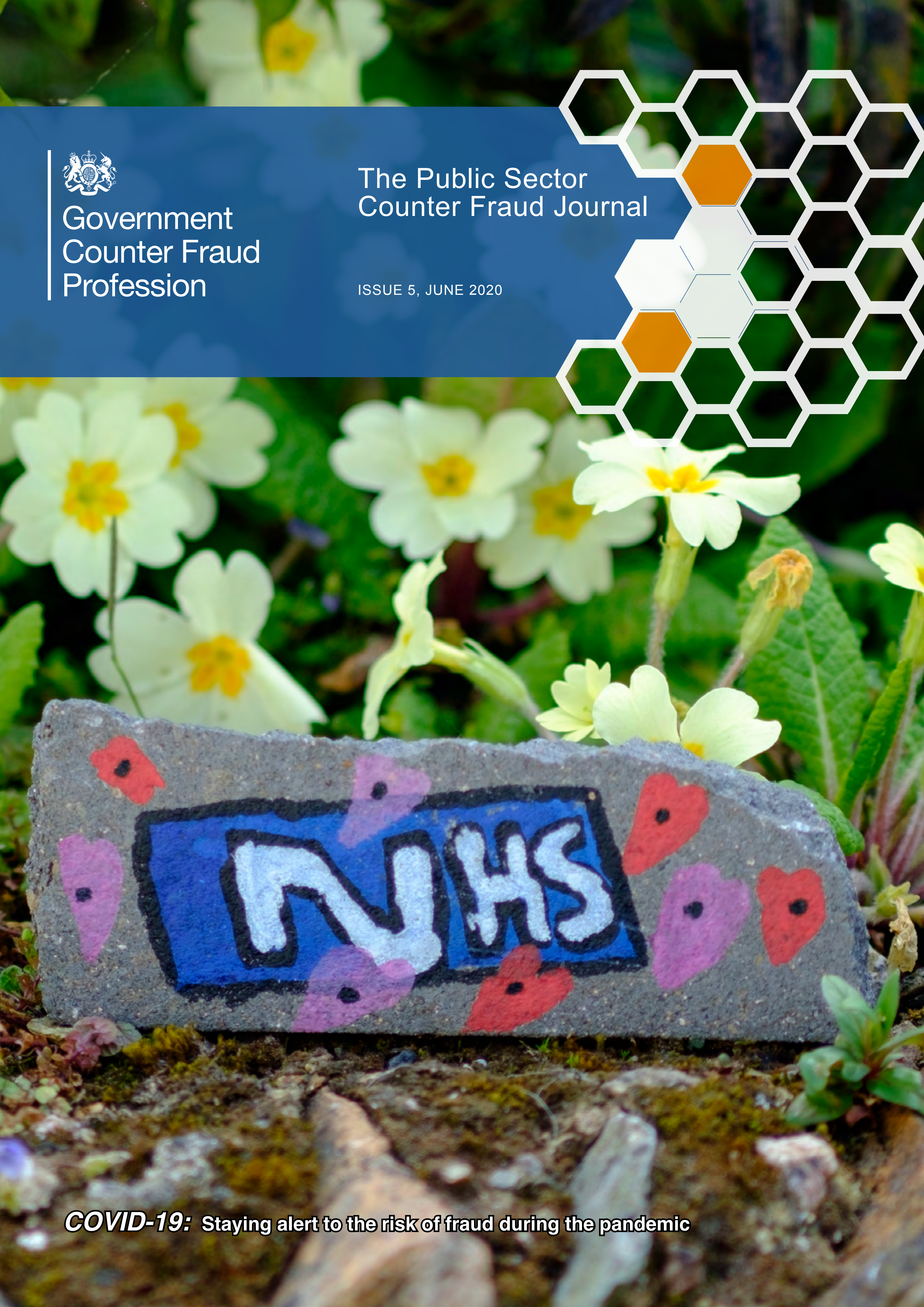
Government
Counter Fraud
Profession

The Public Sector Counter Fraud Journal

ISSUE 5, JUNE 2020



COVID-19: Staying alert to the risk of fraud during the pandemic

Editorial Board

Toni Sless
Chair and Founder
Fraud Women's Network

Jackie Raja
GCFP Development Lead
Department for Work and Pensions

Professor Mark Button
Director of the Centre for Counter Fraud Studies

Mark Cheeseman
Director
Counter Fraud Centre of Expertise, Cabinet Office

David Kirk
Consultant Barrister
RS Legal Strategy Ltd

Maria Kenworthy
Investigator
Ministry of Justice
Counter Fraud and Investigations

Mick Hayes
National Operations Manager
NHS Counter Fraud Authority

Cover image: Pebble painted in NHS colours photographed by Ross Burton, is licensed under CC-BY -NC-ND 2.0

CONTENTS

4 - Editor's Letter and Foreword
6 - Fraud: A wider perspective
8 - The Government Counter Fraud Function's COVID-19 Response
10 - COVID-19: Maintaining a controlled environment
12 - How prepared are insurers for the risk of increasing fraud during and after the COVID-19 pandemic?
15 - Carpe Diem; Seize the day, make a change
16 - Protecting charities from harm: Fighting fraud and cybercrime
18 - Coronavirus, fraud risk, and the use of the term "scam"
20 - Digital detectives in the NHS
22 - How the UK justice system has adapted to the COVID-19 pandemic
26 - COVID-19: The risk of fraud in a crisis
28 - Hunting the elusive Black Swans

Editor’s letter

In the last issue of the Public Sector Counter Fraud Journal we discussed the prevalence of fraud in emergencies and how this could be managed while still ensuring aid reaches those who need it. The COVID-19 pandemic has brought a whole new set of challenges within the UK government moving to an emergency management footing and quickly implementing stimulus schemes.

We have all been affected by COVID-19. At the very least it has changed how we live our daily lives, how we live, work, socialise and our personal finances. Unfortunately, for many people, the impact has been far more significant.

Criminals exploit fears over the pandemic, targeting individuals, businesses and the public sector, with an increasing risk of causing human harm and limiting the impact of the stimulus measures. Some people will be more likely to commit fraud than they would have been otherwise.

During the current pandemic, there are equally multiple pressures on the insurance industry. Companies face an increase in claims and, due to the economic impact of the pandemic, an increase in fraudulent claims. In this issue **David Phillips** considers this, but also how counter fraud capability in the insurance industry has been improved over the years. **Oliver Powell** and **Sophie O’Sullivan** outline the changes that have been made to keep the courts functioning but also how the ways of working necessitated by COVID-19 may actually prompt lasting changes to the legal system.

The impact of COVID-19 is having a profound effect on the legitimate economy, but **Justine Currell** reports on how modern slavery victims are exploited and how the pandemic has already changed this.

Neil Green recounts the story of Gregor Macgregor, an ambitious criminal in the 1800s who lured people with the promise of a new life. Neil talks about the hazards of trusting without verification and gives some examples of real cases where this has gone wrong. **John Baker’s** article also builds on this further, listing some effective measures organisations can take to reduce the risk of fraud, even in the less-familiar environment in which we are now working.

Charities are the focus of **Alan Bryce’s** piece, summarising the comprehensive research undertaken by the Charities Commission and Fraud Advisory Panel into both fraud and cybercrime risks faced by charities.

Dr Rasha Kassem and **Mike Betts** again discuss the importance of using the right language in talking about fraud and the potential dilution of its significance if we fail with this.

Nikki Crook explains how the NHS Counter Fraud Authority operates in the challenging environment of the health service. **Jackie Raja** reflects on her career and how she has taken up an opportunity to use her counter fraud expertise in a new way.

We hope that there is something in the Public Sector Counter Fraud Journal for everyone. It’s an opportunity to showcase the excellent collaborative work happening, learn about less-familiar sectors. But it is also a space to reflect on fraud and how this complex and evolving crime necessitates a strong counter fraud community to find it, and to fight it.

Chris Freeman
Head of Engagement and Membership
Government Counter Fraud Profession

Foreword

Welcome to the fifth issue of the Public Sector Counter Fraud Journal. It is so great to see this journal grow to become now an established, regular and valuable publication - full of great quality articles that challenge us to think differently.

Thinking differently is something that we all need to call upon in our current context. The world is in the grip of a pandemic the like of which none of us have experienced before. It is bringing with it new challenges, new fears and changes to the ways we work and live. For many of us, the comparative 'normality' of 2019 can feel like a distant echo. Like a familiar acquaintance with whom we are, for now, distanced.

We are currently living through the pandemic, and the uncertainty it brings. We are still understanding how it will affect our lives, whether there will be a new 'normal' (as we live with this virus for an extended period) or whether this will be a more short term shock.

The government has acted at pace to support individuals, communities and the economy. In the space of a few weeks, the government stood up support schemes to get money to businesses and individuals, bought supplies for the Health Service in a competitive international market and dealt with a huge increase in demand on government services.

Sadly, in times of crisis, the threat from fraud increases. This is something that has been seen time and time again across the world. We know that many of the schemes that have been developed are facing an inherently high risk of fraud. We also know that many, hard working, dedicated public servants have worked hard to try and reduce these risks. Nevertheless, the risk and threat level remains higher than it was in our distant echo of 2019.

One of the positives coming out of the pandemic has been how the Government's Counter Fraud Function, those people across government who work to fight fraud against the public sector, has come together to deal with the increased fraud threat. We are sharing information on risks, intelligence on potential fraud and best practices, tools and techniques for fighting it on a scale and at a pace we have not seen nor done before. The threat may be higher - but the response is rising to meet it as best it can.

I would like to thank all of those in counter fraud roles for their hard work during the pandemic, whether it has been to support the understanding and reduction of fraud risk in the stimulus effort, continue the important work of finding and fighting fraud against the public sector, or switching into other roles to help support areas of increased demand. You have shown adaptability and commitment and should be proud of the impact you have had.

The pandemic, and our response to it, is likely to be a priority for the foreseeable future. For those working in fraud roles, we will continue to have an important role to play in both finding and dealing with fraud during this period and finding ways to reduce the risk of fraud in any future spending. We know that our adversary will remain committed, and that we will have to remain equally committed. Committed to detecting fraud, to learning from our experiences, to finding new ways to stop those who want to commit fraud, and to thinking differently.

Mark Cheeseman
Director, Counter Fraud Centre of Expertise, Cabinet Office

Fraud: A wider perspective

COVID-19 has presented us with so many challenges locally, nationally and globally. Not just the important changes to the way we live, work and socialise, but also some new challenges from the fraud threats we face. These new challenges, combined with our known existing fraud threats, have made the virtues of vigilance and diligence more important than ever.

About the author:
Neil Green,
Deputy Director, Counter Fraud and Investigation, Government Internal Audit Agency

My team's unique position, at the very heart of government, enables us to obtain valuable insights and provide a wider perspective on the fraud threats faced by the public sector.

Counter Fraud and Investigation joined the Government Internal Audit Agency in 2016, as an internal fraud investigation service, but realised very quickly we had a depth of knowledge that afforded a fuller understanding of the entire fraud landscape which placed us in a position to offer our services and expertise to those requiring support. So far, we have worked collaboratively with more than 70 organisations. Not bad for a relatively small team! We may be small, but we pack a big punch in terms of presence and contribution. Our close involvement in the development of both the Government Counter Fraud Profession and Counter Fraud Framework is testament to this.

Age old threats...

The latest estimated losses due to fraud to UK Government each year is between £2.8 - £22.6bn. A staggering amount, I'm sure you'll agree. Considering the estimated costs of COVID-19 are £2.5bn per day, the need to be vigilant is paramount.

In this cyber age, one would imagine the major threats facing government are 'high-tech' and complex and to detect such fraud, would need sophisticated tools and software. Often this is true but what if the nature of some of the existing and emerging threats has been the same since the beginning of time. Few are familiar with the Poyais Fraud of the 1800s, where Gregor MacGregor, of the British Army, created an entirely fictitious country and sold the dream of a better life to hundreds of people.

This was deception on a grand scale, based mainly on trust. MacGregor was held in high regard, was well travelled and fought for his country. He was credible and provided 'evidence' to support his fraud. It took MacGregor's victims a long journey to Central America to discover the fraud and cost many lives as well as livelihoods. Often identifying and tackling fraud requires little more than human intuition and basic diligence.

Trust, but verify

Of course, new threats are constantly emerging. The COVID-19 crisis has demonstrated this very clearly. At the same time existing threats evolve and we must adapt our approaches to tackling fraud in response. In our four years working across government, we have seen recurring types of fraud, where the prevention of contributing factors should be easily within our grasp.

Let's talk about trust, or more accurately, misplaced trust. This is often a theme running through our work. Finding that the trust you placed in a colleague or supplier has been abused is obviously upsetting. But this doesn't mean we should simply not trust people; when it comes to tackling fraud, trust only goes so far and without appropriate checks and balances, can come with a heavy cost.
Checking the work or credentials of someone you trust, goes against human nature, to see the good in others. It would be unhealthy to live our lives suspecting everyone could be guilty of wrongdoing. So, whilst trust is an integral part of society, so is our instinct to safeguard what's important to us by reducing risks and taking simple precautions. The phrase 'trust but verify' became internationally known when used repeatedly by President Ronald Reagan during the 1980s Cold War with the Soviet Union. Ironically, its origins are from a rhyming Russian proverb, however, the phrase is very relevant in a counter fraud context.

Trust can be built in layers. First you should ask yourself: "Do I have any reason to doubt integrity"? Over time a more comprehensive degree of trust is based on observing and verifying ongoing behaviour. In other words, do someone's actions continue to reinforce your trust? From an organisational perspective, although we do trust our colleagues, we must still have measures, structures and processes in place to check and verify actions, especially those where opportunities exist for fraud. Implementing effective measures, such as segregation of duties and

A Bank of Poyais "dollar", printed in Scotland. MacGregor bartered these worthless notes to his would-be settlers, taking their real British money in exchange. Image source: National Numismatic Collection, National Museum of American History at the Smithsonian Institution

proportionate checking regimes, where those involved are aware of their responsibilities and how to deliver them, should be a given but they are only as effective as the diligence applied to them. Failing to do this has serious consequences.

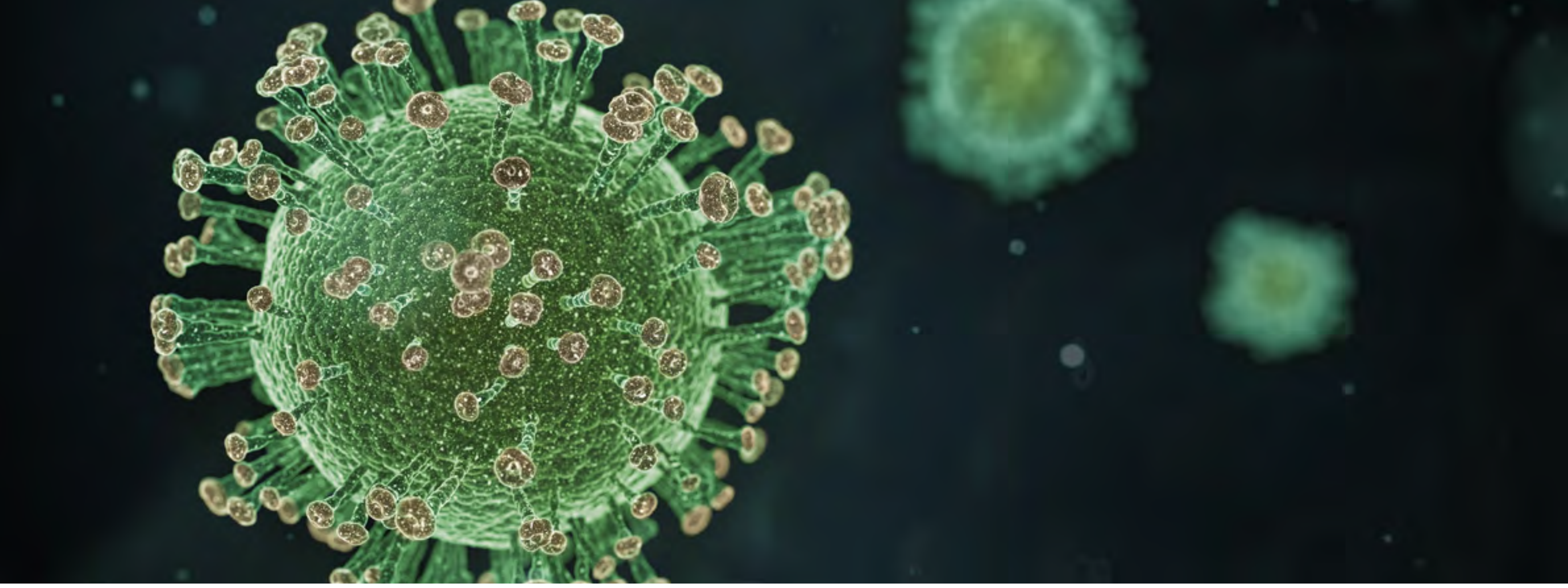
Two investigations come to mind which demonstrate the importance of the trust but verify principle. In the first, the perpetrator embarked on a plan to defraud an organisation by abusing their senior position and using their insider knowledge to 'stay under the radar'. So how did they do it? Planning, knowledge of the business and, importantly, developing and using a relationship with an officer integral to the process.

So, whilst trust is an integral part of society, so is our instinct to safeguard what's important to us by reducing risks and taking simple precautions.

The fraudster built a relationship with an Approving Officer, which meant documents were authorised on an 'as it's you' basis rather than being examined properly. This enabled the fraud to continue, despite the organisation having processes in place, which should have detected (or at least questioned) the fraudster's action. The fraud continued until it was finally questioned, and verified, by someone new to the team.

The second case involved mandate fraud. I'm sure you're familiar with this type of fraud, where a fraudulent request to change a direct debit, standing order or bank transfer mandate is received, claiming to be from an organisation to whom regular payments are made. Although one of the most straightforward types of fraud, it continues to grow year on year. Where successful, the stolen funds which can be significant, generally leave the UK quickly and attempts to trace or recover the funds are often futile. This means that detecting and disrupting the fraud, rather than reacting to it are even more important.
In this case a fraudulent request was received to change bank account details of a supplier. The request, despite being poorly completed, with numerous spelling mistakes, cleared all internal financial controls. A payment of approximately £12 million was issued to the new account. The recipient bank identified that names on the account and credit transfer did not match. Fortunately, due to the bank's diligence, the funds were not released. There were clear 'red flags' in this case and not just those typically found in mandate fraud. A combination of failures to apply basic controls and set procedures for managing and verifying payment change requests, limited fraud awareness and our old friend trust without verification contributed to the fraudulent attempt.

Trusting, but having the appropriate checks and balances in place is not the same as not trusting. It is basic management and governance. As the cases highlighted here show, not having robust processes in place can have significant consequences. Trust me…



The Government Counter Fraud Function's COVID-19 response

Sadly, in emergency management circumstances, experience tells us from the Australian bushfires to Hurricane Katrina in the United States that the threat from fraud and the likelihood of irregular payments increases.

Therefore, when HM Government pivoted to an emergency management footing and introduced a comprehensive package of stimulus schemes totalling £440bn, the Government Counter Fraud Function recognised the need to support departments, agencies and local authorities to understand, find and reduce fraud, mitigate its impact and help the stimulus spend to go as far as possible. There was a need to respond rapidly to an evolving demand of deploying funds as quickly and as safely as possible.

Collaboration of the Function

The function has come together like never before to understand, stop and prevent COVID-19 fraud.

Many agencies opened up intelligence to the centre, and across agencies, to allow for timely dissemination to the public sector to prevent and disrupt fraud where it could. This includes working across traditional law enforcement and public sector boundaries. The types of information and pace at which it shared was key in our success at tackling the harm caused by fraud during COVID-19.

We have collaborated with our international partners to share best and leading practice in fraud management and control across public borders. This is informing our approach as we support other functions in their response to COVID-19 and the unique demands it has created in areas such as procurement.

About the author:
Rob Malcomson,
Head of International Counter Fraud and COVID-19 Response, Cabinet Office

Counter Fraud Response to COVID-19 so far

Great work is happening across the function within government departments, too. For example, DWP used their integrated risk and intelligence service (IRIS) to identify and target the response to attacks by organised crime groups. HMRC pivoted fraud investigation, compliance, risking and cyber teams to focus on COVID-19 specific threats and Department for Health and Social Care have benefited from new flows of intelligence from the NCA, enabling them to react to potential fraud more quickly.

In the Centre of Expertise, we set up a dedicated counter fraud team that could understand the fraud risk at a global level and within specific stimulus schemes. We are supporting departments to understand the fraud risks by embedding expert fraud risk assessors in the teams designing and delivering the stimulus programmes. In doing so, we are able to recommend upfront low-friction countermeasures to help reduce the specific fraud risks identified.

Countermeasures to Protect Stimulus Scheme Spend

Alongside our colleagues in the Government Internal Audit Function and National Audit Office, we have provided direct and 'hands on' support to departments, supporting the existing fraud capability and deploying low-friction upfront

Coronavirus (COVID-19) - CG Illustration by Yuri Samilov is licensed under CC BY 2.0 countermeasures to prevent fraud without slowing down the stimulus payments.

We have implemented countermeasures, such as the Bank Account Verification tool, to prevent and detect fraud where possible. The Bank Account Verification tool assists public bodies to verify the bank accounts of payments before payment. This is supported by the Active Account Checker which will effectively assess the risk of paying invalid, fraudulent or high risk accounts.

We have also laid the foundations in stimulus scheme packages by putting in legal frameworks. This will allow public bodies to recover irregular payments and to pursue legal action where fraudulent activity is identified. We've also compiled the correct data upfront which will help public bodies later determine who is eligible for financial support.

The Impact of COVID-19 on Government's Counter Fraud Work

We recognise that fraud will still happen against departments and programmes during the COVID-19 response. As a function, we are monitoring our ability and capacity to fight it.

Therefore, we have been monitoring the impact of COVID-19 on departments' counter fraud resources from COVID-19 related illness, redeployment and operational disruption from social distancing measures.

So far, departments have experienced minimal impact with, for example, some delayed investigations or prosecutions however, overall it is manageable.

Longer Term Implications of COVID-19 on Counter Fraud

As set out in the Fraud in Emergency Management and Recovery Guidance, the extent to which up front, preventative, counter-measures can be implemented will be limited. As such, it is important that post event activity is undertaken to establish whether the fraud risks established and understood came to pass. Using the fraud risk assessment created during policy and process design, departments are advised to carry out post-event assurance work to check for instances of fraud.

We recognise that departments have a lot of experience in developing post event assurance plans. However, the context of the COVID-19 response represents a challenging environment to make payments at pace whilst applying judgements where the fraud threat is significantly heightened. Therefore, the Government Counter Fraud Function, the Government Finance Function and the Government Grants Function have come together to provide guidance on how to implement post event assurance activity – informed by leading practice across the public sector. You can contact the counter fraud team by email to receive your copy.

For further information, please get in contact with the team:

covid19-counter-fraud@cabinetoffice.gov.uk

Aligning with HMG's Strategic Objectives

Our response tied directly into the government's three of the COVID-19 strategic objectives:

Undertake dynamic fraud risk assessments of COVID-19 impacts, using the best available expertise and evidence to inform decision-making.

We used the best available expertise and evidence to map stimulus spend, understand the fraud risk which informed the design and delivery of the stimulus programmes.

Maintain trust and confidence among the organisations and people who provide key public services, and those who use them.

We worked with departments to develop countermeasures to improve the integrity of the stimulus programmes and reduce irregular payments whilst instilling trust in government's handling of the pandemic and helping the support get to where it was most needed.

Minimise the potential impact on society and the UK and global economy, including key public services.

We helped to reduce the economic and human harm by coordinating and acting on fraud threat intelligence with law enforcement and cyber security. We also laid the groundwork for the post event assurance work to minimise the potential impact on the UK economy.

COVID-19: Maintaining a controlled environment

Keeping safe from Coronavirus (COVID-19) is at the forefront of everyone's minds across the globe. Unfortunately, fraudsters have quickly taken advantage of the disruption and depleted staffing levels to attack organisations and individuals on an increasing scale.

Author:
John Baker,
Director, BDO UK

With reduced staff levels likely to continue for some time and home-working widespread, it is vital to ensure that controls are maintained. Above all, this means making sure that everyone knows what these controls are and applies them. Well-designed controls rarely fail themselves; any problems are more likely to stem from an organisation's people.

The current environment is particularly challenging, however. In reality, many controls will slip due to operational urgency, staff shortages and lack of training for those replacing staff who are ill. Given the social distancing in place, face-to-face meetings are no longer available. Documentation is more likely to be provided electronically, which can make it harder to validate. Increased home-working may give people a false sense of security, even though the control environment may be weaker.

Fraudsters will, without doubt, try to exploit the situation by circumnavigating segregations of duties, especially in finance, HR, procurement, contracting and other payment authorisations. It's likely, for example, that bank mandate fraud will increase as criminals exploit any weaknesses created by key personnel being overstretched or unavailable.

Organisations can fight back by reviewing their checks and controls to ensure they are suitable for mass home-working. For example, video-conferencing can be encouraged to replace face-to-face meetings and reduce the risk of mistaken identities. HR should focus on agency and temporary staff pre-employment checks to ensure recruits are suitable, especially in high-risk areas such as finance and procurement.

Above all, to reduce the risk of fraud, it's important to remain professionally sceptical and cynical, both at work and home. This means not only looking out for scam messages and emails, but also taking the time to revisit your fraud risk assessments to ensure that business continuity plans take into account the rapidly emerging fraud risks.

Your organisation's response to the heightened risk of fraud needn't be complex, however. There are some simple things you can do to reduce fraud risk. Here are a few suggestions:

- Remind staff of their job descriptions and obligations, highlighting any controls for which they have responsibility.
- If not done so already, key controls should be process-mapped and walked through to test them against the current situation. They should then be revisited every time there is a change to staffing, processes or legislation. Even a small change can create an opportunity for exploitation – remember that the strongest chain is only as effective as the weakest link.
- Remind staff of the need to maintain the highest levels of security while home-working. Open tabs on laptops and PCs should be closed down and laptops switched off and stored securely when not in use.
- Be cautious in dealings via email and telephone, remembering that fraudsters can hijack communications in convincing ways.
- Ensure new staff (or staff deployed to new tasks) receive the proper levels of training in applying controls and conducting checks.
- Seek corroboration and additional supporting documentation where appropriate.

Fraudsters thrive on urgency, confusion and change – so now is, unfortunately, a perfect storm. You and your colleagues

may feel under pressure to take decisions swiftly. Fraudsters will create a false sense of urgency, pushing people into making bad decisions or overriding controls. Protect your organisation by applying these guidelines:

- Before you take any actions: pause, reflect and check.
- Check your levels of authorisation on a daily basis. Who is available? If people are put into positions to cover more experienced colleagues, have they received the basic level of training to do the job properly and have they been vetted thoroughly for the role they are doing?
- If being pressured for action that would require controls to be circumvented, consider whether it could wait a few days. Most people are very understanding of the current situation and will probably accept a delay.
- Make sure you know who you are dealing with. Check the provenance of emails and calls before you take any actions, especially in relation to payments, money transfers and, most importantly, changes to bank accounts.

Above all, to reduce the risk of fraud, it's important to remain professionally sceptical and cynical, both at work and home

The COVID-19 outbreak may be requiring some organisations to operate more flexibly, but established policies still apply. It's vital to make sure that staff continue to comply with all essential policies and processes, whilst also staying up-to-date with your organisation's guidance and advice. And, if any changes have been made to working patterns or duties, it's worth testing controls to ensure the organisation is not put at risk.

The need for such vigilance is likely to be required for some time to come, as fraudsters will continue to look for opportunities to capitalise on the pressures that organisations and their staff face. Your best defence is to be sceptical. Never be tempted to take things at face value. Before taking any action, always stop, think and check. And remember, trust is not a control.

Sheffield's Women of Steel photographed by Tim Dennell is licensed under CC BY-NC-2.0

How prepared are insurers for the risk of increasing fraud during and after the COVID-19 pandemic?

General insurers face the continuing challenge of preventing and detecting fraud. Insurance fraud impacts on society at large as valuable public resources, such as those in the NHS and courts, are spent in dealing with fraudulent cases. Unfortunately, it is the honest policyholders who are the true victims of insurance fraud. They may have to pay higher insurance premiums as the costs of fraudulent claims are passed on to customers.

At these times insurers remain committed to providing excellent service and paying all genuine claims as quickly as possible. It is important to stress from the outset that the vast majority of policies and claims that insurers deal with on a daily basis are genuine. Sadly, a small minority of individuals and businesses, who either through greed or finding themselves in financial difficulties, will attempt insurance fraud.

Author:
David Phillips MA,
Claims Validation Technical Manager, NFU Mutual and ABI General Insurance Fraud Committee member

Insurance fraud can be seen in all areas. With policy application fraud, a prospective policyholder may deliberately or recklessly provide false information when applying for insurance. The lies told by the applicant are fraudulently used to either obtain cover they would not usually be entitled to or to reduce the premium. It can happen during the lifetime of a policy where falsely obtained policy documentation is used to support other financial criminal activity. It is seen in claims where a policyholder or third-party claimant creates a false claim, or dishonestly inflates the value of an otherwise genuine claim. In some extreme cases, there are highly organised criminal gangs, for example fraudsters involved in 'crash for cash' motor fraud scams. Insurers will also be aware of the risk of fraud perpetrated by so-called professional enablers (such as rogue accident management firms) who orchestrate insurance fraud, often to the detriment of unwitting and innocent claimants.

Fraud remains a significant threat to the insurance industry. So, to protect honest customers, the industry has invested, and will continue to invest, significant resources in deterring and detecting insurance fraud. Insurers invest at least £250 million each year to detect and identify fraud.

What is the scale of the problem? In 2019 the Association of British Insurers (ABI) reported that, during 2018, general insurers were uncovering some 1300 insurance scams every day, with the average value of these scams being £12,000. These results arose in, what could be considered as, a generally stable economic climate.

There is much academic research and several studies over some 30 years that report non-violent crimes are more likely to increase as unemployment rises. Fraud practitioners who are interested in more detail on the profiling of insurance fraudsters would do well to refer to the UK Government's report following the Insurance Fraud Taskforce of 2016. Recessions increase the risk of fraud for insurers.

The insurance industry is now preparing itself for the challenge that another economic downturn might bring. It is now widely reported by both government and financial commentators that the UK economy is likely to see a significant downturn due to the impact of the COVID-19 pandemic. This is and will continue to impact large parts of the population on an individual basis, as well as impacting businesses large and small.

The ABI statistics from around the time of the so called Great or Global Recession, circa 2007 to 2008, showed there were clear indications that the economic downturn led to an increase in general insurance fraud. So how prepared is the general insurance industry in 2020 to deal with the arising fraud risk that is now widely expected?

At the time of the last recession many insurers relied heavily on a manual intervention to detect fraud, with handling staff flagging suspicious cases. Manual intervention is still an important part of the insurer's counter fraud strategy. However now, compared to the last recession, insurance staff are better trained, their general counter fraud awareness and technical skills are far more advanced. Many insurers promote professional qualifications, such as through the Chartered Insurance Institute (CII).

In the last 10 years insurers have continued to develop and grow dedicated counter fraud teams. These counter fraud teams are far more technically astute, with dedicated validation teams in underwriting and claims. Counter fraud technicians regularly advance their competencies by undertaking professional counter fraud studies, such as the Accredited Counter Fraud Technician and Specialist qualifications. A great example of this is my own employer, NFU Mutual, who encouraged my counter fraud development, sponsoring me to obtain a Master of Arts in Fraud Management in 2013.

Back in the last recession some insurers did have in place anti-fraud systems, but with the majority of these in claims area. These were by today's standard very simplistic, looking for known fraud scenarios. In 2020 all insurers now use a variety of systems to detect fraud. Counter fraud technology now covers all areas, through quote, sales and underwriting, into and joined up with claims systems. These systems not only identify known fraud indicators but can also look further at insurance transactions in a more holistic way, considering the risk and threat an entity brings. Many systems now are self-learning, AI systems see and learn new emerging threats much faster than humans can. In fact, many insurers have dedicated counter fraud intelligence and fraud analytics teams.

In addition to insurers improving and building their own counter fraud capabilities, our industry has been building and growing a joined up strategic approach. I sit as a member of the General Insurance Fraud Committee (GIFC), a cross-sector group. It is a committee of senior fraud managers, the majority of whom hold a full-time role within one of the ABI member companies, Lloyd's Corporation and others. Formed in 2017, the GIFC's purpose is to 'develop and drive the general insurance industry's strategy to counter fraud'. It works to achieve this by:

- Providing technical advice, guidance and recommendations for the industry's counter fraud strategy;
- Identifying new threats to the industry and working on solutions to address these threats;
- Informing the industry's responses to government and regulatory consultation exercises; and
- Overseeing, reviewing and supporting the work of the core utilities

Some of these core utilities are accessible not only to insurers, but work has also been done to develop access for affiliate users such as brokers and law firms who are actively

involved in insurance counter fraud work.
At the heart of the core utilities is the Insurance Fraud Bureau (IFB), a not-for-profit company established in 2006 to lead the insurance industry's collective fight against insurance fraud. The IFB acts as a central hub for sharing insurance fraud data and intelligence, using its unique position at the heart of the industry and unrivalled access to data to detect and disrupt organised fraud networks. It helps insurers identify fraud and avoid the financial consequences. They also support police, regulators and other law enforcement agencies in finding fraudsters and bringing them to justice. The IFB also tries to raise public awareness of types of insurance fraud: how they work and how to spot them, so that the chances of being a victim of fraud are reduced.

Fraud remains a significant threat to the insurance industry. So, to protect honest customers, the industry has invested, and will continue to invest, significant resources in deterring and detecting insurance fraud.

An important part of the core utilities that insurers have access to is the Insurance Fraud Enforcement Department (IFED), a specialist police unit dedicated to prosecuting insurance fraudsters which was formed in 2012 by the City of London Police. IFED is in part funded by British and European insurance companies, through arrangements with the ABI.

Another recent core utility for insurers has been the development of the Insurance Fraud Register (IFR). The IFR went live in 2013 and is the first industry-wide database of known insurance fraudsters. It was developed by the insurance industry for the insurance industry to help prevent and detect fraud and its perpetrators. The ABI is the sponsor of the IFR on behalf of its members. The IFR is managed by the IFB in partnership with the ABI.

The most recent core utility now open to insurers is the Insurance Fraud intelligence Hub (IFiHub). This platform, which went live in 2019, was built for the insurance industry by the insurance industry. Insurers can now share, in real time, fraud intelligence in a consistent, efficient and secure way. It allows insurers to collaborate as new fraud threats emerge.

In recent weeks the ABI and GIFC have been overseeing the coordination of these core utilities to prepare the industry for the disruption and uncertainty that has been caused by COVID-19. GIFC issued a bulletin to insurers about the potential emerging threats that are and will be seen. The ABI has also issued a warning for people to be on their guard against criminals looking to cash in on the financial hardship that COVID-19 is causing. The warning highlights that fraudsters could offer bogus insurance products, steal money and personal data. Individuals and businesses are encouraged to be on their guard and report any suspicious activity to the industry's confidential Cheatline service at www.insurancefraudbureau.org.

Resource from within the IFB and from insurers' own intelligence teams and fraud experts has been coordinated to continue the work of building a strategic threat assessment looking directly at the ongoing economic situation COVID-19 now brings.

IFED are coordinating the investigation of criminal activity where consumers are being actively defrauded as a result of COVID-19 related insurance fraud or where criminals are attempting to use this time to perpetrate insurance fraud linked to the COVID-19 uncertainty.

As we have seen across the nation, it is only by working together, by sharing and combining resources, will we create an effective force to counter the risks and challenges the COVID-19 pandemic has brought to us all.

References:

Association of British Insurers (2019), Detected Insurance Frauds in 2018 available at https://www.abi.org.uk/news/news-articles/2019/08/detected-insurance-frauds-in-2018/ (Accessed: 15th April 2020)

HM Treasury (2016) Insurance Fraud Taskforce final report available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/494105/PU1817_Insurance_Fraud_Taskforce.pdf (Accessed: 15th April 2020)

Carpe Diem - Seize the day; make a change

Author:
Jackie Raja
Grants and Fraud Team, Department for Digital, Culture, Media and Sport

Who remembers Brexit? It's amazing how quickly one crisis can be so quickly replaced by another, and how our collective efforts to tackle can be re-purposed almost seamlessly.

During 2019, government departments were asked to provide staff to help the EU Exit 'no deal' effort, affectionately termed 'surge staff'. Many hundreds of Civil Servants changed roles overnight, either within their own departments or were loaned to new ones. In October, I agreed to take up an opportunity to work with the Department for Digital, Culture, Media and Sport (DCMS) in Whitehall, until the potential 'no deal' exit date.

For the last 41 years of my career I have been part of the Department for Work and Pensions (DWP) and its predecessors, starting as an Executive Officer on Supplementary Benefits (a forerunner of Universal Credit), eventually becoming national fraud intelligence lead, and then latterly lead for developing the Government Counter Fraud Profession. Moving Departments, even temporarily, adding to that a daily London commute to Whitehall, was well outside both my comfort zone and normal considered decision making, especially without initially knowing what the role was! It transpired that DCMS needed someone with counter fraud knowledge and some experience of team leadership to support some 'No Deal' preparation activity Having spent much of my career leading operational fraud teams, it did seem I might have something to offer.

I discovered that my knowledge was valued, I was asking the right questions, and was able to influence decisions on their policies and processes.

I found myself not only in a new department, but a new culture, with new ways of working, new IT systems and moving from operations to policy work. I also found myself amongst a wonderful team of inspiring people who were passionate about the great work DCMS does - of which I knew little. Now I know much more! I discovered that my knowledge was valued, I was asking the right questions, and was able to influence decisions on their policies and processes.

As we know, it transpired that 'No Deal' became 'Deal', however DCMS asked me to stay until January 2020 to help review their existing counter fraud strategy. The work took off, with more resources deployed. I was able to help develop a DCMS Strategy commitment to making fraud - and protecting public money - everyone's business, as well as working with their many arms-length bodies. I met many new colleagues and have made new friends. My loan to the department was extended to March.

And then came COVID-19…

As I write this, I'm still with DCMS, working on the Government response to COVID-19, which includes grants channelled through DCMS to various charities and other organisations. I'm helping to secure the programmes to ensure the money goes to those who most need it while protecting these vital funds from criminals. Our last Public Sector Counter Fraud Journal reflected on the challenges of 'disaster' fraud, and there are lessons to learn for the COVID-19 response about managing the risks. The pace has been frenetic, the challenges immense, and continuing.

In a rare quiet moment I reflected on the past seven months, considering how, as a counter fraud professional, I have been able to put my own knowledge, skills and experience, built over the course of my career, to use in a different way. From operations work to policy, to starting in a new department - if I can do it in the latter years of my career, anyone can.

The Government Counter Fraud Profession was set up to recognise the skills and knowledge of the counter fraud community and to enable exactly these types of opportunity, working across the Counter Fraud Function. Counter fraud professionals know their business and can share those skills in a myriad of situations, making a real difference. Policy experts will definitely have something to offer in operational roles, and vice-versa. I would encourage anyone within the Counter Fraud Function, when thinking about development and career goals, to consider what other opportunities may be out there to make a difference.

Having the chance to share my knowledge, and passion for my job, right at the heart of Government, during one of the most challenging periods for the UK in the last 100 years, has been a privilege. If you get that opportunity yourself - take it.

Protecting charities from harm: Fighting fraud and cybercrime

In recent weeks we have heard much about the threat that COVID-19 fraud and cyber-attacks pose to the public and private sectors. There is the same threat to charities. At the 2020 national fraud conference I spoke about the key findings of recent research into both fraud and cybercrime targeted against charities. Although this research pre-dates COVID-19, the prevention lessons that can be drawn remain valid and provide timely insights into how COVID-19 scams can be tackled.

Author:
Alan Bryce,
Head of Development Counter Fraud and Cyber Crime, Charity Commission for England and Wales

Understanding the threat

There is relatively little charity-specific research available to help understand the nature of the fraud or cybercrime threats facing the sector. That is why last year, at the Charity Commission we undertook, in partnership with the Fraud Advisory Panel, the largest ever charity fraud and cybercrime survey in the UK, and potentially worldwide.

We asked a representative sample of 15,000 registered English and Welsh charities to complete a voluntary fraud and cybercrime survey. This achieved an impressive 22% response rate, higher than many similar surveys in the private and public sectors, reflecting the increasing importance that charities now place on tackling fraud and cybercrime. For the first time we now have statistically significant, representative findings that inform our understanding of the fraud and cybercrime risk faced by charities. The results are generally encouraging. So, what were the main findings? Fraud first.

Perceptions of fraud risk

Charities are increasingly aware of the risk of fraud:

RNLI Lifeboats at Harwich, photographed by Andrea Kirkby,is licensed under CC BY-SA 2.0

- Over two thirds of charities (69%) think fraud is a major risk to the charity sector (51% in 2009);
- A third (33%) think fraud is a greater risk to the charity sector than other sectors (25% in 2009);
- In general, larger charities (particularly those that have suffered fraud) are more likely to acknowledge the risk of fraud.

However, there is still far more that charities can do to protect themselves:

- 85% of charities think they're doing everything they can to prevent fraud, but almost half don't have any good practice protections in place;
- Less than a third (30%) of charities have a whistleblowing policy (18% in 2009);
- Less than a tenth (9%) of charities have a fraud awareness training programme (4% in 2009);
- Charities believe they are vulnerable to fraud because of a lack of fraud awareness training (28%), and over reliance on goodwill and trust (26%) and/or excessive trust in one or more individuals (22%);
- Just under half (47%) think their charity contributed in some way to the fraud occurring, with nearly a third (30%) stating their charity was too trusting;
- A third (33%) did not report the fraud to any external organisation, such as the police or Charity Commission.

Cybercrime is a relatively new issue compared to fraud. Perhaps unsurprisingly, our survey showed that charities' perception of the threat is less developed

Of greatest concern is that over a third (34%) of charities think they're not vulnerable to any of the most common types of charity fraud - experience shows that even those charities with the strongest counter fraud defences will on occasion experience fraud. So, recognising potential vulnerability is an important step towards ensuring that counter fraud defences are both in place and operating effectively.

The results suggest that about a third of charities have yet to acknowledge the significant threat that fraud now poses to the sector, are unaware of the vulnerabilities common to charities that fraudsters seek to exploit and have yet to adopt good practice arrangements to increase resilience. The good news is that this can easily be addressed. For example, more than eight in ten frauds are identified as a result of a charity's financial controls or by audit or whistleblowing. Rigorously applying a set of basic controls can make the biggest difference and can be implemented with little or no additional cost.

Analysing charity frauds

- Mandate/Chief Executive Officer (CEO) fraud is the most common type of fraud targeted against charities. This is a type of social engineering, involving impersonation of legitimate organisations the charity deals with, or senior staff within the charity itself, usually conducted via hoax emails;
- Over half of charities (53%) knew who committed the fraud;
- Nearly two thirds (60%) of frauds occurred over a six month period.

The full results can be found in the Charity Commission report Preventing Charity Fraud, published in October 2019 as part of International Charity Fraud Awareness Week.

Perceptions of cybercrime risk

Cybercrime is a relatively new issue compared to fraud. Perhaps unsurprisingly, our survey showed that charities' perception of the threat is less developed:
Just over half of charities (58%) think cybercrime is a major risk to the charity sector;
Almost a quarter (22%) believe cybercrime is a greater risk to the charity sector than other sectors;
In general, large charities are more likely to appreciate the risk of cybercrime.

Analysing charity cyber attacks

- Phishing and malicious emails are the greatest cyber threat (39%), followed by hacking/extortion (15%)
- Over a third of charities (36%) don't know which type of cyber-attacks they're most vulnerable to.

Encouragingly, two thirds of charities took action to strengthen their defences after a cyber-attack, with revised IT security arrangements and new or updated training being the principal responses.

The future

Changing how charities think about fraud and cybercrime is key to making the charity sector more resilient. The starting point is to accept that every charity will, at some point, fall victim. In the digital age, with some 70% of frauds now cyber enabled, sadly this is inevitable. What matters is that charities can demonstrate they have done everything they reasonably can to prevent fraud and have arrangements in place to identify and respond appropriately when a fraud or cybercrime does occur.

With all the guidance and good practice now available, charities should feel empowered to play an appropriate, proportionate role in the fight against fraud and cybercrime.

The full results of the cybercrime survey can be found in the Charity Commission report Preventing Charity Cybercrime. Additional guidance and a range of free online resources are available at:

https://www.gov.uk/guidance/protect-your-charity-from-fraud

https://gateway.on24.com/wcc/experience/elitebba/1917599/2071337/charity-fraud-awareness-hub

Coronavirus, fraud risk, and the use of the term “scam”

The current Coronavirus crisis has increased the opportunities available for fraud criminals to defraud more victims. This requires all anti-fraud professionals, regulators, academics and the wider community to work together to counter the increased risk of fraud by using a clear and consistent prevent message. In this article, we raise awareness about the use of the term “scam”, and the continued debate and subsequent confusion over the meaning and scope of the word fraud.

Authors:
Dr Rasha Kassem*, Senior Lecturer in Accounting, School of Business and Law, Coventry University,*
Mike Betts*, Head of Learning and Counter Fraud Studies, CIFAS*

Confusion over the meaning of fraud and the words associated with it are not helpful in countering fraud or in making the language of fraud accessible to potential fraud victims, particularly in times of crisis. This article presents examples and current scenarios to highlight this confusion and to shed light on its impact. We believe there is significant merit in all key stakeholders revisiting the meaning of fraud in the 21st century, and to agree on common terms to harmonise the response and provide improved interoperability between organisations and sectors.

One of the issues we have come across is the use of the word “scam”. The actual meaning of this word is subject to debate. In the meantime, there is no evidence of the actual origin and validity of the word “scam”. In academic research and professional reports, the words “fraud” and “scams” are used interchangeably[1], while others believe there is a difference between scams and fraud. For instance, in a recent report by KPMG this year, scams are classified as one of the types of fraud.[2] This is seen again in the Home Office Counting Rules for Recorded Crime for fraud where the word scam is used to describe a particular fraud type i.e. Code NFIB1D “Dating Scam”[3].

The media also contributes to this confusion by using a variety of words to describe fraud including scams. For example, the headline from Sky’s Business Twitter account[4] shows phrases like: ‘Surge of ‘smishing’ scams as criminals exploit coronavirus crisis’. The continued use of other terms to describe fraud, including scams, smishing, and spoofing prevents the word “fraud” from resonating in the public’s conscience, which in turn, may reduce the likelihood of identifying fraudulent activities.

Conversely, banks differentiate between fraud and scam. From the bank’s perspectives, “scams” refer to those situations where the victim has been tricked into authorising a payment to a fraudster. A “fraud” is where a payment is made without the authority of the customer.[5] Yet, this distinction between fraud and scam is ungrounded and rather more confusing to fraud victims and anti-fraud professionals.

To clarify the meaning of fraud, the origins of the word fraud comes from the Latin word “fraudem” meaning ‘a cheating deceit’ which later evolved into the French ‘fraude’ deception, fraud.[6] This indicates that trickery and deception are at the heart of fraud. According to Cambridge Dictionary, a scam is an illegal plan for making money, especially one that involves tricking people. It is also defined as a fraudulent or deceptive act or operation according to the Merriam-Webster dictionary. Therefore, there is no distinction between fraud and scam.

After much debate, consultation and reflection The Law Commission[7] recommended that the offence of fraud is committed where, with intent to make a gain or to cause loss or to expose another to the risk of loss, a person dishonestly: (1) makes a false representation; (2) wrongfully fails to disclose information; or (3) secretly abuses a position of trust. These recommendations were

[1] *Stajano, F., and Wilson, P., 2011. Understanding scam victims: Seven principles for systems security. Communications of the ACM, Vol. 54 (3): 70-75*

[2] *KPMG. 2020. Fraud Barometer 2019. available at http://kpmg.com/uk*

[3] *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/877782/count-fraud-apr-2020.pdf*

[4] *https://twitter.com/SkyNewsBiz/status/1244581185088565249*

[5] *https://www.telegraph.co.uk/personal-banking/savings/scam-fraud-banks-mince-words-limit-payouts-victims*

[6] *http://www.lawcom.gov.uk/app/uploads/2015/03/lc276_Fraud.pdf*

[7] *http://www.lawcom.gov.uk/app/uploads/2015/03/lc276_Fraud.pdf*

encompassed in the Fraud Act 2006 which was intended to simplify the offence of fraud and make it accessible to all stakeholders concerned with investigating and prosecuting fraud. Therefore, the counter fraud community were presented with an excellent definition of fraud. However, we continue to use various words to define fraud, which it can be argued confuse and muddle, rather than clarify and simplify.

Therefore, we highly recommend and urge everyone to stop calling fraud a scam as there is no difference between fraud and scams[8]. Lincolnshire police in the United Kingdom also share our perception as they believe "There is no difference between fraud and scam, all scams ARE fraud". Using different terms to describe fraud will cause nothing but confusion. This confusion over the language of fraud will reduce the ability of anti-fraud professionals and fraud victims to identify fraudulent activities.

Confusions over the language of fraud will increase fraud risk, and could cost fraud victims even more, especially during times of crisis.

The language of fraud does not resonate in the public conscience like other crime types because fraud lacks its own personality and is often suffering from a multiple identity disorder.[9] Using a word like "scam" to describe "fraud" will dilute the actual meaning and harm caused by fraud as a crime. The language of fraud should be altered to better represent the reality of the impact of this crime. Therefore, fraud should be referred to as a crime and not a scam. Similarly, fraudsters should be referred to as fraud criminals instead of scammers.

Indeed even worse the inference for each word can be construed in a different manner; pause and reflect on the phrase; 'you've been scammed', one might argue that the emphasis here is on the victim for being a gullible party. Susceptibility in a fraud sense is borne out of trusting people, information and technology, surely this is the type of society that we want to inspire. Contrast the use of the word scammed with 'you've been the subject of fraud abuse' which is harder hitting and rightly moves the burden of the offence to the fraudster. When we use the language of fraud it is important to clarify the message we are sending to the receivers as this is more likely to impact their perception of this crime and how they would react to it.[10]

The impact of this confusion over the term scam has also resulted in implications for fraud victims. Surprisingly, some banks in the UK previously limited pay-outs to victims as a result of this confusion over the terms scam and fraud. According to an article in the Telegraph[11], banks could refuse to offer compensations when their customers fall victim to scams because they believe there is a difference between fraud and scams. Consumer groups warned that this confusion gives banks room to do little or nothing to help genuine victims. With the introduction of the voluntary Authorised Push Payment Scam Code which launched on 28 May 2019 most banks will pay customers for their loss. However, the Code is still widely referred to as the 'Scam Code'.

Nevertheless, we are not sure if the banks should be blamed for this confusion when we have helped in unnecessarily creating another term that dilutes the true meaning and harm caused by fraud. Therefore, we urge all fraud professionals, educators, regulators, and the media to pause and reflect before calling fraud, a scam. We all need to be consistent in our perceptions of and use of fraud terms to reduce fraud risk.

[8] *https://www.lincs.police.uk/reporting-advice/fraud-and-scams/*

[9] *Betts, M. and Kassem, R. 2019. Is the Language of Fraud Failing its Victims? The Public Sector Counter Fraud Journal, UK Government Counter Fraud Profession, Cabinet Office, Vol.105 (3), pp.6-7*

[10] *Betts, M. and Kassem, R. 2019. Is the Language of Fraud Failing its Victims? The Public Sector Counter Fraud Journal, UK Government Counter Fraud Profession, Cabinet Office, Vol.105 (3), pp.6-7*

[11] *https://www.telegraph.co.uk/personal-banking/savings/scam-fraud-banks-mince-words-limit-payouts-victims/*

Digital detectives in the NHS

Nikki Crook, Technical Lead at the NHSCFA's Forensic Computing Unit, describes the challenges of the job

When people ask me where I work, I am proud to say the NHS Counter Fraud Authority (NHSCFA). My answer seems to surprise most people, provoking the shocked response: "There's fraud in the NHS?!"

Unfortunately fraud is everywhere, including against our NHS, which most of us respect, treasure and protect. The next question is often, "Well who would want to defraud the NHS?" And the answer to that is a fairly long list of rotten apples in a variety of fields, though I stress that in each case they are a small minority.

People are perhaps most shocked to hear that fraud is perpetrated from within the NHS as well as by external parties preying on it – or sometimes a toxic partnership of outsiders and insiders.

All this is particularly hard to stomach when the hard work, professionalism, integrity and sacrifice of the great majority of people working for the NHS is on full display in the fight against COVID-19. But we must never switch off or turn down the dimmer switch in our vigilance against fraud. Because that would only harm the honest majority further.

Author:
Nikki Crook,
Technical Lead,
NHSCFA Forensic
Computing Unit

The NHSCFA is intelligence led and builds the most accurate picture it can of where the vulnerabilities might be in the system, how frauds occur, and how to prevent them. We engage at every level in the NHS in England to embed this knowledge and to promote best practice, working closely with our colleagues in Wales.

In addition, the NHSCFA itself investigates and prosecutes the largest and most complex NHS frauds, as well as assisting the network of Local Counter Fraud Specialists (LCFSs).

So where do I come in? I have worked at the NHSCFA for nearly six years and manage the Forensic Computing Unit within its National Investigations Service. We are a small team providing the digital forensic services throughout the course of an investigation: initial technical advice; capturing and preserving evidence; examining and analysing the evidence; ultimately producing and giving evidence at court. In our organisation, we are unique in also providing our services to other NHS departments, for example to our counterparts in Scotland and Wales.

Some assume the NHS is one organisation, one system, so I can just sit at my desk and access any digital data I require from anywhere within it. Wrong! My team often has to travel all over England, Wales and Scotland to capture and preserve evidence forensically, to the required standards. Typical missions:

- accompany the police and CFA investigators on a PACE warrant at a home or business address;
- visit the IT department at a hospital or NHS body to forensically retrieve data from their network or forensically image a user's laptop / computer; or
- visit business premises (for example a dentist or pharmacy) to take a forensic copy of any devices or practice databases.

The last example can be either by mutual agreement or with a Health Act production notice. The Health Act 2009 provides CFA investigators with a unique power under which they can obtain medical records and patient records.

Our investigations cannot have a detrimental effect on the service that the NHS provides to the public. In other settings, investigators with a warrant can physically carry off numerous devices for their forensic unit to add to the imaging queue, but this is not an option for us. We cannot put a pharmacy or dentist out of action by borrowing its IT equipment, nor take a hospital's server offline while we forensically image it, potentially causing a risk to patient life. Therefore, on our travels we frequently work through the night in order to cause minimum disruption to legitimate services. This often raises eyebrows, when we arrive to check in at hotels or B&B's in small towns at 4am, asking what time breakfast is served.

The challenges that apply to all forensic units apply to us, but can often be exacerbated by the vast landscape that the NHS covers. Other forensic practitioners might think we have it easy, that any NHS trust which issued an encrypted laptop, for example, must surely want to help us out by immediately offering a decryption/recovery key; and where they can they do. However, due to the numbers of staff employed by the department, the extensive and sprawling IT infrastructure and its administration our request is not as simple as one might think. But no hurdle has yet proven insurmountable.

In the last financial year my team has handled 272 items of evidence including computers, laptops, hard drives and mobile phones, equating to over 43TB of data. More businesses and individuals than ever before rely on technology in their day to day life, increasing the likelihood that key evidence found in our investigations is digital, be it communications, invoices, spreadsheets etc. This in turn provides a potential disclosure nightmare for the investigators.

In December 2011 the Forensic Science Regulator (FSR) issued version 1 of the "Codes of Practice and Conduct for forensic science providers and practitioners in the Criminal Justice System". This included a timetable by which the FSR expected all digital forensic units (police, government or private) across the country to achieve ISO 17025:2005 (general requirements for the competence of testing and calibration laboratories) accreditation. After a long and arduous journey, I am pleased to say our labs are accredited to the latest version, ISO 17025:2017 and we are accredited for both the imaging and analysis of computers and digital storage devices.

The work never stops, technology continues to change, and we have to continuously keep our skills up to date to deal with the latest challenge thrown our way. Upon joining, every member of my team undergoes training to become an Accredited Counter Fraud Specialist, as well as building on their own forensic expertise. I love the challenges and the variety of work that comes our way, meaning that no two days are the same. It provides great job satisfaction knowing I have played my part and applied my digital forensic skills and knowledge to help prevent and detect fraud and safeguard the NHS, which we need now more than ever.

How the UK justice system has adapted to the COVID-19 pandemic

The lockdown of the United Kingdom in response to the coronavirus (COVID-19) pandemic has had profound effects on every sector of society. In the legal sphere, the steps taken by the government and judiciary in response to the near total shutdown of the courts system has been dynamic and fast moving. Alternative audio and video technologies have been rapidly adopted by the courts to facilitate remote hearings and ensure the continued functioning of the courts system.

The legal framework within which these changes have taken place derive from judicial and governmental guidance, as well as the recently passed Coronavirus Act 2020, whose provisions set down powers for the remote operation of the courts system via audio and video technology.

The Royal Courts of Justice photographed by Trey Ratcliff is licensed under CC BY-NC-SA 2.0

The Coronavirus Act 2020 and remote court hearings

The Coronavirus Act 2020 ('the Act') received Royal Assent and became UK law on 25 March 2020. This emergency legislation marked the implementation of a legal framework within which the country is to operate during the pandemic. The scope of the Act is vast, covering almost every aspect of societal living, from port operations to pensions.

Sections 53 to 57 of the Act (and the associated Schedules 23 to 26) provide the powers for court and tribunal proceedings to take place remotely via video and audio technology. The Act temporarily consolidates and expands upon provisions in pre-existing legislation insofar as they relate to remote court hearings. The amendments extend the courts' existing, but far more limited, powers to enable the use of technology across a wider range of hearings and with a number of different participants.

Generally, hearings are to be broadcast to allow public access, however for civil proceedings there is a practice direction and judicial protocol that permits remote hearings to be conducted in private if broadcast is not practicable. Unauthorised recording of court proceedings remains a criminal offence.

A policy of case prioritisation has been adopted whereby urgent cases, for example, an application for an account freezing order or restraint order under the Proceeds of Crime Act 2002 ('POCA'), will be heard before less time-sensitive matters.

The Act, together with the individual guidance published by each court division in the preceding weeks regarding remote court working, directs that, so far as it is achievable through such technology, all listed hearings are to take place. There is one exception to this protocol: jury trials. The particular features of a jury trial which currently determine its incompatibility with remote hearings is considered in more detail below.

Access to justice during lockdown: how civil and criminal proceedings have been affected

This sudden and comprehensive move across to remote technology by most court users was by no means planned and, as a consequence, its benefits and flaws are being discovered 'on the job'. Pre-hearing tests are widely conducted to ensure that all participants have adequate audio or video facilities to engage fully in the proceedings. These additional measures, although certainly necessary, are time-consuming and costly. Equally, many hearings require the assistance of an interpreter, which adds another layer of complexity to the adversarial process of the UK courts' system.

About the authors:

Oliver Powell *is ranked in both Chambers & Partners (UK) and The Legal 500. He undertakes instructions that involve the regulation of business activity and commerce. His practice encompasses: asset forfeiture & civil recovery; business crime; commercial fraud; financial services; indirect tax and sanctions.*

Sophie O'Sullivan *practices in business crime and regulation. She undertakes instruction in matters relating to commercial fraud and financial crime, financial services, confiscation and asset recovery, corporate investigations, health and safety and professional regulation.*

Indicative of the challenges of remote court working is the fact that the number of listings in UK courts has been markedly lower than before lockdown. On 16 April 2020, the Law Society Gazette published figures stating that across all jurisdictions around 40% of hearings have continued, with the "overwhelming majority" of those completed having been shorter hearings without difficult or emotive evidence.[1]

Civil proceedings

Civil proceedings are, so far as is possible, to proceed in accordance with the technological alternatives having been encouraged and adopted widely. Indeed, the first judgment which addressed the effect of COVID-19 on a forthcoming trial fixture was reported on 6 April 2020. In Re One Blackfriars Ltd, Hyde v. Nygate [2020] EWHC 845(Ch) John Kimbell QC, sitting as a Deputy High Court Judge, refused to adjourn a 5-week trial relating to a claim for damages of £250m due to start in June, ruling that it should proceed remotely by video-link.

As such, there is nothing to preclude, for instance, a remote trial proceeding in the High Court in relation to an application for a Civil Recovery Order under Part 5 POCA. However, in recent guidance, the Lord Chief Justice identified certain types of civil proceedings which may be unsuitable for remote hearing, such as those involving child welfare decisions or vulnerable witness evidence.[2]

Criminal proceedings

Under the Act, the court is permitted to conduct all such hearings remotely if: (i) it is in the interests of justice to do so; and (ii) the parties have had the opportunity to make representations.

With regard to jury trials, by way of statement dated 23 March 2020 setting out the working principles of the court systems during lockdown, The Lord Chief Justice of England and Wales, Lord Burnett of Malden, was clear that unlike nearly all other criminal court proceedings which should adopt alternative technologies to continue working within the social distancing framework, jury trials would not be possible while the lockdown was in force.[3]

The distinction drawn by the Lord Chief Justice between jury trials and other criminal court proceedings has been reiterated by practitioners, who have emphasised the symbiotic relationship between the trial-by-jury process and the courtroom environment. On 16 April 2002, Caroline Goodwin, QC, Chairwoman of the Criminal Bar Association, stated that: "There is no substitution for both open and efficient justice by having a live trial in one physical space with jurors, barristers, a judge, witnesses and defendants all able to engage fully and solemnly with the full range of verbal, non-verbal and visual cues."[4]

[1] https://www.lawgazette.co.uk/news/top-judges-seek-to-mute-unruly-parties-in-remote-hearings/5103873.article

[2] https://www.judiciary.uk/wp-content/uploads/2020/04/Message-to-CJJ-and-DJJ-9-April-2020.pdf

[3] https://www.judiciary.uk/announcements/review-of-court-arrangements-due-to-covid-19-message-from-the-lord-chief-justice/

[4] https://www.thetimes.co.uk/article/split-despite-success-of-remote-trial-tp383b3sh

Setting aside the practical challenges of achieving a remote jury trial, there is a real concern that: remote trials may jeopardise the integrity and sanctum of jury deliberations; risk inadvertent degradation of the rights of defendants and complainants; and lead to protracted and costly appeals being pursued by those convicted.

Perhaps, in recognition of these myriad risks to the preservation of transparent justice, HM Courts and Tribunals Services have confirmed that whilst fully remote hearings in Magistrates' Courts will be introduced in due course, there are no similar plans for Crown Court hearings.

Finally, whilst there is no specific provision in the Act for proceedings arising from POCA, on the premise that they are civil proceedings, it is very likely that proceedings such as confiscation and enforcement hearings are captured under the sentencing provisions and will be conducted remotely (s 57A(3) of the Crime and Disorder Act 1998 (as amended by the Act)).

The CPS response

The current moratorium on jury trials has put extraordinary strain on the Crown Prosecution Service and other enforcement agencies, as the backlog of cases continues to grow without resolution by jury trial. As a consequence, on 14 April 2020, the CPS published guidance in which prosecutors are asked to prioritise more serious cases and "review both new and existing cases on their own merits, and consider every available course of action including community resolution". This guidance does not change the Code for Crown Prosecutors but, as the text provides, clarifies prosecutors' review responsibilities in the context of the COVID-19 pandemic.[5]

It should be noted, however, that given the harm caused and the seriousness of most fraud and economic crime which would fall to be tried by a jury, it is highly likely that the public interest test would still be met following a review of such cases.

Conclusion

Whilst the shift to remote hearings was a reactionary one, born out of a necessity to keep the UK courts system functioning during the lockdown; the efficacy and cost-saving potential of remote hearings may represent the legacy of COVID-19 on the legal system. Indeed, such enthusiasm to embrace technology, which has facilitated the remote assembly of all participants in court proceedings across all jurisdictions, is likely to change the manner in which hearings are conducted and justice is dispensed with for years to come.

[5] https://www.cps.gov.uk/legal-guidance/coronavirus-interim-cps-case-review-guidance-application-public-interest-covid-19

Lincoln Crown Court, inside the grounds of Lincoln Castle photographed by Barnyz is licensed under CC BY-NC-ND 2.0

Modern Slavery and COVID-19

Every national and global crisis we face brings with it a plethora of challenges and opportunities. As people face personal and professional hurdles in the light of an international pandemic and an uncertain future, the prospect of economic crime increases as unscrupulous individuals eagerly reap the benefits.

COVID-19 is bringing its own challenges, not least for the health workers on the front-line. Sitting from the comfort of our own home, adhering to social distancing measures, we could be lulled into a false sense of security, assuming that many of the risks we face on a day to day basis are no longer upon us. Unfortunately, that is not the case. With each pandemic, crisis or economic crash callous individuals will move in to strike while the iron is hot, making as much money as they can off the back of someone else's misfortune or strife. We have already heard of the many international scams in operation, offering much needed equipment or medicines to an unsuspecting public, or promising vaccines or immunity from the virus which are simply not available.

It is no different for the army of workers facing exploitation on a daily basis. Before the UK entered lockdown, we could see so many of these workers in our local car wash, nail bar or construction site – hidden in plain sight. Where are they now? With little money and often nowhere to go, exploited workers are moved to where the cash is. Herded like animals and treated no better, exploiters will seek out opportunities to make as much cash as possible. Holed up in unsanitary conditions, often in outhouses, dilapidated caravans or disused garages these very vulnerable workers have nowhere to turn.

In these trying times we have seen the demands for food and personal protective equipment such as gloves, masks and gowns increase significantly. With those increased demands comes the need for an agile and temporary workforce who can be moved swiftly to the farms, factories, food processing and packaging sites and distribution centres to keep up with the rising demand. With no way of getting out of the situation and nowhere to go, vulnerable workers become even more trapped.

To meet the challenges that present themselves effectively we must remain vigilant and stop the criminals from infiltrating our supply chains. Due diligence is needed now more than ever to ensure that we don't create an environment where we forget that our actions can have unintended consequences. The desperation to meet the PPE needs of our front-line workers or to keep up with the increased demands on food in supermarkets can often pressurise us to take actions that ordinarily we would think twice about doing. Economic crime is not faceless. It is real, and the consequences are several-fold. Modern slavery is an economic crime – it is all about the money but unlike other economic crime it has the exploitation of people at the very heart of it. Women, men and children forced to work, sell sex or drugs for the benefit of others. If we don't consider our decisions fully, we could inadvertently become complicit in the exploitation of others.

IF YOU NEED HELP, OR YOU THINK SOMEONE MAY BE A VICTIM OF SLAVERY OR EXPLOITATION, CALL THE CONFIDENTIAL UK MODERN SLAVERY HELPLINE 24 HOURS A DAY, 365 DAYS A YEAR.

CALL 08000 121 700

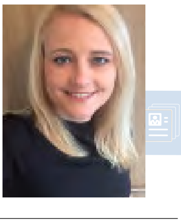
WORKING TOWARDS
A WORLD WITHOUT SLAVERY

Since the COVID-19 pandemic was realised, the Modern Slavery Helpline, operated by Unseen, has seen an increase in the percentage of calls from people themselves in exploitative situations or those in direct contact with a potential victim. Workers who we would ordinarily have seen on our high streets are now no longer in sight but that doesn't mean they are not in our midst. Arguably, their plight could have increased with the lack of public visibility. No longer washing cars, working in restaurants, or cleaning offices their only opportunity is to move to where there is the greatest need – the food chain or other 'deemed essential' supplies.

As with modern slavery, economic crime knows no boundaries and the ease with which money, supplies and people, in normal circumstances, can be moved creates and facilitates a breeding ground for both. Whilst our focus and attention is quite rightly on the crisis in hand, let's not forget the risks that are ever present not only in global supply chains but those in the UK.

If you suspect someone may be a victim of modern slavery, call the UK-wide Modern Slavery Helpline on 08000 121700.

Author:
Justine Currell,
Director, Unseen UK



Shop sign photographed by Duncan C is licensed under CC BY-NC 2.0

COVID-19: The risk of fraud in a crisis

Author:
Alex Jay,
Partner, Gowling WLG

Many, if not all, businesses are feeling the economic repercussions of COVID-19 as they struggle to remain financially liquid. This means that often businesses are seeking new trade and business opportunities, and offers of such are therefore hard to turn down.

With rising fear that the economic fallout due to COVID-19 will be likened to the Great Depression, businesses are accepting new opportunities with haste. This can, however, leave businesses at serious risk of fraud

Lessons from history

In the 2008/2009 financial crisis, fraud increased significantly. It was reported by KPMG that the UK courts saw cases of more than £1.1billion worth of fraud in this period, which at the time was the second highest amount in the survey's history.

Moreover, during 2009 the overall level of fraud increased by 9 per cent according to Cifas (a major UK anti-fraud body). The rise in fraud in 2009 was attributed to three main factors: identity fraud, false insurance claims and a rise in misuse of funds made available to try to help the financial crisis. The UK Financial Services Authority warned that more than 12 million people may have been targeted by salesmen selling shares in worthless, non-existent or near bankrupt companies.

It appears that history is repeating itself. In the US, the National Fraud Intelligence Bureau reported that 105 cases of fraud recorded in February - March 2020 have caused losses totalling almost £1 million. Many of the cases related to coronavirus-themed phishing emails, which include:

claiming to be from a research group mimicking the World Health Organisation, offering fake insurance schemes and trading advice, and pretending to be from the government, offering tax refunds.

In more recent news, on 14 April 2020 Interpol released a statement saying that they had intercepted a multinational face mask supply fraud worth £1.3 million. The scheme involved the use of compromised emails, advance payment fraud and money laundering.

While some of the issues raised above are relatively minor in financial terms, the true levels of fraud, and the biggest cases, are often only revealed years after the crisis.

Case examples of fraud arising from crises

There are many examples of crises historically generating significant frauds:

With rising fear that the economic fallout due to COVID-19 will be likened to the Great Depression, businesses are accepting new opportunities with haste. This can, however, leave businesses at serious risk of fraud

2001: UK Foot and Mouth Crisis

The foot and mouth crisis of 2001 generated a significant logistical exercise for UK agriculture. However, it was also reported that a number of frauds arose in that time.

Indeed, the National Audit Office published a report in 2002, which noted that the first four months of the crisis placed a huge strain on the government's financial control systems, as they tried to respond to control the disease. This led to a process of subsequent correction of overpayments and irregularities, and resulted in a number of disputes.

2004: Indian Ocean Tsunami

In 2004, the Indian Ocean Tsunami resulted in international aid of more than $6.25 billion being advanced to assist those affected. It was, however, reported that those funds were the targets of significant fraud. The Sunday Times wrote an article in relation to fraudsters targeting UK charities.[1]

Indeed, our firm was involved in one case of suspected misuse of international aid funds worth over €50 million, resulting in a major investigation many years after the crisis.

2005: Hurricane Katrina

In August 2005, Hurricane Katrina hit Louisiana, it was the most destructive natural disaster in U.S. history.

Nonetheless, fraudsters began to take advantage of the situation within hours of the hurricane landing. The FBI estimated that within a week, there were approximately 2,300 fraudulent Hurricane Katrina-related internet sites.

More significantly, more than $110 billion was set aside by the US for reconstruction. The relief money was handed out at a rate of more than $500 million per day, and the speed in which contracts were handed out was unprecedented. It was reported that bills arrived for deals that were sealed with a handshake, with no formal documentation to back them up, and 80% of the $1.5 billion in contracts were awarded without bidding. It was suspected that substantial sums were lost to fraud in this way.

2010: BP Oil Spill

Following the 2010 Gulf oil spill, a couple engineered a complex scheme to move funds from businesses they owned so it would appear as if they had made a financial loss due to the oil spill.

They subsequently received $2.1 million in compensation for revenue loss, which they were later ordered to return.

2017: Grenfell Fire

The Grenfell tower block fire was one of the worst disasters to affect the UK in recent memory. It did not prevent fraudsters trying to capitalise though.

In March 2020, two individuals were convicted of fraud. They claimed (wrongly) to be living in the flat of a deceased Grenfell Tower resident at the time of the fire, and defrauded the local council out of £47,802 in doing so. They were not alone. It was reported that around £1 million was lost to fraudsters seeking to benefit from aid intended for victims of the fire.

Comment

In times of economic hardship fraud comes to the fore. The same is true in times of natural disaster. The present COVID-19 crisis looks set to bring elements of both: it is a global pandemic, which will most likely leave a legacy of global recession in addition to the health issues it has created.

This is likely to create a perfect storm for fraudsters. The state authorities, anti-fraud bodies, legal and accountancy professions as well as companies and the wider public will all need to be vigilant to limit the damage that could be caused through fraud in these times.

[1] https://www.thetimes.co.uk/article/massive-fraud-hits-tsunami-aid-95jdb375dkt

Hunting the elusive Black Swans

Author:
Chris Freeman
Government Counter Fraud Profession

In 2019 the Government Counter Fraud Profession launched the first Fraud Risk Assessment Standards and a pilot training programme. This has allowed the Profession to transform capability in the Fraud Risk Assessment discipline, which has been an invaluable tool in the Counter Fraud Function's response to the COVID-19 pandemic.

In the standards "[a] risk is defined as the possibility of an adverse event occurring or a beneficial opportunity being missed. If realised it may have an effect on the achievement of objectives and can be measured in terms of likelihood and impact. Fraud Risk Assessment covers how to effectively identify, describe and assess individual fraud risks and develop these into a comprehensive fraud risk assessment for the entire organisation. It covers how to identify and evaluate mitigating controls, including understanding their limitations."[1]

In this article the focus is on those risks that are not identified at all. They are the 'unknown unknowns' (UU). Had they been identified, they would, when placed into a fraud risk assessment matrix, be found in the corner showing risks assessed as being of low likelihood with a high potential impact. How can fraud risk assessors ensure such risks are identified so that they can be properly understood and therefore managed effectively?

Black Swans

The 'Black Swan' is an often misconstrued concept proposed by Nassim Nicholas Taleb in his book "The Black Swan: The Impact of the Highly Improbable". The metaphor behind the titular swan is that it was thought (by those in Europe) that all swans were white, because nobody had ever seen a black one. It was perhaps an antiquated equivalent of '... and pigs might fly'. Of course, observing a single black swan would be enough to disprove this rule.

Indeed, there were black swans in Australia, it was just that no European had yet seen one and so the mere possibility was dismissed. Dutch explorers reached Australia in the late 17th century and saw black swans for themselves. The black swan metaphor became redundant.

Taleb's Black Swan is an event which has three attributes: "First, it is an outlier, as it lies outside the realm of regular expectations, because nothing in the past can convincingly point to its possibility. Second, it carries an extreme 'impact'. Third, in spite of its outlier status, human nature makes us

[1] *Government Counter Fraud Profession Fraud Risk Assessment Standards*

Black swans at Lake Wendouree, Victoria, Aus. photographed by Ed Dunens is licensed under CC BY-NC-ND 2.0

concoct explanations for its occurrence after the fact, making it explainable and predictable."[2]

Mediocristan and Extremistan

Taleb uses the theoretical realms of Mediocristan and Extremistan to describe the impact of different types of risks.

In Mediocristan the law of large numbers holds true. For example, by selecting 1,000 convicted fraud criminals at random and measuring the height of each allows the mean average height of the sample to be calculated. Half of the sample will be shorter than the mean average and half taller. If the world's tallest or shortest person happens to be included in the sample their presence will barely affect the average because of the other 999 people in the group being either side of the average.

Taleb's Black Swan is an event which has three attributes: "First, it is an outlier, as it lies outside the realm of regular expectations, because nothing in the past can convincingly point to its possibility. Second, it carries an extreme 'impact'. Third, in spite of its outlier status, human nature makes us concoct explanations for its occurrence after the fact, making it explainable and predictable."

In Extremistan, however, things are much more volatile. Using the same sample the measurement of the value of the fraud that each perpetrated can again be used to generate an average, with half obtaining less than average and half more. If, however, the sample happens to include Bernie Madoff (who perpetrated a $65 billion fraud[3]) the average would be significantly skewed. Of the sample 999 people would probably have obtained less than the mean average of the sample and one person (Madoff) would have obtained more.

The crimes of Madoff and Allen Stanford ($7 billion) were linked to Ponzi schemes involving many investors, hence the scale of the losses. However any organisation can be the victim of fraud. Dixon, Illinois, USA has a population of around 16,000. The City of Dixon (the local authority with an annual budget of around $45 million[4]) was the subject of fraud in the same way as any other comparable city authority; some larger frauds, some smaller, which could be expected to group around a fairly modest average value. Rita Crundwell served as comptroller[5] for the City. Over the course of 20 years she stole $53.7 million from the City, including $5.8 million in 2008 alone.[6] Compared to all other fraud cases experienced by the city during that time, Crundell's crimes are clearly exceptional, but evidently not impossible. Fraud belongs in Extremistan.

Unknown Unknowns

For an event to be a Black Swan it must lie "...outside the realm of regular expectations, because nothing in the

[2] *The Black Swan: The Impact of the Highly Improbable, Nassim Nicholas Taleb, 2007*

[3] *https://www.reuters.com/article/us-madoff/madoff-pleads-guilty-is-jailed-for-65-billion-fraud-idUSTRE52A5JK2009031*

[4] *https://www.ci.dixon.ca.us/DocumentCenter/View/12114/FY-19-20-Adopted-Budget?bidId=*

[5] *Someone who is in charge of the accounts of a business or a government department*

[6] *https://www.justice.gov/usao-ndil/pr/former-dixon-comptroller-rita-crundwell-sentenced-nearly-20-years-federal-prison-537*

past can convincingly point to its possibility". Taleb uses the example of a turkey being raised for the table for Thanksgiving dinner to illustrate this point: From when it hatches the turkey is provided with food, water and shelter by the farmer. From the turkey's point of view it seems farmers must really like looking after turkeys. The farmer's perspective is, of course, rather different. Just before Thanksgiving, however, the turkey is in for a shock.

If, when identifying potential risks, consideration is only given to recurrences of previous events those UU will be neglected. Flood defences, could be designed to be sufficient to contain the river when it reaches its highest recorded levels, based on the scale of floods previously experienced on that river. But what if the next flood brings twice the level of water of any previous storm ever experienced? Those same defences will not be sufficient as the scale and nature of what has been observed previously does not limit the extent of what will happen in future.

In the process of identifying fraud risks it is therefore necessary to resist confining thoughts to recurrences of previous types of fraud encountered, in the same way as just by concentrating solely on historical river levels would make for inadequate flood defences. We can learn lessons from the cases of Madoff, Stanford and Crundell (and any other detected fraud case) because they were caught. However, absence of evidence is not evidence of absence. Despite all efforts some frauds will be successful and go undetected. Fraud continues to evolve and failing to consider the potential of new modus operandi leaves a significant gap in knowledge. They are UU.

The Johari window[7] (below) helps explain this further. In the assessment of fraud risk those risks known to both the assessor and those in the organisation are easily identified (corner A). The fraud risk assessor's own training and expertise, access to good practice and networking with other counter fraud professionals will address corner C. Effective workshops, interviews etc. will help identify those risks known by those in the organisation but not by the assessor and this will help address B. Corner D is where those 'UU' are found. This is also the domain of the Black Swans.

	Known to self	Not known to self
Known to others	A	B
Not known to others	C	D

The fraud risk assessor can reduce the number of Black Swans that lurk, turning as many UU as possible into identified and assessed fraud risks. Workshops and interviews with people from across an organisation, combined with the skill of a fraud risk assessor, will help tease these out. Those that work with systems and processes can provide insight and, collaboratively and creatively, identify risks that were previously not thought of. Lateral thinking and imagination are both very useful in these exercises. Encouraging participants to 'think like a criminal' to generate ideas will definitely help.

Hindsight

It is unsettling when our predictions turn out to be wrong, or something happens that we did not expect. The human mind has a variety of cognitive biases which seek to help us overcome this feeling. Recollection of our previous thoughts on the matter are bent and adapted after the fact. This is a subconscious process, but we can at least be aware of its existence in ourselves and others. We are surrounded by randomness in all aspects of life and it is not possible to anticipate the ultimate consequences of every event we encounter. It is, however, cognitively more comfortable to adapt our recollection to a simple chain - event C was caused by events A and B, rather than acknowledging that the picture was far more complex than that and that chance played a large role.

From an organisational perspective a fraud which successfully eludes all controls is likely to trigger questions of why opportunities to prevent it were missed. But, again, care needs to be taken not to underestimate the complexity of the events and circumstances that led to the success of the fraud. Most important is that any points of failure are looked at again and the lessons learned are used to inform future fraud risk assessment activity.

Conclusion

Black Swans, as described by Taleb, are rare but remain a possibility. Risks identified in a fraud risk assessment cannot be Black Swans, because in being identified they are no longer UU. They may be assessed as having a high potential impact but a low probability, but this allows for the risks to be appropriately managed in line with the organisation's risk appetite.

It is impossible to anticipate every fraud risk an organisation will face; there will always be UU and some of them may even turn out to be Black Swans. Skilled fraud risk assessors are invaluable assets to an organisation; this is why the Government Counter Fraud Profession has started to transform capability in this discipline. By thinking creatively, being aware of the wider world of fraud and working collaboratively with others, fraud risk assessors can root out those elusive UU.

[7] *Developed by psychologists Joseph Luft and Harrington Ingham in 1955*

Get Involved

We would really like to hear your views on the Public Sector Fraud Journal. What would you like to see in future issues? Would you like to contribute an article?

Please email us at: pscfjournal@cabinetoffice.gov.uk

Government
Counter Fraud
Profession

Crown Copyright Notice

All of the material here is owned by the Counter Fraud Profession for HM Government. It is all subject to Crown Copyright 2020.

This material should not be disseminated in anyway that may prejudice harm or infringe on the purpose and aims of the Counter Fraud Profession for HM Government.

Contact us:

Email: gcfp@cabinetoffice.gov.uk
Web: https://www.gov.uk/government/groups/counter-fraud-standards-and-profession