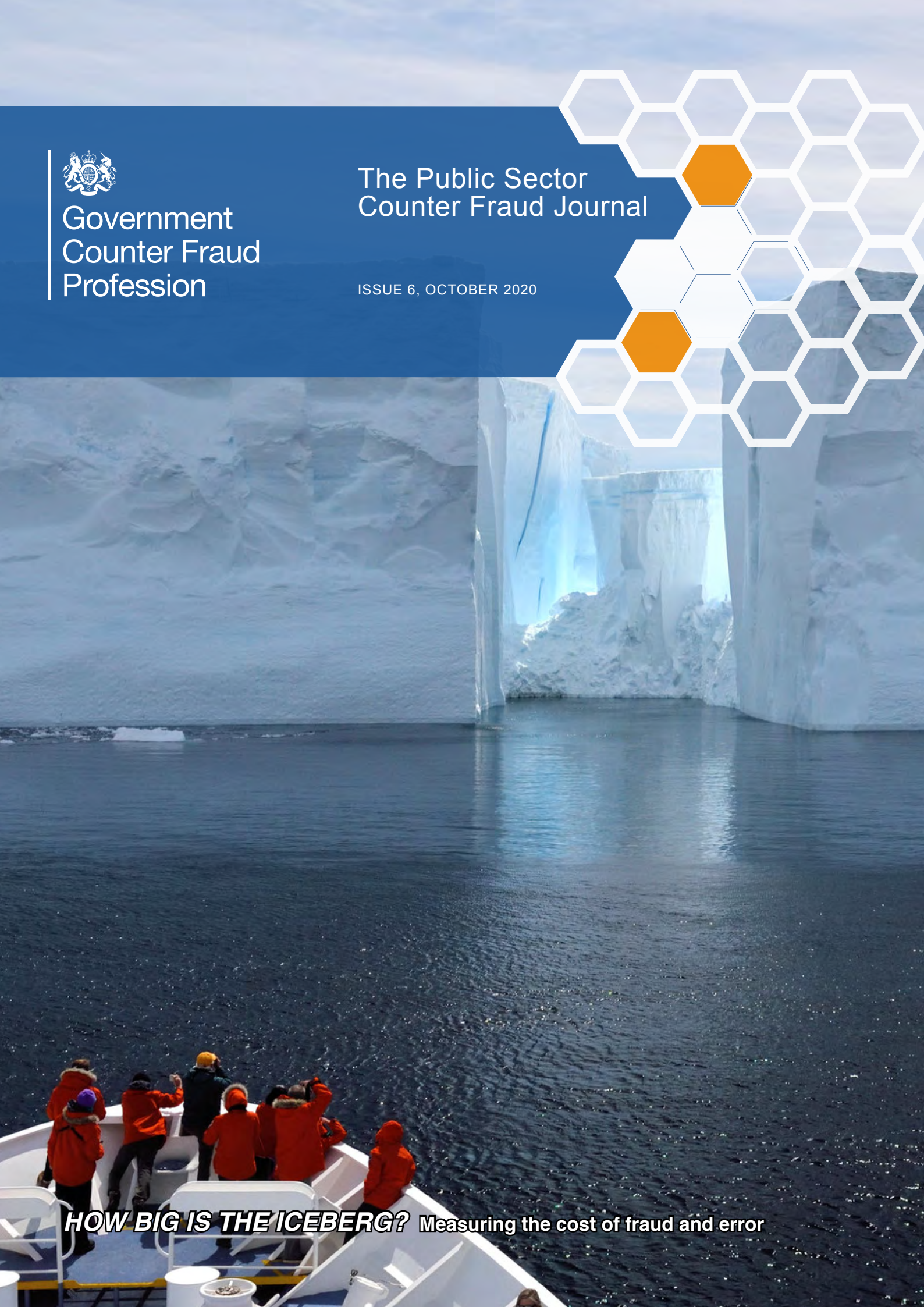
Government Counter Fraud Profession

The Public Sector Counter Fraud Journal

ISSUE 6, OCTOBER 2020



HOW BIG IS THE ICEBERG? **Measuring the cost of fraud and error**

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

CONTENTS

Editor's letter

I would like to start with a thank you on behalf of the Editorial Board to everyone reading this, the 6th issue of the Public Sector Counter Fraud Journal. Your interest and support has seen the Journal go from strength to strength, since it was launched in 2019. We have seen readership grow from a few hundred for the first issue to over 9,000 downloads of Issue 5 when it was released in June 2020, reaching an international audience from the US to Germany, India to Belgium. For me, this is testament to the aspirations of the Journal from its inception - to reach a network of fraud specialists representing many different skill sets, sharing good practice and innovation, as well as challenging and enriching all our thinking.

Fraud is an economic pandemic, bringing misery and deprivation to its victims, whilst its perpetrators find ever more devious ways to amass wealth at the expense of others. We can, however, stem the tide; the collective professionalism of everyone working in counter fraud can make a difference.

At time of writing, COVID-19 remains a serious issue - both to our health and to our economy. In this issue you can read about some successes in the fight against those who try to exploit the pandemic through fraud, with David Clarke writing with passion about the work of the Fraud Advisory Panel to improve cross-sector intelligence sharing.

Kevin Newe explains HMRC's Illicit Finance Strategy, designed to understand, disrupt and confiscate criminal finances. When I worked in financial investigations I was told that the Proceeds of Crime Act 2002 was one of the pieces of legislation most hated by criminals; they were no longer able to simply finish their jail term to then return to their mansions and flash cars. More power to our Financial Investigators and Forensic Accountants!

Those working for the Department for Work and Pensions (DWP) have been at the forefront of supporting many in financial distress resulting from COVID-19. Andy Macdonald's piece examines how DWP's Serious and Organised Crime teams adopted a 'rapid response', using the risk and intelligence tools available to them, to tackle the inevitable rise in fraud attacks on the benefit system, helping ensure money only goes to those most in need.

If you want an intellectual work out, Rob McGregor's article on telecoms fraud expounds on the technical challenges of prevention in the internet age, and the eye watering sums involved. The once-simple phone scammers have moved on apace.

We often refer to the 'fight against fraud'. It is a battleground, and knowing how to combat the enemy through cunning and strategy is as important, if not more important than physical interventions. Tim Barlow from the NHS Counter Fraud Authority (NHSCFA) shares his thoughts on the importance of proper fraud risk assessment. There's also an instructive piece on the government's Fraud Measurement and Assurance Programme, looking in depth at how fraud can be reliably measured.

There will be time soon to reflect on what we have learned during this strangest of times - what we can do better, what we need to do more of, and importantly, what is no longer effective in the 'new normal'. What we know already is that working in relationships built on trust, and, crucially, sharing intelligence legally and simply to thwart the fraudster before they strike must be our new normal. One of my favourite leadership reads is The Art of War for Executives by Donald G. Krause. Using the teachings of Chinese warrior Sun Tzu, Krause illustrates how modern leaders can use various principles of war to effect success. One of those principles is 'simplicity': "The supreme art of war is to subdue the enemy without fighting".

Jackie Raja
Government Counter Fraud Profession Development Lead, Department for Work and Pensions

Following the money

How HMRC is increasing its impact by focusing on illicit financial flows

Author:
Kevin Newe,
Illicit Finance Strategy lead, HMRC

Those who commit Fraud tend to be motivated by one thing: profit. These ill-gotten gains, sometimes described as the proceeds of crime, can be defined by a rich and diverse language that can mean different things to different people. Is it about money laundering, or asset recovery, or criminal investigation and conviction? For HMRC, it is all these things and much more. And to help establish consistent understanding, it defines all this work as Illicit Finances (IF).

Why Illicit Finances? Well, it helps remove that association with criminal gangs and criminal investigation. What HMRC really want to identify and disrupt, are all the financial elements of the tax frauds their Fraud Investigation Service (FIS) have a mandate to tackle, which includes abuses of businesses HMRC supervises under the Money Laundering Regulations. These businesses can often inadvertently help launder the proceeds of many different crime types, including drug trafficking or modern slavery, so HMRC's role goes beyond just tax and customs administration.

The tone is set from the very top, with FIS Director Simon York recognising that illicit financial flows can seriously undermine the UK's economic prosperity and reputation. If people feel the system is being exploited and there is inequality in HMRC's response, it can shake their sense of faith and fairness, which increases the risk of them becoming non-compliant. By putting illicit finances at the heart of the HMRC response, the combination of the department's unparalleled intelligence capability, and the breadth of its investigation toolkit can deliver a whole system response, ensuring no criminal is beyond HMRC's reach.

To embed that approach, HMRC has developed an Illicit Finance Strategy prioritising three key areas:

Threat Understanding: In simple terms, a better understanding of illicit finance risks leads to a better response, whether that's operational or policy-led, in closing loopholes. IF risks are not static and the methods used today won't necessarily be the same methods used tomorrow. So, it is about being constantly vigilant, analysing and assessing how the IF landscape is changing.

Anti-Money Laundering Supervision: HMRC is one the UK's 25 anti-money laundering supervisors, tasked with ensuring businesses considered at risk of money laundering or terrorist financing are aware of their obligations and have in place systems and processes to monitor and flag risk. It is about helping the compliant majority meet their regulatory obligations, while delivering suitably robust interventions against those who choose to be non-compliant, or worse, are criminally complicit. This can include the imposition of substantial financial penalties, the revocation of an individual's authority to trade, or the ultimate sanction of criminal prosecution and a custodial sentence.

Illicit Finance disruption: With additional insight from their approach to threat understanding, HMRC embeds consideration of IF vulnerabilities and opportunities in all their significant investigations, whether civil or criminal. The department has access to the most powerful asset recovery

tools in UK legislation, including confiscation post-conviction, a broad range of civil recovery powers (i.e. not requiring a criminal conviction) and an award-winning approach to lifetime offender management.

All this activity is about delivering measurable impacts on tax frauds, while reducing the opportunities to abuse HMRC's supervised businesses. And that is best evidenced by HMRC's Proceeds of Crime Intervention Team (PoCIT), which was set up in 2015 to tackle sophisticated money laundering networks that use and abuse the tax system and HMRC's supervised businesses to clean their dirty money.

PoCIT works closely with domestic and international partners such as the National Crime Agency and foreign tax and customs administrations, brokering cooperation through HMRC's network of Fiscal Crime Liaison Officers.

PoCIT exemplifies HMRC's approach to using all its powers to disrupt these pernicious money laundering networks. Not only do they seize millions of pounds of suspicious cash amounts, from tens of thousands to millions per seizure, but they also arrest individuals for money laundering offences, working with the UK's prosecuting authorities to secure successful convictions, leading to years of custodial sentences.

But the disruption doesn't stop there. They will work with HMRC's Anti-Money Laundering Supervision teams to shut down businesses suspected of laundering these cash amounts, taking these complicit individuals out of the system.

HMRC teams also have access to powerful asset recovery tools, including Account Freezing Orders and Account Forfeiture Orders (AFOs), introduced via the Criminal Finances Act in February 2018. These powers allow HMRC officers to freeze and recover monies without needing to commence a criminal investigation. HMRC has significantly grown its use of AFOs and continues to work with banks to identify, freeze and recover the proceeds of tax frauds that move through the UK's financial system.

HMRC's blended approach to tackling illicit financial flows has resulted in the recovery of nearly £360 million in the last two years alone, with HMRC taking on increasingly complex investigations in the face of ever more sophisticated money laundering mechanisms used by tax fraudsters.

All of this highlights the vital role HMRC plays as part of the UK's overall response to fraud and economic crime, complementing the work of others across government and the private sector.

Proceeds of Crime Act 2002

The Proceeds of Crime Act is a powerful piece of legislation designed not only to strip criminals of their ill-gotten gains following conviction but also to disrupt criminals, frustrating their criminal enterprises. In addition, it confers the ability to bring civil proceedings without the necessity for a conviction in some cases.

There are three money laundering offences covered under the Proceeds of Crime Act:

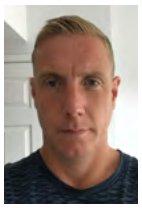
Section 327 covers concealing criminal property; this includes disguising, converting, transferring and removing criminal property from England and Wales or Scotland or from Northern Ireland.

Section 328 details how a person commits an offence if they enter into an arrangement to control or retain criminal property with prior knowledge or suspicion of that criminality.

Section 329 covers acquisition, use and possession. A person commits an offence if he acquires criminal property, uses criminal property and or has possession of criminal property.

Big results from a small team

Author:
Mark Crowther,
Proceeds of Crime Intervention Team, HMRC



HMRC's Proceeds of Crime Intervention Team (PoCIT) was set up in April 2015 with a focus on gaining a greater understanding of the modus operandi of criminal groups, by targeting the cash couriers and businesses used for money laundering.

Since then, the 10-officer team has made hundreds of seizures and arrests for money laundering offences, freezing bank accounts and closing businesses involved in laundering the proceeds of crime.

Utilising powers under the Proceeds of Crime Act among others, the team are ready to deploy any time, day or night, across the country, and use a range of covert surveillance techniques to target their quarry.

Those skills were needed in December 2017 when the team received a tip-off from a major bank that an individual had been observed in several branches in Lancashire depositing large sums of money.

The bank completed a Suspicious Activity Report and the team sprang into action, mounting a surveillance operation on the suspect's home. He was followed as he visited several other branches and was eventually stopped under Section 289 of the Proceeds of Crime Act, where a search of his car revealed £100,000 hidden inside. He was arrested on suspicion of money laundering.

A further search of his home revealed £840,000 hidden beneath floorboards and a number of large holdalls containing vacuum-sealed bags of amphetamine. Bank slips and notepads revealed he had laundered £10.8m over the previous four months. The cash was seized and forfeited while the drugs, with a street value of £8.4 million, were destroyed.

Following a joint prosecution undertaken by HMRC and Lancashire Police, the individual was jailed for ten-and-a-half years and his house and car were confiscated.

PoCIT is also a valued partner of other law enforcement agencies, often working cases and suspects together. These can be lengthy and involved, as clearly shown by their work with the National Crime Agency to dismantle a money laundering network operating out of Lancashire and Yorkshire.

The investigation unfolded after the team discovered that a number of bank accounts in the region were being used to routinely and exclusively move large sums of money to Asia and the Middle East. Establishing a pattern of suspected money laundering, officers turned their attention to identifying the couriers responsible for moving the cash.

Over the next 12 months, they used covert surveillance techniques to monitor the movements of the couriers' vehicles. These were analysed and so-called "dirty runs" were identified where the couriers were moving the money.

Linking up with local police forces, the couriers were stopped and found to be carrying not only money, but also drugs and other commodities funding the proceeds of crime. It's these sorts of operations that demonstrate how the team are having a real impact on organised criminals across the UK. The team can be contacted on 03000588223 or via mark.crowther@hmrc.gov.uk for referrals or questions.

Suspicious Activity Reports

Suspicious Activity Reports (SARs) are made by financial institutions and other professionals such as solicitors, accountants and estate agents.

They are a vital source of intelligence, not only on economic crime, but on a wide range of criminal activity. They provide information and intelligence from the private sector that would otherwise not be visible to law enforcement.

SARs can also be submitted by private individuals or businesses where they have a suspicion of Money Laundering. The reports are completed online and are collated by the National Crime Agency.

Measuring the iceberg: the Fraud Measurement and Assurance Programme

Foreword by John Smart, Independent Chair of the Fraud Measurement and Assurance Oversight Board

The Fraud Measurement and Assurance (FMA) programme has been running since 2014 and has now overseen sixty fraud measurement exercises undertaken across fifteen different government departments. This is an ideal opportunity to take stock, celebrate what the programme has achieved and also to reflect on lessons learned; so this article by Steve, Sara and Grace is timely. I believe we have achieved our primary aims and the output from the programme is driving better recognition of fraud exposures across government.

The aim of the FMA programme is to save public money from being lost to fraud and error, by helping government departments understand their fraud risk exposure, and to use measurement to estimate actual levels of fraud and error losses.

Author:
John Smart,
Independent Chair of the Fraud Measurement and Assurance Oversight Board

To support and achieve this aim the programme seeks to make fraud measurement sustainable and widely-practised across government, to agreed standards as part of the Counter Fraud Function, supported by the Government Counter-Fraud Profession (GCFP). It has a desire to see fraud measurement programmes recognised as a key component of the assurance landscape within each Government department.

The FMA programme works on the premise of testing residual fraud risks. Residual fraud risks provide a window of opportunity for fraud to happen as they represent the risk that remains despite any controls in place. Therefore, testing seeks to identify whether these gaps in controls have led to fraud occurring, and, if so, by how much. It is perhaps the mirror opposite of internal audit, whose focus is primarily to test the operational effectiveness of controls.

Government is currently facing significant fraud risks arising from COVID-19 stimulus and support schemes and Ministers have asked departments to undertake post-event assurance activity including fraud measurement. The Counter Fraud Function across departments is better placed to do this because of experience gained through the FMA programme and associated guidance that has come from the centre.

Background and history of the programme

Authors:
Steve Selley, Sara Dobson and Grace Brown, *Centre of Expertise for Counter Fraud, Cabinet Office*

The government's Fraud Measurement and Assurance Programme can trace its origins to 2014, when the Cabinet Office Minister took a paper to the Ministerial Committee on Public Expenditure: Sub-Committee on Efficiency and Reform (PEX(ER)) to discuss how to further develop counter-fraud and error reduction capability in government.

The paper recognised that, outside of the Department for Work and Pensions (DWP) and Her Majesty's Revenue and Customs (HMRC), government departments and their Arms Length Bodies reported losses due to fraud and error of only £220 million from a spend of £227 billion (0.1%). However, available comparators, such as the United States, where the measurement of fraud and error (improper payments) is mandated, indicated levels of 3.53% might be expected and comparators from the private sector had an average of 5.47%.

The conclusion, therefore, was that it was likely that reported fraud levels across UK government departments represented the 'tip of the iceberg' and were significantly below actual levels, with serious frauds potentially going undetected. To provide evidence as to whether this hypothesis was correct, the PEX(ER) Committee was asked to agree to the following recommendation:

"By December 2014, all departments should undertake two small, targeted random sampling exercises to identify and measure fraud and error losses in their highest risk payment areas."

In that first year, 14 departments participated delivering a total of 28 exercises. These varied in quality as departments often lacked the capacity and skills to undertake this type of exercise. However, the better quality exercises, which focussed on testing residual risks to find fraud did find fraud and error, with levels of irregularity reported between 0.6% - 11.7%; well in excess of the overall level of 0.1% being reported at the time.

Therefore, it was agreed that departments should be encouraged to participate in an annual programme to detect instances of fraud and use the results to estimate and measure what actual losses might be across a wider population. Thus the Fraud Measurement and Assurance programme was born, although it was known in those early years as the Random Sampling Programme.

An independent governance structure was created to oversee the programme consisting of an Oversight Board made up of fraud measurement leaders drawn from across the public and private sector; and an Experts Panel (again drawn from the public and private sectors), whose role was to review and quality assure future exercises.

What the FMA programme has achieved

The results of the FMA programme have allowed conclusions to be drawn about how much fraud and error loss there might be in the areas of spend where government departments do not actively look for fraud and error. The hypothesis of the existence of unknown, undetected and unreported fraud had been represented by the 'iceberg

model'. This model illustrated the difference between the known loss (detected or estimated levels of fraud) and the loss we do not know about - the unknown fraud.

The FMA programme has provided an evidence base to validate the existence and likely extent of the 'unknown' element of the Iceberg model. In December 2017, following four years of fraud measurement exercises, the FMA Programme Oversight Board concluded that the programme had achieved its first objective, that is, to test the hypothesis that the public sector is detecting considerably less fraud than it suffers. Based on the evidence of exercises completed to date, the Oversight Board concluded that if you test the residual fraud risks in a high risk area where no fraud detection activity has previously taken place, fraud or error will be detected. In November 2018, the Oversight Board further concluded that when a good quality exercise was undertaken, it was likely to find a rate of fraud and error between 0.5% and 5%. This decision was based on the results of high quality exercises and considered available comparators from the private sector, academia, and the US. This range of 0.5% - 5% is now used to calculate the estimated level of fraud and error loss within the "unknown" section of the iceberg model (above) and is accepted as a standard in wider contexts, such as being referenced in a recent report[1] focused on the UK Government's response to fraud during the Covid-19 pandemic.

From the 60 measurement exercises that have been carried out between 2014 and 2020, a range of areas of spend across government have been covered, and where exercises focussed on finding fraud they have identified significant amounts of fraud and error loss.

Besides enabling measurement of fraud, two thirds of exercises reported that control improvements had been implemented as a direct result of the FMA work. In addition to this, FMA allowed in-depth investigation of specific cases, as well as recovery of public funds where losses had been identified.

Lessons learned - what methods have worked well

There are certain characteristics that were common to the good quality exercises successful in finding fraud and error.

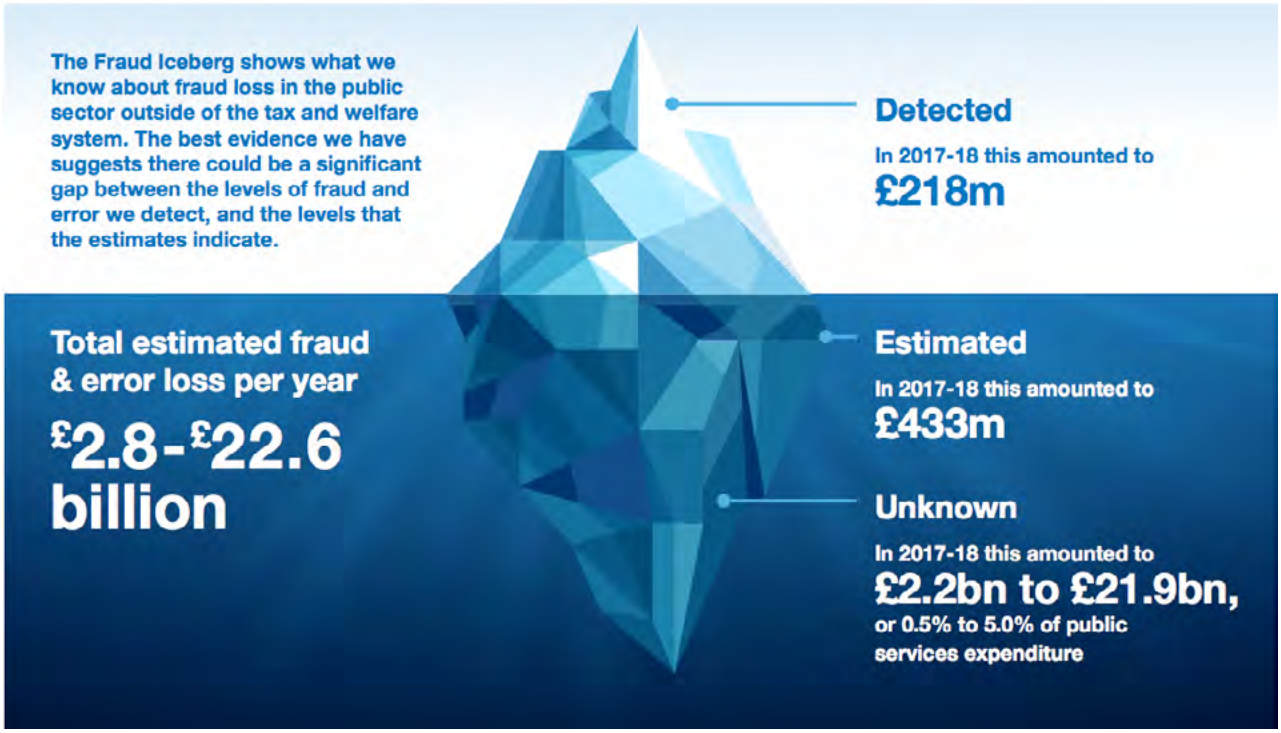
A detailed Fraud Risk Assessment (FRA) is vital

A detailed FRA identifies fraud risks, relevant controls and any limitations of those controls, and importantly describes residual risks - which are the gaps that allow fraud to happen despite any controls in place. These residual risks are then the focus of testing. Each of these sections - the fraud risks, the controls and their limitations - impact on the residual risk identification, and so if any of these sections are not accurate, the residual risk won't be either, which will likely lead to testing in the wrong direction.

Using new information to look for fraud and error

It is important to think carefully about what information can be used to look for fraud and error. This could be, for example, using data from another government department or a credit reference agency to confirm an applicant's age, or using Companies House information to identify a company. Using information already held within the scheme or process will often result in very little fraud or error being found, as

1 https://policyexchange.org.uk/wp-content/uploads/Daylight-Robbery.pdf



it's likely to have been used in the decision making process. The best type of information is usually from an independent source, like another organisation, or information that is found by online research, or site visits.

This work is different from audit activity

FMA activity specifically looks for fraud and relies on a fraud risk assessment (FRA) being completed to direct this activity. In the course of conducting an FRA, it is common to find processes that aren't working as they should or, checks that aren't being completed with 100% accuracy. These findings are often part of audit work, but FMA work then identifies residual risk (which is how fraud could still happen with controls in place) to test selected residual risks in order to conclude if fraud or error has occurred. This final stage is key and is different from audit whose focus is predominately on testing the operation of controls. There must be this focus on specifically looking for fraud for a successful FMA to be completed.

Choosing a set of payments or cases (a sample) that is representative of all of the payments/cases

Once an organisation has decided which residual fraud risks to test, a decision must be made as to how many payments/cases can be tested and how these should be selected. It is frequently impractical to test a whole population of payments so statistical sampling is used, but it is vital that the sample selected is representative of the whole population. It can be tempting to simply choose a sample of payments or cases that look suspicious. This does make it more likely to find fraud, however it means that the results of any testing can't be applied across all of those payments or cases. For example, if a representative sample of 200 payments is tested, any fraud rates can be applied to all cases, i.e. if a 0.5% fraud rate was found in a representative sample it can be estimated that there's a 0.5% fraud rate for this specific fraud risk across all payments. However, if a sample of 200 suspicious cases is tested, no conclusions can be drawn around the overall rate of fraud in all payments, as there's likely to be a much higher fraud rate in the suspicious payments chosen for testing.

Selecting enough cases to test

The more cases that can be tested, the more confidence there is that the test results from the sample reflect the wider population from which the sample was drawn. To get the most value from testing, we recommend testing on a statistically valid sample size; a statistician can help calculate this number for any given population. It is also necessary to achieve a balance between the number of cases you can test thoroughly with the amount of resources available. The good quality exercises were those that performed testing in detail, rather than conducting less detailed testing on a larger number of cases.

Focus on fraud

Throughout the planning and testing phases, it is important to focus on looking for fraud. Poorer quality exercises that found less fraud often focused on what is easy to test, rather than testing the most significant residual risks; or focussed on testing controls rather than the gaps in controls that residual risk represents. Overall, those exercises that keep looking for fraud as the main driver in this activity produce good quality results that are useful to the organisation.

Examples of exercises undertaken

9.3% of fraud and error was detected in Bus Service Operator Grants through using online mapping to calculate bus route distances. Grants were made to bus service operators based on eligibility and mileage and in some cases, operators were claiming for more mileage than necessary to complete the route. Fraud and error estimated at £23m.

11.7% of fraud and error was detected in a Facilities Management Contract. The facilities management company invoiced and was paid for work that should have been included under a fixed-rate agreement. Fraud and error estimated at £175k.

2.8% of fraud and error was found in Prescription Payments. Individuals were avoiding paying prescription charges when they were not eligible for exemption based on various eligibility criteria, including age, income, or receipt of certain benefits. Fraud and error estimated at £234m

10.2% of fraud and error was found in the Domestic Renewable Heat Incentive Scheme. Reviews of documentation and site visits found cases of ineligibility, as well as cases where claimants were found to have not declared changes in circumstances, or moving house, which would have made them ineligible to keep receiving payments under the scheme. Fraud and error estimated at £9m.

1.5% of fraud and error was found in a grant scheme run by Sport England where site visits and testing on organisational status found that grants awarded for projects had either not been carried out or completed, or non-eligible organisations were recipients. Fraud and error estimated at £327k.

3.25% of fraud was found by matching data held by the Student Loans Company with HMRC records where students were (wrongly) double claiming the Child Care Element of Working Tax Credit from HMRC and Child Care Grant from Student Finance England (SFE). Fraud and error estimated at £1.1 million.

Fraud measurement and assurance - a vision for the future

The FMA programme has already provided an evidence base to support the hypothesis of the iceberg model and indicates that levels of fraud and error between 0.5% - 5% of expenditure are likely to be found where there is a dedicated and skilled effort to look for it. Although the programme has covered spend areas totalling nearly £4bn since 2014, this is still a small fraction of the total annual expenditure for central government of £667bn[1] that was budgeted for the financial year 2019/20.

The COVID-19 crisis has currently curtailed activities within the FMA programme during 2020, yet ironically it also perhaps gives us a vision for the future. Because of the speed at which COVID-19 support and stimulus measures have been delivered, the risk of losses due to fraud or error has been recognised as abnormally high. All departments have been asked to produce Post-Event Assurance Plans to detail how they will obtain assurance of the extent of losses which may have resulted from fraud or error, and how consequently such losses might be recovered.

The criteria underpinning these Post Event Assurance (PEA) Action Plans have been built, in part, on FMA programme principles. Departments will be using detailed fraud risk assessments to identify areas of residual risk that could have allowed losses from fraud or error to occur and then undertake testing to ascertain where such losses have occurred. The development of statistically valid methods for testing will allow the results to be extrapolated to estimate actual levels of loss within specific schemes and inform business decisions on the value of continuing or expanding testing to maximise recovery of public funds.

This should provide a comprehensive assurance picture for COVID-19 related spend. But what about normal, business as usual, spend? From our own research undertaken during 2019 we know that there appear to be significant gaps in the levels of fraud and error being found within some major areas of government spend. For example, UK government departments spend over £100bn each year procuring goods and services, yet in 2018/19 only 5 departments reported finding any fraud and error within procurement with a total value of only £50 million (0.05%). Similarly most departments pay grants in some form - totalling over £126bn per annum, yet in 2018/19 only five departments reported finding any grant fraud with a total value of £10.6m (0.01%).

It therefore seems a natural extension that PEA Action Plans should perhaps be seen as part of a department's assurance landscape. Forming an ongoing activity to cover all significant spend areas - seeking to identify where losses from fraud or error may have occurred and using statistical sampling and testing to measure and evaluate in order to give government departments for the first time a true understanding of their fraud and error losses.

To contact the FMA Programme please email: fma-programme@cabinetoffice.gov.uk

1 *(source: https://www.ukpublicspending.co.uk/)*

Positives in difficult times

It is difficult to start any summary of recent months, without resorting to the overused word 'unprecedented'. But, as the word encapsulates what the Department of Work and Pensions (DWP) has faced since March, it is unavoidable.

Author:
Andy Macdonald,
Senior Investigations Leader, Serious ad Organised Crime, DWP

It may be difficult for some to find any positives in such challenging times, with the human impact we see around us, but, for us as an organisation, how we have responded to the urgency of the situation has driven development of our Serious and Organised Crime (SOC) investigation and intelligence capabilities at a commendable pace.

Like all of our public sector colleagues, we were aware that the emergency situation created by COVID-19 would be exploited by organised criminals. DWP identified some time ago that to manage fraud you need to have a security and fraud holistic view and maximise the intelligence and insight both areas can provide.

Although, unlike colleagues in HMRC and Local Authorities, we were not paying out COVID-19 specific grants, from the earliest days it was clear that the impact on the economy would have a significant knock-on effect on the number of claims to Universal Credit (UC) made. We knew that this pressure on existing systems would be viewed as a weakness by organised criminals and make DWP a target, so a decision was made from Director level to maintain resources in the 'Serious and Organised Crime' part of our business, to ensure our defences were robust.

DWP's Counter Fraud, Compliance and Debt directorate (CFCD) were braced for attacks and aware that our response needed to be rapid and flexible. It was essential to deploy our resources in the most focussed and effective way.

From the initial identification of multiple attacks, CFCD ensured we had a strategic plan, investing resources in rapid disruption and 'Prevent' teams, while maintaining our focus on the 'Pursue' demands of criminal investigations. This strategy was reliant on the full input of all relevant teams – the Integrated Risk and Intelligence Service (i-RIS) team, who come together to share intelligence, insight, and perform data analysis; the Economic Crime Group for financial intelligence and investigations; and SOC Investigations. Daily meetings were scheduled with these stakeholders, allowing a holistic view of the attacks to be formed, and bringing a shared pool of knowledge, experience and technical skills to bear on the problems.

CFCD has recently published a SOC-specific strategy, to articulate our commitment and role in the Home Office Serious

and Organised Crime Strategy. DWP's strategy highlights, among our goals, the importance, in the digital age, of developing intelligence-led packages for investigators and maximising the exploitation of data that we have. However, achieving these long term strategic goals suddenly became more pressing, as we sought to ensure we had the clearest picture of the criminality taking place, with UC online fraud. One vital springboard early in this process was through analysing patterns of banking intelligence, sourced from our representation on the Joint Fraud Task Force (JFT). JFT is chaired by the City of London Police, whose contribution during this period was invaluable.

When a new type of attack was recognised, the i-RIS could apply their skills to identifying the patterns in both existing claims and new claims. This allowed our investigators to respond quickly to potentially fraudulent claims, preventing any payment being made, and to add vital intelligence to existing investigations. This rapid response intervention has prevented significant losses to the taxpayer, and continues to do so.

As anyone in the law enforcement business knows, all of these technical advances are crucial in responding to an emergency situation, but the real key to success is our people – the most valuable resource.

Some staff find it easier than others to respond to change. After all, many staff were still adjusting to working from home, while their daily duties changed around them. As we embedded the dual disruption/investigation route, and asked staff to be flexible, they responded with commitment and a real sense of purpose. Colleagues from other parts of CFCD, who were new to SOC work, were brought in to provide much needed support. There was a need for our criminal investigators and financial investigators to develop existing close working relationships into a fully symbiotic relationship.

Since April, it has been an ever evolving situation, and this crisis situation has brought out the best in our staff. I know that the challenges I've described will have been replicated through our partner agencies, especially the need to respond to new challenges in the scale of attacks.
It is worth noting that, through this period of new challenges, there was still our 'business as usual' to be handled– some of it not so 'usual'.

Our Economic Crime Group had its first ever virtual confiscation hearing. This was a case listed for the 2nd April 2020 in Manchester Crown Court, which was removed from the list due to COVID-19. The Crown Prosecution Service (CPS) wrote to the court, suggesting that in addition to the need to complete confiscation proceedings, it would be in the interests of justice and, as a minimum, accord with the Criminal Procedure Rules, to deal with the case efficiently and expeditiously. So, on the 8th April, with the defendant's consent, it was heard virtually, and a Confiscation Order for £147,000 granted. An excellent result, owing much to the close working between the CPS, the Economic Crime Group investigator and the prosecuting counsel.

In contrast, on the 14th April, in Isleworth Crown Court, the DWP SOC investigator attended a sentencing hearing, where the traditional physical court attendance was required – although appropriately socially distanced. The main defendant received a 16-month custodial sentence, having pleaded guilty to a £162,000 fraud for false claims to benefit, using a hijacked identity.

These unprecedented times have created an environment where everyone recognises that the wider picture is vital to understanding the threat. Within CFCD, the awareness of what each part of the business brings to the table has significantly increased, driving the development of new ways of working. CFCD's closer working relationship with 'front line' DWP staff has also increased awareness of the challenges we each face and how to support each other, in the identifying and prevention of fraud.

Finally, our representation and full contribution on cross-government bodies through this time has increased our awareness of how we fit into the broader law enforcement picture, allowing us the chance to share with our partners what DWP can bring to the arena of SOC investigation. Although there is still a great deal of uncertainty, for me the important thing to recognise is that there have been positive advances, despite the dreadful circumstances.

The next step is to take stock; evaluate where we are; and ensure we build on this foundation, as we look to the future.

Can risk be your friend?

Tim Barlow (NHS Counter Fraud Authority) talks about how effective risk management can make our life easier as counter fraud specialists

Author:
Tim Barlow,
Senior Quality and Compliance Inspector, NHS Counter Fraud Authority (NHSCFA)

As Roman philosopher Seneca the Younger once wrote, "It's not because things are difficult that we dare not venture. It's because we dare not venture that they are difficult." I like that idea and I think it speaks to a basic truth: if we didn't take some risks in our lives, we wouldn't be able to live at all. Identifying risks and deciding what to do about them is indeed something we do all the time, often without realising it.

Think about the risk assessments most of us have been making every day since the start of the COVID-19 pandemic. Should I go to the supermarket to do my shopping? Should I take public transport? While I have plenty of guidance and information to help me decide, ultimately the answer to those questions depends on some kind of risk assessment which I have to make.

What's all this got to do with fraud? Quite a lot, as I have found out in my current role working for the NHS Counter Fraud Authority (NHSCFA). But first let me tell you a bit about my career, and how my background in risk management has shaped my approach to counter fraud.

My professional journey

I can vividly remember my interview for my first role in the NHS nearly 30 years ago. The building is still standing and the room where the interview took place is still there, although like me the room has had many changes in its use and what it has to deliver!

I started life working for a local health authority, as a maintenance supervisor and painter and decorator. Over the next few years, I progressed through various roles in the estates and facilities department, the last one being that of building manager for a large acute trust. With the private finance initiative (PFI) came significant changes to the provision of non-clinical services at my organisation. I accepted an offer to remain within the NHS as security manager and

NHS Spitfire, photographed by Airwolfhound, is licensed under CC BY-SA 2.0

corporate governance lead for the trust.

This was a turning point in my career. While my previous roles had often had a governance element to them, security management was less familiar territory. The role was also my first encounter with both the NHS Counter Fraud and Security Management Service (a predecessor organisation of the NHSCFA) and counter fraud work.
Jump forward a few years and I moved across to NHS Protect (another predecessor of the NHSCFA) taking up the post I currently hold within the quality and compliance team.

Improving fraud risk management in the NHS

A few years ago I started thinking about how NHS organisations assessed and recorded risks relating to fraud, bribery and corruption, and I felt this was an area where improvements could be made.

The NHSCFA has a set of standards for NHS organisations' counter fraud work (these will be replaced by the Counter Fraud Functional Standard next year). One of the standards relates to the management of fraud risks within organisations.
I suggested some changes to this standard, whereby fraud risk assessments had to be undertaken at a local level and fraud risks had to be recorded and managed in line with the organisation's own risk management policies. These changes were implemented last year, and the NHSCFA's quality and compliance team started an exercise to measure the level of fraud risk assessment undertaken across 500 NHS organisations in England and Wales.

The findings showed that risk analysis was being undertaken by local counter fraud specialists (LCFSs), but this was of mixed quality and detail. Furthermore, very few health bodies were recording fraud risk assessments in line with their own policies and managing risks accordingly.

The NHSCFA supported me in delivering a series of workshops to support our LCFS colleagues in fraud risk management. I tried to put a practical slant on the topic, as I always do, and since most LCFSs had little or no risk experience I adapted the workshop from my old life in governance to my new life in fraud.

The workshops were followed some months later by the testing of those 500 organisations again on their compliance with our standard. The findings showed a big improvement in fraud risk assessment at a local level. Following the initial evaluation and the workshops, there was an increase of 130% in organisations undertaking local fraud risk assessments and managing them in line with their own policies.

This was really positive and spurred me on to continue to develop this area of counter fraud work within the NHS.

The road ahead

The NHSCFA will assist and support the NHS in complying with the Counter Fraud Functional Standard and my fraud risk management journey will continue.

This year, with the help of my colleagues, I will deliver a further series of workshops to embed the Government Counter Fraud Profession (GCFP) fraud risk assessment methodology.

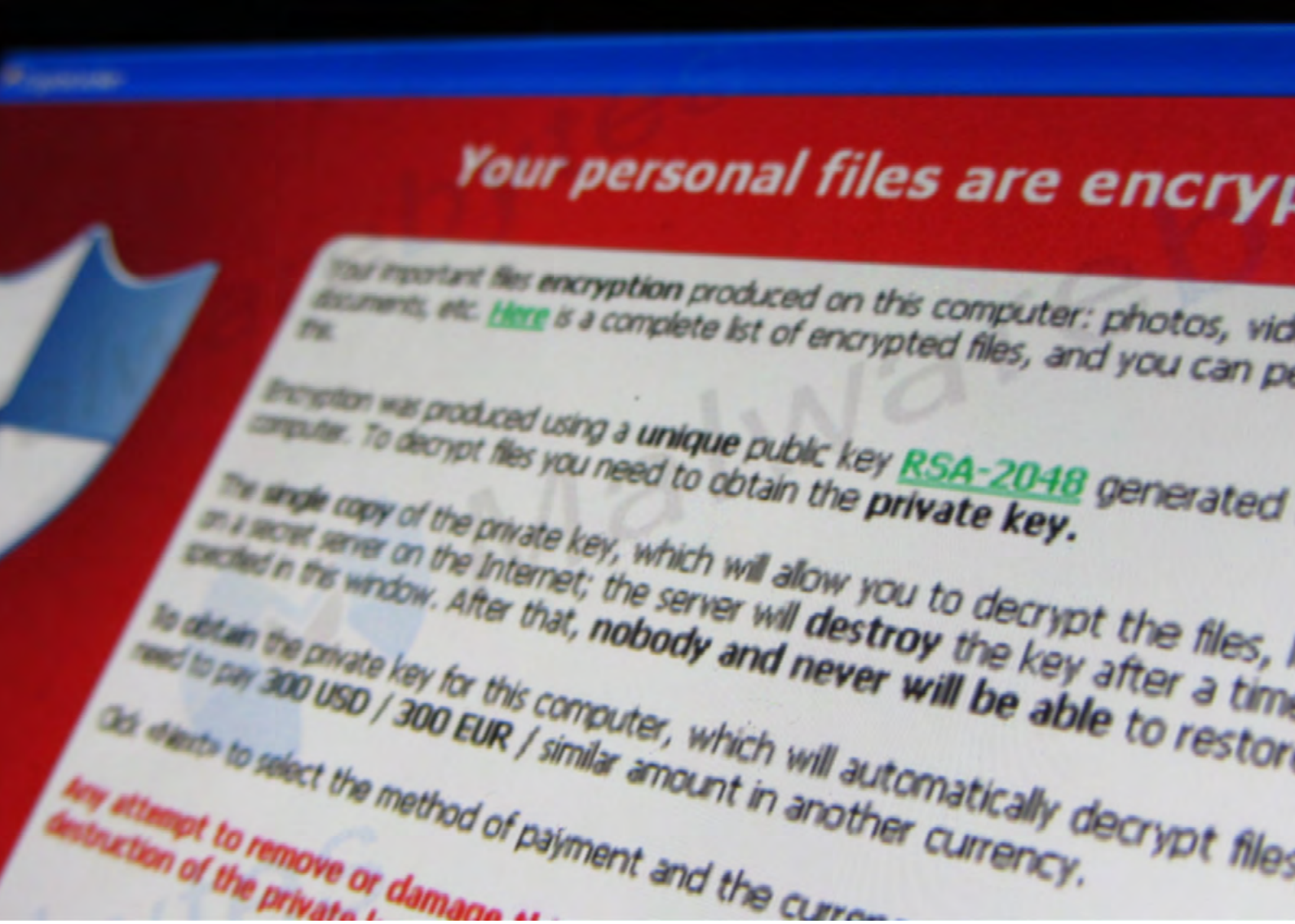
This work will develop the skill sets of LCFSs, not only in fraud risk assessment, but also in how it can contribute to proactive counter fraud work. This will help ensure that fraud risks become truly embedded within organisations, with ownership resting with those people who can put in place any mitigation that may be required at a local level. This is important as an LCFS could not possibly undertake all actions identified to mitigate areas of risk. For example, staff undertaking pre-employment document checks should be trained to enable them to identify forgeries.

"It is really important that we make the link between detailed fraud risk analysis utilising the GCFP fraud risk assessment methodology and proactive fraud exercises undertaken across the NHS," said Sue Frith, Chief Executive Officer of the NHSCFA and a member of the Counter Fraud Function Board.

"This will ensure local counter fraud resources are used effectively. The NHSCFA are committed to reducing fraud risk and I am confident that the work we are currently undertaking in this area will support health bodies in mitigating their local fraud risks."

This work will be undertaken locally within the NHS and overseen at a national level by the NHSCFA, who in turn will report back to the Government Counter Fraud Function.

We are all experiencing change, at a pace we may have never had to deal with before. This makes it all the more important for us GCFP members to follow Seneca's advice: if we take the lead and ensure that fraud risks are identified, mitigated and reduced as far as is reasonably practicable, this will make it easier for government to fight fraud and protect the resources that are entrusted to it.



Fraud fighters unite to defend the UK from COVID-19 crime

David Clarke, Chair of the Fraud Advisory Panel (FAP) and a former police head of the National Fraud Intelligence Bureau explains how the charity is acting as a conduit for information and intelligence sharing to protect businesses during the pandemic.

Author:
David Clarke,
Chair, Fraud Advisory Panel

This is an extremely grave time; a tragic moment when people are fearful of losing their jobs, and as governments around the world are providing life support systems for businesses and citizens. And yet it is also a time when criminals are lining up to kill that support.

Fraudsters are devious, cruel and heartless and will strike when a victim is most vulnerable and has least protection. Stealing an elderly widow's life savings or faking accounts to trick investors are all part of the dirty game for those who abuse trust. The pandemic has provided an army of criminals with the perfect battlefield; they have the high ground, they've also had weeks in lockdown to prepare their mass attack on targets with riches to plunder and weak defences.

Cryptolocker ransomware, photographed by Christiaan Colen, is licensed under CC BY-SA 2.0

To bolster those barricades, the fraud-fighting community across the public, private and third sectors have united like never before and the Fraud Advisory Panel is playing a crucial, coordinating role.

As the respected, independent voice of the counter-fraud profession since 1998, our vision is to see the world free from fraud and for everyone to have access to knowledge, skills and resources to protect against economic crime in all its forms. We bring together the greatest talent in the counter fraud world and promote advice, education, collaboration and research. Most advice is provided free of charge by volunteers who are experts in their field. We also actively engage in public consultations, provide commentary for the TV and press and lobby government to implement change to the law and policy.

When lockdown was announced in March, the Fraud Advisory Panel, many of whose members have been on the frontline preventing, investigating and prosecuting fraud for decades, mustered their forces to take the battle to the enemy with the formation of the COVID-19 Fraud Watch task force. This cross-sector, cross-industry coalition of trusted partners meets online to share information on emerging fraud threats affecting businesses and consumers. It acts as a conduit to get fraud advice out far and wide - particularly to businesses that may not be aware of risks - and to encourage people to share intelligence with the authorities.

Whilst 2019 seems an age ago, this was a busy year for us. We commenced a strategic review to transform the way we support our members, with exciting plans for the Future Fraud Professionals Network – those who will continue the fight in the decades ahead. We participated in two inspection reviews by Her Majesty's Inspectorate of Constabularies; one was looking at the police response to fraud and the other at cybercrime. It was pleasing to see many of the things that we suggested reflected in the findings. We also helped shape the Action Fraud review and guidance that has been issued. We are very supportive of the service and want to see it improve.

This was also the fourth year in which we've jointly led the award-winning annual charity fraud awareness week with the Charity Commission. This is now a global event and last year involved partners in Australia, New Zealand and the United States of America. The finishing touches are currently being put to this year's campaign, which will take place on 19 – 23 October, at a time when the services and support provided by charities are in great demand. It's a fabulous achievement that protects noble organisations and people who do so much good and yet are targeted by bad people.

March 2020 brought the pandemic and the severity of lockdown. Like many businesses, my own included, our charity was impacted. Training and events were temporarily suspended and my two full-time colleagues, Mia Campbell and Zara Fisher, who do terrific work, immediately upped tools and moved to remote working. They not only continued their normal duties but also helped us to divert all our efforts into protecting society during the pandemic.

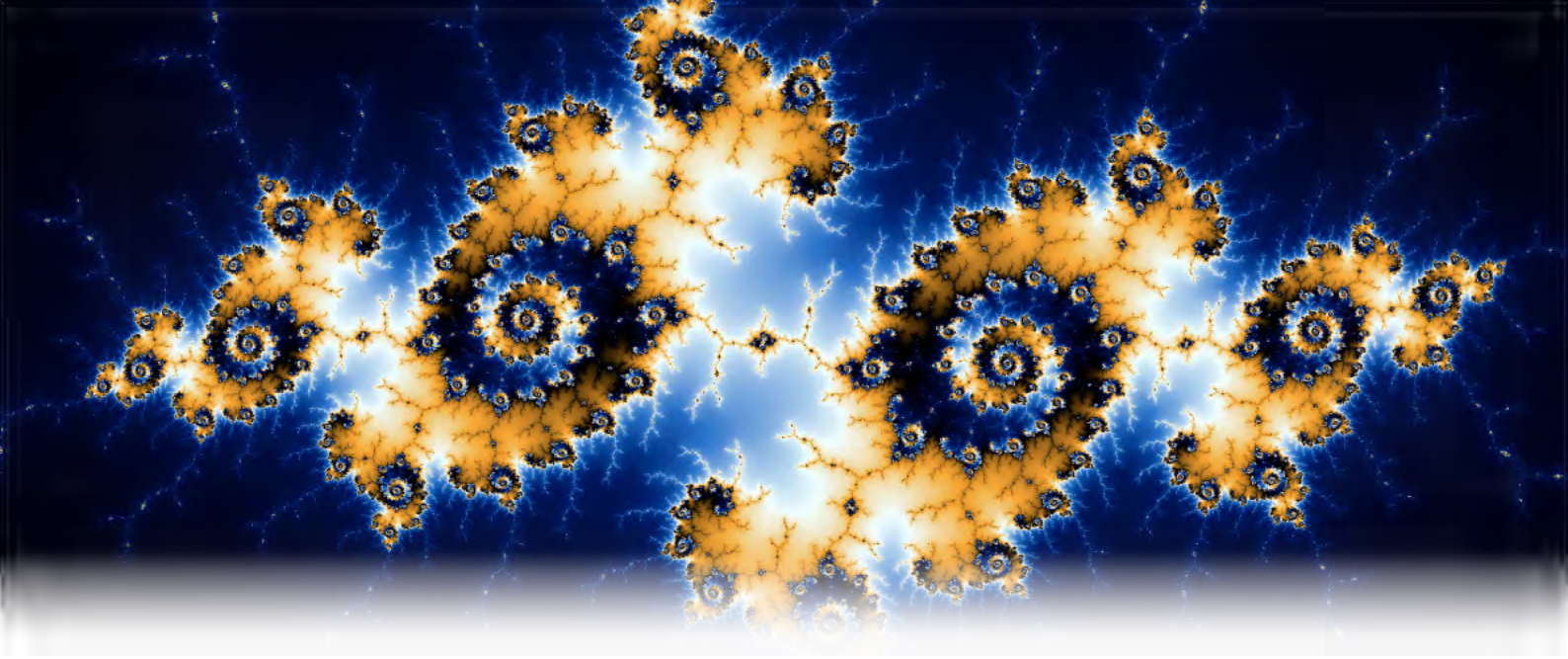
I am honoured to see so many partners rallying behind the Fraud Watch banner and grateful to the Cabinet Office and the City of London Police for their continued support with our weekly bridge call. I can't go into detail but we have shared considerable intelligence that has been acted upon including things related to PPE and other fraud against stimulus packages. I'm also grateful to my own company, Guildhawk for supporting my Fraud Advisory Panel role during this challenging time.

Fraud related to Bounce Back Loans led us in June to write to the Chancellor of the Exchequer to request that the names of companies receiving taxpayer backed loans be published to allow data matching and offering our support.

In our recent special report entitled, The Calm Before the Storm, we asked if this would be the year when the country made the necessary changes to turn the tide on fraud or when it dropped the ball completely?

Only time will tell if gatekeepers have done enough to protect us from a potential tsunami of fraud but we do know that the rubble from the 2008 financial earthquake was not cleared before the coronavirus and the world feels similar tremors once again.

Globally, governments and businesses know the impact of not doing enough to prevent fraud and unlike the 2008 crisis, this time there will be no hiding behind, 'I did not know'. We know it is every leader's duty to do everything in their power to prevent the devastating impact of a financial crisis made worse by fraud.



Companies House Intelligence and Enforcement Unit: evolution to revolution

Author:
Mark Buckley,
Head of Intelligence and Enforcement, Companies House

There's a saying 'mighty Oaks from little acorns grow' and this can be said of Companies House's new Intelligence and Enforcement Unit. The Unit was formed in 2014 with a remit to gather enforcement functions together, help enforcement agencies tackle economic crime and tackle data integrity on the public register of companies.

As I look back, 2014 seems like a lifetime away; we were at the start of what has become a very exciting journey. But before I get to that, I should start at the beginning: Companies House was at the start of its transformation, the recent government consultation on reform to the company register hadn't been conceived and we were cautious about changing incorrect data on the public register because we were limited by tightly defined statutory powers.

Our interaction with enforcement partners and our ability to identify suspicious activity on the register was reactive and often, by the time we discovered it, the perpetrators had vanished leaving nothing or no-one for enforcement partners to investigate. Our goal was to become less reactive and, within our existing powers, become better at identifying suspicious activity closer to the event. No small task.

We identified pockets of incorrect data on the register, impossible things like dates of birth from 1066, customers using the wrong forms and a whole list of others which we tackled by correcting data or contacting the company asking them to submit corrected information. This was labour intensive, retrospective action and we recognised this was not sustainable longer term.

One of my key roles was to engage with enforcement partners, 'Grow the Brand' and explain the type of data the registrar held which could potentially assist with investigations. This was a challenge; we hadn't engaged for a while and organisations had differing understanding of the Registrar's role. Some organisations thought we had investigative powers, others thought we should be able to validate all information, many felt we were too passive in our registration approach. However, by engaging and communicating our role, our statutory obligations and, more importantly, our valuable data set, my colleagues and I built trust and Companies House has become a key partner for many agencies.

We routinely deal with the police, Insolvency Service, Government Agency Intelligence Network, HMRC, Trading Standards, and over 70 other organisations, including agencies related to the prevention of money laundering, organised crime and fraud. As a result of this activity, our workload has increased exponentially and is around 2,000%

greater than when we started. There are still organisations out there that do not utilise our valuable resource, but we are working on it.

The work in the early part of our evolution was reactive and labour intensive. We had to write to companies to fix data, and analytics were time consuming due to having to access multiple systems. We needed to find solutions to improve our delivery. Our engagement was successful, and we were in danger of outstripping our ability to service the growing demand.

The next part of our evolution involved implementing new legislation. In 2016 we introduced the world's first publicly accessible Beneficial Ownership register. This was a learning curve for us from a data perspective as, six months in, Civil Society groups identified 500 variants of the word 'British'. We needed to fix this and develop a solution to prevent the error recurring. Using data science, we digitally cleansed the incorrect data. By removing an open text field and introducing industry standard drop down lists, we eradicated the problem overnight. We were changing our approach to data capture and our data science team is now at the centre of decisions around data strategy.

Since then, we have introduced Registered Office and Director Disputes legislation which gave customers who had had their home address used as a Registered Office or had been appointed as a director without consent a means to correct that error. We are now providing services to mitigate risk to citizens who have had their personal data used. These new processes surface suspicious activity which we pass to enforcement partners to investigate. Introduction of other processes such as Report it Now and first-time director notices have pushed discovery of suspicious activity closer to the event which in turn allows enforcement partners the opportunity to catch those responsible.

In collaboration with the Cabinet Office, HMRC and the Insolvency Service, we were the first organisations to make use of the powers in the Digital Economy Act – we initiated a trial, analysing accounts data held by HMRC and Companies House to identify potential errors in reporting. This helped HMRC identify millions in unpaid revenue and the Cabinet Office Digital Economy Act Board signed off the process as business as usual in 2019.

In January this year we developed the Obliged Entities reporting scheme under the 5th Anti Money Laundering Directive and we have received more than 4000 cases through the portal since its introduction. This process allows Obliged Entities such as financial institutions to report any discrepancy they see in the person of significant control data they have been provided compared with information on the public record. This is another proactive tool helping us determine suspicious activity closer to the event.

I mentioned earlier some partners felt Companies House was too passive in its checks and should undertake more verification and validation of information applied to the public register. This is one of our challenges; Companies House is a registry of information and the purpose of the Registrar of Companies has not changed fundamentally since 1844.

In 2018, following lobbying by enforcement partners and other organisations, the need for register reform was recognised in Government and in 2019 the Department for Business, Energy and Industrial Strategy (BEIS) issued a public consultation that will potentially be the biggest change to the register since 1844.

The Government's response to the consultation has now been published. The proposed reforms will require, Companies House to validate and verify information applied to the public register including identities of those filing information with the Registrar. There are also many other proposed changes to help ensure the register information is relevant and trusted. This will help enforcement partners fight economic crime and deter anyone wishing to use the register as a mechanism to commit crime. The Government's response can be accessed through the following link: https://www.gov.uk/government/consultations/corporate-transparency-and-register-reform

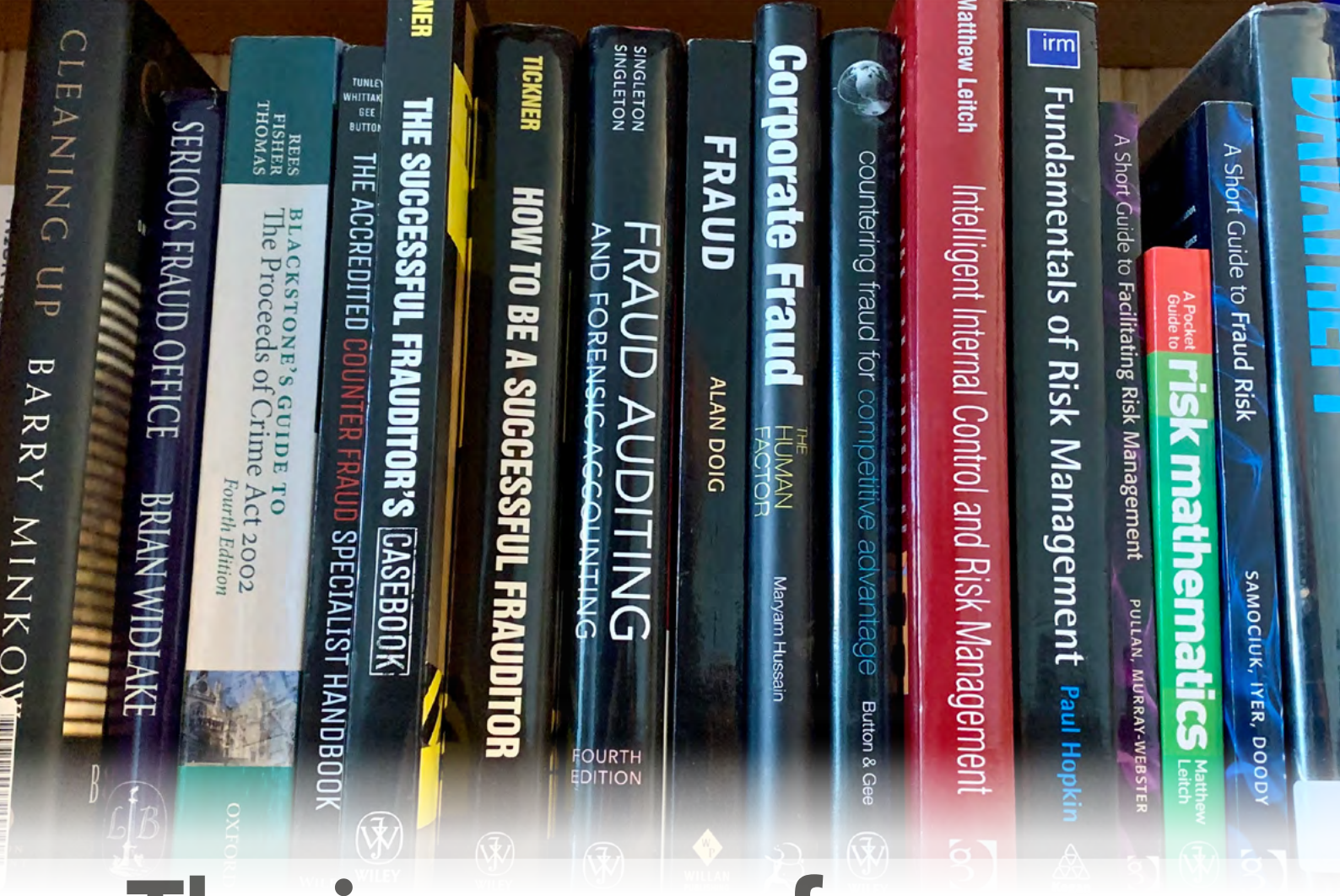
Over the next year, we aspire to develop our people under professions. We have started to roll out the Operational Delivery Profession and Intelligence and Enforcement are committed to creating a development programme aligned with the Counter Fraud Profession. We have plans for this to be in place by next year. Once embedded, we are committed to joining the Counter Fraud Profession and see membership of the profession as a key part of developing a centre of excellence for Intelligence and Enforcement.

We recently introduced a new role as Head of Intelligence, Matthew Pennell, who is collaborating closely with Intelligence and Enforcement partners. During the coronavirus (COVID-19) outbreak, the Intelligence hub has run daily analysis for the Cabinet Office, in real time, to identify suspicious patterns linked to Government levies. Matthew is developing our Intelligence capabilities and is building on the great work we've done with enforcement partners to date.

I mentioned earlier the need to find ways to improve our analytic capabilities. Over the next few years, we will be seeking to develop analytic tools utilising Artificial Intelligence to identify suspicious activity on the register. This is an exciting development, still currently in discovery, but we have already identified patterns of company filing linked to suspicious activity and built algorithms to capture this information. This will truly move us to a proactive model and improve our ability to turn around large intelligence tasks quickly.

We are now starting the next chapter in our 'Revolution', with the advent of register reform, developing modern analytic tools, developing colleagues as Counter Fraud professionals, creating an Intelligence function and improving our capacity to service enforcement partners' needs. The future is bright and exciting.

Companies House is in a position where it has the capability and skills to be making a real difference in the UK's fight against fraud, money laundering and economic crime. We have come a long way in the last 6 years. Who knows what the next 6 will bring?



The journey of a distance learning counter fraud graduate

Author:
Ellie Gilbert,
Head of Investigations and Monitoring, Bank of England

Joining the Metropolitan Police as a member of civilian staff at 19 was only ever supposed to be a temporary stopgap until I worked out what I wanted to do. This decision, however, turned out to be a little longer-lived than that, with a career spanning four very different departments and a period just shy of 17 years. During this time, I moved from recruitment to case management, then spent a decade working in an intelligence unit and finally on to fraud investigation. Towards the end of my time in intelligence, I began working with a financial investigator to profile organised groups, committing fraud and money laundering offences at and against Heathrow Airport, and from this point on, fraud had me hooked.

I had finally found my passion and a real thirst to understand why these offences were committed, alongside a curiosity of why people and organisations fell victim to this particular crime type. By sheer coincidence, around the same time, the Metropolitan Police were setting up a new unit dedicated to fraud investigation - Operation Falcon - and were also trialling the use of police staff investigators to work alongside teams of police constables and detective constables carrying independent caseloads. I knew at once this was the opportunity I was looking for, to compliment what I had already started, and I successfully gained a promotion to join a volume fraud hub in 2014.

Joining Operation Falcon was a baptism of fire; I had no idea of the levels of fraud committed locally, nationally and internationally, and the volume of cases being reported into the hubs just never seemed to decline. I quickly took on my own cases and was exposed to the full judicial process. The inner analyst in me soon began to notice trends and patterns in offending which I wanted to explore more. However, joining the intelligence picture up wasn't a priority at the time, having opened

the floodgates of cases coming in. This exposure and hands-on experience was the spark I needed and, aged 34, I successfully applied to join the Counter-Fraud and Criminal Justice BSc programme with the University of Portsmouth, as a distance learner.

Re-starting my education as an adult learner was an exciting experience. This time around I was focused, interested, and invested in everything I was learning about. Coupled with this, the majority of what I was studying I could apply directly to my day job, or gave me a better understanding of why this crime happened at all. I remember vividly sitting through the first onsite induction days in a university lecture theatre, listening to a talk about prisoners and offending patterns, and having at least two or three 'light bulb' moments. It brought it home to me that my daily exposure to the criminal justice system and associated processes were just one small cog in a slightly broken system.

A knock-on effect for me during my first two years of study was that it helped me to focus on my future career opportunities and what I wanted to do with a developing skill set and interest in fraud and investigations. I knew that I didn't want to go into uniformed policing and that I had limited prospects as a civilian investigator. With that in mind, I decided to leave policing for the world of corporate investigations. This decision was made harder by the fact I still had three years of study ahead of me, and modules to complete while learning the ropes of a new role, and a new industry.

Thankfully, I persevered and quickly found my feet. Once again, the skills I had picked up from my time of studying in the preceding two years helped shape my entire experience at work (a bold statement, I know). The apparent benefits included the structure and delivery of reports and incident management statements, critically reviewing my work from an academic submission point of view helped me strip out the superfluous details and focus the content for a busy professional audience. However, the surprise benefits for me included a better relationship with stakeholders and members of senior management by virtue of the fact I had become used to seeing arguments from both sides of the table and could, therefore, act as an empathic listener and a persuasive speaker.

Distance learning, however, doesn't come without its challenges, and it would be amiss of me to misinterpret this undertaking as one of all positives. It has been incredibly challenging to manage my time at points throughout the past five years, with the most challenging aspect being trying to complete my dissertation in lockdown while homeschooling four children and managing a team of staff remotely in a global pandemic. I wanted to throw it all in on more than one occasion and, had it not been for a close group of fellow students facing similar challenges, I would have walked away a long time ago. It cannot be emphasised enough just how important a strong support network is, be it fellow students, supportive family and friends or an understanding employer.

Likewise, the physical separation from everybody on your course can be equally isolating, especially when you're trying to complete assignments at the end of a module (often, in my case, all weekend and through the night), and you feel like the only student in the world at the point going through the pain of writing. It wouldn't be unfamiliar for a 2:00am WhatsApp chat to kick off when one of us was hitting the proverbial wall and couldn't find the willpower to finish off: just the accountability of sending a 'word count check-in' to the group was sometimes the little push we needed to get us over the finish line.

However, in conclusion, the opportunities that have arisen from my time of study, alongside the enjoyment of just increasing my knowledge around a subject I find fascinating, has made all the hard work worth it. I would recommend anybody considering going 'back to school', to jump in and try it. Often courses will let you take it year by year, so you're not committing to 4/5 years all at once, alongside the financial burden that accompanies it.

My next adventure? I haven't quite finished my learning journey yet and have signed up to continue onto an MSc course in September. They say what doesn't kill you makes you stronger, and if I can write a dissertation during a lockdown, I can make it through the next time the world turns upside down.

Hold the line: the fight against telecoms fraud

Author:
Rob McGregor,
Verizon, currently the Chairman of TUFF's Board of Directors

Telecoms fraud is usually described as the misuse of telephony services for financial gain. The sector has a long-standing history of suffering fraud, but it can take many different forms and is often difficult, and sometimes impossible, to identify the perpetrators. Losses can grow very quickly, meaning that action has to be taken immediately to prevent putting businesses into financial jeopardy. Furthermore, it is often seen as a victimless crime, which can result in a reduced emphasis on preventative measures. Such fraud is well understood and the methods and efforts needed to ensure that losses are reduced are in place in most telecom companies across the globe.

Telecoms is a fast-moving technological minefield of threats, suffering from a regular resurgence of fraud losses where old methods to commit fraud return and new methods to subvert security are made available, with added features. There can often be a mind-numbing level of complexity to get to grips with but, focusing on fundamental tried and tested methods often provides an appropriate start point.

Prevention efforts can be focused on areas known to be at great risk of fraud and monitoring is key to ensuring that any loss-causing events are detected quickly and controls used to ensure that those losses are minimised. But monitoring involves many different elements: sets of products; services; processes; inventories; and, people.

Additionally, physical security measures must be in place to protect physical assets. Fraud and security departments should be 'joined at the hip' on this, pooling resources and expertise to avoid a fragmented and weakened approach.

In summary, telecoms businesses must ensure that they perform regular risk assessments, instigate suitable monitoring, activate the necessary controls and be ready to perform investigations.

This all, of course, leads to questions about what we have learned already that can be of use in other sectors? What shared threats can we take direct action against together as an industry? How can we get ahead of the risks, and stop risks turning into losses?

One thing that has been learned, which can be applied everywhere, is that effective measurement and monitoring tools must be in place. In telecoms companies this means that we must be able to see the transactions that occur in every area that could be manipulated or that show fraud happening.

We are moving to an IP telephony world[1] where calls are not all chargeable events and that presents its own problems. Call records are primarily only useful where calls are being charged for. However, where calls are non-chargeable, this is where the biggest threats with the greatest loss growth-rates can occur.

Although there are many types of fraud occurring in the telecoms industry right now, most telecom companies agree that one of the main threats facing us all is International Revenue Share Fraud (IRSF), also known as International Premium Rate Fraud (IPRF). These fraud types are such a threat because they rely on the fact that laws do not usually cross country borders. Tracking down call routing through many carriers, who are often just reselling minutes, can be so arduous that it stops all meaningful investigation. Criminals also have the ability to anonymise originator activity, where phone systems being attacked are internet connected and being targeted via VPN privacy channels in multiple originating countries. In such cases there is almost no chance of finding the perpetrators.

In some ways, it is worse that there are companies, who are legitimately working on selling the termination services, allowing

1 *IP telephony uses "internet protocols" to communicate over the internet, rather than traditional phone systems.*

Disguised mobile phone mast ar Parc El Harti, Marrakech, Morocco, photographed by Images George Rex, is licensed under CC BY-SA 2.0

these frauds to occur. They are in contravention of rules set by the International Telecoms Union (ITU) in their documentation E.164. These rules relate to number hijacking, telling operators that they may not terminate calls to a number range for one country in a different country. This is often called short-stopping, and simply means that you can terminate the calls more cheaply than anyone else while collecting a large inbound payment for delivery of the call. You can share this excess revenue with your customers and offer to pay them very quickly - even before you have been paid. The issue is that the calls being made to these numbers can be illegally increased and the out-payment collected so quickly that the funds are in the hands of criminal entities to the detriment of legitimate businesses. In researching this article, I have found that the ITU have added a reporting tool to their website that allows carriers to report misuse of international number ranges.

It is such a significant issue that telecom companies are now resorting to not paying each other for traffic found to be of this type, in breach of existing contracts. This has resulted in legal action being taken between companies as well as termination of contracts.

Worryingly, even with the reduction of funds being passed between carriers, cases keep occurring. Even with protections in place, and detected fraud resulting in non-payment, there is still room for a money laundering equivalent where the calls are paid for and reported as legitimate, and the revenue share collected from the termination point, leaving the criminals with 'clean' money.

This insight into one particular fraud type highlights some of the difficulties that arise and really shows how even simple problems can escalate into huge losses for businesses that we cannot stand.

Having been involved in the Telecommunications United Kingdom Fraud Forum (TUFF) since it began, in one way or another, and currently being the Chair of the Board of Directors, it is clear that we, as fraud professionals, need to ensure that we have a route to share data to prevent crime and limit losses.

Forums are the most important part of our response both as a business sector and across industries. They allow a non-competitive arrangement, where threat data sharing can occur that does not breach data-sharing regulations, and which allows a wider discussion than is usually possible within organisations working in isolation.

That is the key element of support for telecoms fraud professionals that TUFF and other forums seek to achieve. I strongly recommend, as a starting point, to become a member of one or more of the fraud information sharing groups. TUFF would welcome operators from around the globe and more information can be found at www.tuff.co.uk.

In 2018 telecoms fraud was estimated to cost $17 billion. In 2019, it was $28 billion.

Some of the more common types of telecoms fraud are:

Interconnect bypass or SIM box fraud

Where the mobile phone to mobile phone rate is less than the international termination rate, local SIMs are used to terminate international traffic to mobile customers.

International Revenue Sharing Fraud (IRSF)

This has been the most damaging fraud scheme for the telecoms industry to-date. It involves transferring monetary value from one carrier to another, based on the inter-carrier trust between telecom operators. Patient criminals wait for the call logs to expire before executing any further money laundering steps.

Vishing calls

Vishing (a combination of the words Voice and Phishing) is a phone scam in which fraudsters trick victims into divulging their personal, financial or security information or transferring money to them.

One (ring) and cut or Wangiri

Japanese for 'one ring and drop the call' – is a telephone scam where criminals trick victims into calling premium rate numbers. A fraudster will set up a system to dial a large number of random phone numbers. Each call rings just once then hangs up, leaving a missed call on the recipients' phones. Users often see the missed call and, believing it to be legitimate, call the premium rate number back. Even if the caller hangs up immediately, they will still be charged for the call.

Previous issues

Issue 2, July 2019

- Bringing the Government together on fraud risk
- Three credos of cyber crime
- DFID's counter fraud community
- Why you should really consider breaking your own fraud controls
- The benefits of data sharing: a fraud pilot
- Scambusters: Using technology to tackle criminals intent on conning the elderly and vulnerable

Download now from: https://bit.ly/journal-issue-2

Issue 3, December 2019

- Is the language of fraud failing its victims?
- Grants fraud
- Claims farming in insurance
- A career in counter fraud
- Scottish counter fraud community

Download now from: https://bit.ly/journal-issue-3

Issue 4, March 2020

- Countering fraud in disasters
- The counter fraud fucntion
- Fraudsters are people too!
- National trading standards
- Mass-marketing fraud
- Preventing and detecting fraud using machine learning
- Tackling Economic Crime Awards
- Local authority counter fraud
- Network rail
- Apprenticeships
- International collaboration

Download now from: https://bit.ly/journal-issue-4

Issue 5, June 2020

- A wider perspective
- Government Counter Fraud Fucntion's COVID-19 response
- COVID-19: Maintaining a controlled environment
- Insurance fraud
- Career change
- Coronavirus, fraud risk and the use of the word "scam"
- Digital detectives in the NHS
- How the UK justice system hs adapted to the pandemic
- Black swans

Download now from: https://bit.ly/journal-issue-5

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

Contact us:

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