Government
Counter Fraud
Profession

The Public Sector Counter Fraud Journal

ISSUE 9, FEBRUARY 2022

ISSN 2755-1024

Collaborative working: More than just a slogan

Editorial Board

Cover Image: Josh Calabrese on Unsplash

CONTENTS

Editor’s letter

This issue’s letter is provided by Chris Freeman, Head of Engagement and Membership for the Government Counter Fraud Profession.

Is this the first time you have picked up a copy of the Public Sector Counter Fraud Journal? Or have you perhaps been a regular reader since it launched? Either way you are in good company; last year we saw the Journal surpass the milestone of a combined 50,000 downloads across all issues since it was first made available online. In fact, we are - at time of writing - past 53,000.

The success of the Journal could be attributed to many things. But I prefer to think of it as indicative of the willingness of those working in counter fraud around the world to learn more about the subject and the fact that even people who do not work in counter fraud find it a fascinating area.

Diversity brings strength. However, fraud is diverse in its type, scale, who falls victim to it and who it is perpetrated by. Because of this it impacts us all, personally and professionally. Countering fraud effectively, therefore, also needs a diverse response in order for it to be successful. And, as fraud continuously evolves, the response must continually evolve too.

This Journal, therefore, aims to bring you content to help build an understanding of the different types of fraud, modus operandi and the approaches taken to mitigate fraud. And, in the event mitigation hasn’t been successful, the actions taken to resolve and, where possible, prosecute.

In this issue you will learn more about collaborative working: how a group of businesses in banking, technology and telecommunications came together to develop a service to keep their customers safe from fraud; how the NHS Counter Fraud Authority worked with the Crown Prosecution Service and Greater Manchester Police to prosecute a prolific criminal determined to cover his tracks; and how the Government Counter Fraud Function has worked with other organisations to run a public communications campaign to raise awareness of COVID Pass fraud.

Professor Michael Levi provides an in-depth piece on how criminals use ‘money mules’ to evade anti-fraud and anti-money laundering measures and the efforts taken to stop this. Dr Benjamin van Rooij and Adam Fine, authors of 2021’s The Behavioural Code, write about the difficulties of designing rules aimed at prevention rather than prioritising liability, including the intriguing case of a multi-billion dollar company which has a policy on travel, gifts and hospitality that comprises just five words.

Duncan Warmington reflects on his lengthy career in counter fraud and how the Government Counter Fraud Profession represents a significant step forward for building capability in the public sector. It was Duncan, through his passion for continuing development, who finally convinced me in 2008 to study for a Master’s in Fraud Management; I suspect I am not alone in that and his article is a reminder of the varied career paths possible in counter fraud.

You will also find articles on corruption in the Nigerian public sector, the potential insider threat due to remote working and how HMRC taxes the proceeds of crime.

If, like me, you find the footnotes and references for articles really useful for directing your further research you will now find these all on page 31. This allows a little more space for the articles without any clutter. You will also find links to previous issues of the Journal on page 30, so if you have missed any you can still catch up.

We always welcome feedback and suggestions or ideas that could be featured in the future, so please do get in touch via gcfp@cabinetoffice.gov.uk

Chris Freeman
Government Counter Fraud Profession

When collaborative working is more than just a slogan

David Hall, Fraud and Financial Investigation Lead of the NHS Counter Fraud Authorty, explains how a prolific fraudster was put behind bars by agencies working together

Author:
David Hall
Investigation Lead, NHS Counter Fraud Authority

As Aristotle said, the whole is greater than the sum of its parts. In modern times we talk of agencies working together, collaboration, joined-up thinking and working in partnership. There is no shortage of feel-good phrases or slogans to describe these important aspirations in the counter fraud community. But what do they look like when actually put into practice?

Having spent 45 years in law enforcement, I was moved to nominate this recent fraud investigation for the prestigious Tackling Economic Crime Awards (TECAs) as I wanted to showcase some excellent collaborative teamwork that led to a significant, successful prosecution and sentence. The TECAs recognise and celebrate those who have demonstrated commitment and outstanding performance in tackling economic crime. Although we did not win the award on the night, we are very proud to have reached the finals. By "we" I mean my organisation (the NHS Counter Fraud Authority), Greater Manchester Police (GMP) and the Crown Prosecution Service (CPS).

This case saw a wide investigative and prosecution

Photo by Ray Harrington on Unsplash

team collaborating to ensure a successful conclusion, with Stephen Day - who defrauded £1.3m from private clients and the NHS - sent to prison for 11 years, subjected to a Serious Crime Prevention Order and facing confiscation proceedings.

At court, Day did his best to frustrate and delay proceedings, but the high morale and determination of our combined forces thwarted that. The prosecution began in 2016 and we applied relentless pressure until Day accepted the true value of his fraud in 2021. The final year of that process was achieved amid the COVID-19 pandemic lockdown. The sentencing judge called it an "exceptionally complex case" and a "very high standard" investigation. The former demanded the latter and it is hard to see that if any one of the partners had shouldered this case on its own, we would have got anywhere close to the same result. Collaboration was a necessity rather than an optional extra.

GMP investigated the private client frauds, NHSCFA the NHS fraud, CPS managed the prosecution, and all collaborated closely. The investigation embraced the broad vision of the Counter Fraud Profession, bringing cross-sector skills together to deliver the right outcome. Is that just more feel-good talk? What difference did it actually make?

The material seized from Stephen Day filled two Transit vans. As a skilled accountant he did his best to hide his fraud. For example, he falsely labelled multiple transactions as payments to HMRC when sending money to his own companies. Our team had to painstakingly find the pieces and assemble a huge jigsaw of evidence.

Playing to the relative strengths of our team members was crucial. The Police had seized large amounts of digital data from Day but needed help with its analysis. The NHSCFA had a dedicated team of forensic computer specialists but needed greater access to Day's data. Drafting a bespoke Memorandum of Understanding (MOU) to enable our teams to share and exchange data and skills unlocked our full capabilities.

We kept our prosecution strategy under constant review. A key stage was instructing a forensic accountant. We needed a high quality report, and fast, to respond robustly to the defence challenge. All pulling together, the CPS paralegal officer ensured that the forensic accountant had the required material (which was substantial). The NHSCFA FCU provided copies of Day's SAGE records. The Police lead investigator gave guidance on the material and explained how it fitted together. CPS lawyers gave guidance on the key areas of defence challenge and explained what the report had to contain to address it. The result was a fast and detailed report which finally forced the defendant to concede the true value of his fraud.

The momentum of the successful operational outcome pushed onwards into how we handled communications too. Press officers who were used to "beating" each other to break news to the media and put their own brand in pole position, took a longer, more relaxed view and planned their strategy together.

We found that having made the commitment - the leap, even - to a fully collaborative approach made it hard to go back to anything less. In short, the collaboration had already brought multiple rewards:

- Strengthened evidence
- Improved team skills and access to equipment
- Faster expert report produced
- Data access and improved responses to disclosure requests
- Day was sentenced for the true value of his many frauds
- Day's lack of remorse was fully registered and reflected in the sentence
- Extensive media coverage and corporate communications maximised, enabling the lessons learned to be spread widely.

But collaboration does involve certain risks – including letting go of a long-established mindset, where you stick to the safety of working within the boundaries you know, with the people you know, in the tried and tested ways you know. This case was about embracing the concept of 'dare to share', using regulatory channels and lawful gateways to share information and data. This is at a time when investigators and prosecutors may feel (rightly or wrongly) trussed and bound by the requirements and rules they are under - especially around use of data - compared to the extensive rights afforded to defendants.

If you were to read the Serious Crime Prevention Order that topped off Stephen Day's punishment, however, it would be very clear who ended up feeling constrained. Day is now only allowed one current account, one savings account and one credit card. Enough for most of us, but an unimaginably tedious future to a man used to playing fast and loose with other people's trust, time and money, and who for a while was able to run rings around the investigation: he had set up so many options for himself to move money and facts around, at times it felt like nailing jelly to a wall to prove anything against him. But our collaboration gradually cut off all his escape routes and ended his games.

After Day's sentencing, His Honour Judge Batiste gave a 'commendation plus' - a higher level than the regular commendations given - to Detective Sergeant Stuart Donohue and Financial Investigation Manager Ben Evans (both of GMP) and Mick Meade, a senior investigator for NHSCFA. The entire collaboration of 14 or so people shared in their pride, and a TECAs award nomination seemed to me a fitting recognition for the full cast, particularly given the struggles of the NHS through this pandemic and the importance of ensuring every penny goes to patient care.

We don't give up easily, and we await the outcome of ongoing Proceeds of Crime Act 2002 confiscation proceedings to recover all we can. Again, this involves all the partners working together.

Details of the case

Stephen Day obtained the positions through two employment agencies which were both unaware of his deception.

From November 2012 to January 2013, Day simultaneously held full-time interim Director of Finance or equivalent posts with Merseyside Commissioning Support Unit (CSU); South East Staffordshire and Seisdon Peninsula Clinical Commissioning Group (SESSP CCG); and Cheshire and Wirral Partnership Trust (CWPT). He failed to disclose his employment to all three organisations.

Day worked as a full time Director of Finance for both Merseyside CSU and SESSP CCG between 1st November 2012 and 14th January 2013. This enabled him to fraudulently earn a combined salary of £2000 a day. During this period, in December 2012 he accepted a third simultaneous NHS Director of Finance position, with CWPT. The total loss to the NHS amounted to £88,000.

What started in May 2013 as a locally-led NHS investigation was tasked to the NHSCFA's National Investigation Service in September that year. Its investigators uncovered that Day had spared no effort to maintain the illusion of carrying out his multiple responsibilities. To cover his tracks, he would contact his NHS employers with a range of excuses for his numerous absences - from needing to "work from home", to having to receive "cancer treatment". On one occasion, when he needed to attend an NHS job interview in London, he said that his father had died.

On top of his NHS posts, he had extensive private business interests to run. Day declined to use NHS mobile phones and laptops and was only available through his personal assistant at his private business.

At the start of his employment at CWPT he commenced a two-day handover with the outgoing Director of Finance. Day was still employed at SESSG CCG and, unbeknown to him, the outgoing Director of Finance at CWPT was taking up a new role overseeing all the Directors of Finance in the Staffordshire area including the role at SESSG CCG, which Day occupied.

This was the start of his undoing and it was quickly ascertained that Day had held the position of Director of Finance at Merseyside CSU and Director of Finance at SESSG CCG at the same time for a period of about nine weeks with neither NHS organisation aware of the matter.

During his interview under caution, he tried to defend his criminal actions by saying that it did not stipulate in his contracts that he had to declare other employment.

The NHSCFA was assisted by Greater Manchester Police with the arrest of Stephen Day and subsequent property searches. Greater Manchester Police later launched their own investigation into Day after receiving four separate allegations against Stephen Day which amounted to over £1.3 million in suspected fraudulent activity.

Day pleaded guilty to 12 charges of fraud and theft, including three counts relating to the NHS, but disputed the amounts he had stolen for the Greater Manchester Police investigation. Day was sentenced on all 12 counts, with all sentences to run consecutively, totalling 11 years and 5 months. Day is to serve a minimum of half of the sentence in prison, with the remainder on licence.

Alex Rothwell,
Chief Executive Officer of NHS Counter Fraud Authority

"I am continuing, and ramping up, NHSCFA's close working with the Cabinet Office and other top-level authorities, as well as the panoply of regional and local partners to fight fraud. The Government Counter Fraud Profession's 2021 conference was an inspiring example of what can be achieved when people and organisations are brought together to reflect on their achievements and share their expertise.

I felt proud when NHSCFA's Senior Quality and Compliance Inspector, Tim Barlow, received an honourable mention in the GCFP Awards ceremony at this conference. Tim's job title might sound intimidating but his achievements are all about collaboration, support, giving recognition and boosting morale – not about meting out criticism or focusing on the negatives.

This is the sort of NHSCFA I intend to run. This is the sort of counter fraud effort by the NHS and its partners that the criminals fear most. Of course we spend only a tiny fraction of our energies on entering awards but nobody should underestimate the importance of recognising and celebrating good counter fraud work. Although we did not win a Tacking Economic Crime Award this time, we'll try again next year!"

Confronting the monolith: Fraud and corruption in the Nigerian public sector

The fight against fraud and corruption in the UK has many challenges, but in this article, I set out how things are in Nigeria, where I have been Chief Superintendent Legal (Prosecution), with the Independent Corrupt Practises and Other Related Offences Commission (ICPC), since 2005. My work has involved practising law in fraud and corruption cases in the High Courts through to the Supreme Court of Nigeria, securing convictions and recovering the proceeds of crime in fraud and corruption cases. Corruption is not about dropping a banknote into somebody's pocket, but rather a system of politics and interrelated norms, which are far more complex to control in Nigeria. Corruption permeates the economic, political, and social stratum of society. A Senior Director at the National Salaries Incomes and Wages Commission (NSIWC) explained to me:

"In Nigeria the corrupt have control over power; it is a very big problem. That is why people kill themselves to get into powerful positions; once in there; it gives them economic power, it gives one political power, it gives influence, it gives everything, so on the strength of that, people do everything possible...."

It is useful to distinguish both grand and petty corruption in operation in Nigeria. Grand corruption involves massive government contracts and project financing: it has completely incapacitated the developmental growth of Nigeria because of huge sums of money involved. It penetrates the highest echelons of a central government, resulting in a wide corrosion of public trust in good governance, compliance with public standards and economic development. Grand corruption sets the tone for society and starves public services of the resources necessary.

Petty corruption happens in different ways: small amounts of money exchanging hands (bribes); the granting of small favours by those seeking preferential treatment from public officials; and the employment of relations and cronies in minor public positions. Otherwise known as "administrative" or "bureaucratic" corruption, it refers to a situation where corruption is no longer an isolated case, but rather it has become the rule, not the exception, in all public affairs.

Author:
Dr Musa Bala Zakari,
Chief Superintendant Legal (Prosecution), Independent Corrupt Practices and Other Related Offences Commission (ICPC), Nigeria

For most, petty corruption is necessary to survive and to access basic functions and considered normal by the tone from the top. When Nigerians seek a service from their government, they routinely expect that they will have to navigate corruption at all levels of the bureaucracy. Everything from obtaining birth certificates, registering a company, applying for a passport or renewing a motor vehicle registration all normally require some sort of payment in addition to the official fee. People frequently rely on the aid of intermediaries. In fact, at almost every major bureaucracy that provides essential services, one finds a small number of intermediaries to expedite business.

A consequence is bureaucratic corruption, which normalises corrupt practises into the structures of the state and society. Petty corruption may be more common, as there are more incidents, but grand corruption sets the tone, creating the economic conditions for corruption to flourish and probably amounts to more in terms of monetary impact.

My Doctoral research at the University of Portsmouth focused primarily on grand, rather than petty corruption in Nigeria. I conducted interviews and examined allegations made to the dedicated Nigerian anti-corruption agencies (ACAs) between 2016-19. These showed that the corrupt acts most commonly reported involved embezzlement, abuse of office (including nepotism, favouritism and wide discretionary powers), conflicts of interest/ mismanagement of public resources (including fraud, theft and misappropriation), and procurement fraud. A review of 20 convictions, and the views from the majority of the participants, show that nepotism and procurement fraud are the biggest forms of corruption in the public service in Nigeria. Bribery was not considered relevant, largely because it is under-reported and viewed as "an accepted

Image: Lekki Ikoyi Link Bridge, Lagos, Nigeria by Prince Akachi on Unsplash way of life" to get things done (systemic corruption). Thus, the following forms of corrupt practises are generally widespread in the public service.

Embezzlement, Theft and Fraud

Embezzlement, theft, and fraud all involve stealing of money, property or other valuable items by an individual exploiting his or her position of employment (opportunity). Embezzlement is the stealing of public funds or property by a person who occupies a position of trust or authority: a minister, for instance. Fraud entails the utilisation of deceit or false information to influence the owner of property to part with it freely. For example, as this senior instructor from one of the dedicated anti-corruption agencies remarked: *"Based on where I work, the Economic and Financial Crime Commission (EFCC) has seen public sector corruption come in different forms and types, but generally is in embezzlement of public funds, misappropriation, and money laundering. Now cases decided has shown that this embezzlement and misappropriation are usually also in different guises (characteristics) for instance; it can be what we call over invoicing; that is the person embezzled by over invoicing, contract inflation. We have also had issues with a public servant having companies and using these companies to secure contracts, which is against the Code of Conduct law." (Senior Instructor, EFCC)*

Procurement Fraud

Procurement fraud is common in Nigeria. Research shows that vast sums of money have been lost due to overpriced contracts and non-delivery of purchased products and services. An effective public procurement system is a requisite pointer and evidence of good governance through accountable and efficient deployment of public funds for public good. In one interview, a participant enumerated some of the most rampant forms of procurement fraud that they encountered while carrying out their duties: *"During our review, we discovered many things; like bid rigging, using fake documents during award of contract, conducting, or attempting to conduct occasional fraud directly or indirectly, attempting to influence in any manner of the procurement process to obtain unfair advantage in the contract, and use of altered documents." (Procurement Officer)*

Nepotism and Favouritism

Nepotism and favouritism are rampant in Nigerian society. Such infractions ordinarily entail benefit that is not personal to the official, but rather advancing the interest of those associated to them through consanguinity relationship (blood ties), political interest and, ethnic or religious affiliations (Langseth, 2006). These characteristics of corruption were identified by one interviewee as the most common forms of fraud in the public sector. And, unlike embezzlement, fraud and theft, nepotism, and favouritism do not involve financial consideration: *"…so, beyond money related corrupt practises there are corrupt practises regarding say favouritism in employment where the situation has gotten so bad that virtually every young Nigerian believes that one cannot get a job in the public sector without knowing some big wig. So that is very pervasive, where people cannot get what is due them unless they know somebody [...] that people who do not deserve certain things get these privileges because they know someone… So, nepotism and favouritism is rampant. And one even finds that beyond employment it is found in organisational human resources processes of appointment, training, posting, and welfare issues. One will find corrupt practises creeping into these processes. People within an organisation in such a system will believe unless they have "godfathers", they will not be promoted as and when due, even when they deserve the promotion." (Senior Official, ICPC)*

Extortion and Bribery

Bribery is the offer or exchange of money, services, or other valuables to influence the judgement or conduct of a person in a position of entrusted power. The advantage does not have to be directly for the public official at issue - it can be for their spouse, children, relatives, associates or even the official political interest, such as a donation to his political party.

Extortion depends on compulsion to influence compromise, such as threats of violence or the disclosure of sensitive information. Like other types of corrupt practises, the victim can be the individuals adversely affected by a corrupt conduct, the public interest, or both, exemplified in this case: *"A deputy Superintendent of police of the Nigerian Police Force (DSP), in charge of homicide section attached to the office of the Assistant Inspector General of Police (AIG), in Benin, Edo state, was sentenced to 7 years imprisonment with hard labour in January 2012. For demanding the sum of N 1,000,000 (One million naira), from a (Suspect), in return for writing a favourable report about them as part of the investigation. The person against whom criminal complaints were made, and on account of the said criminal complaints being investigated as an inducement to write, secure, procure and confer a favourable report of the suspect in respect of the criminal complaints." (Typewritten Judgement of the High Court-B/ICPC/2/06)*

Conclusion

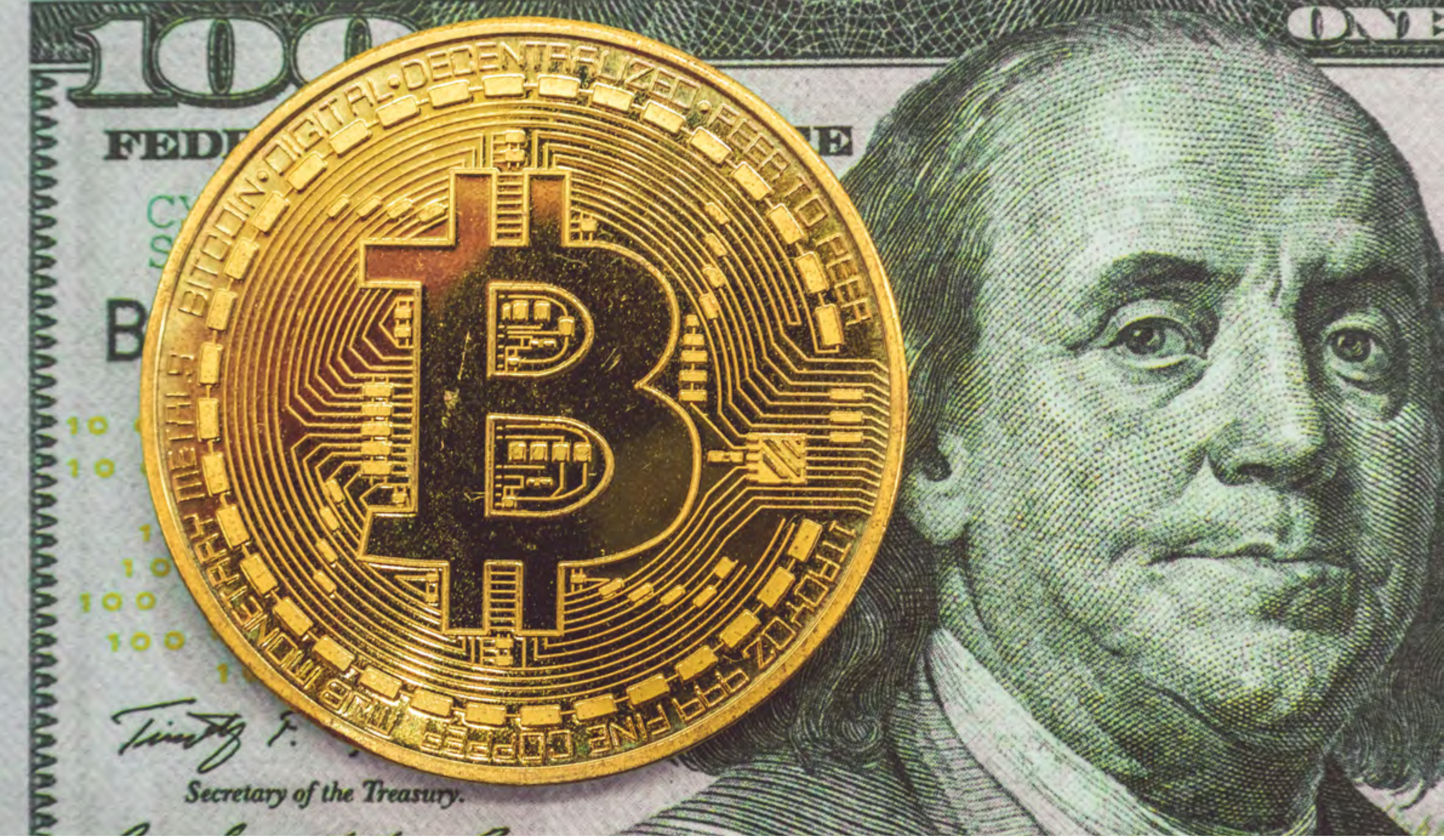
The findings from this research illustrate the endemic status of corruption in Nigeria. All are faced with bureaucratic structures that can only be negotiated by the petty corruption of paying bribes to secure basic services. Where a person's status in society is higher this leads to increased opportunities for grand corruption, where the techniques shift to embezzlement, theft and fraud (particularly in procurement), nepotism and favouritism, as well as bribery and extortion.

The dominance of the public sector in Nigeria and the reliance of the private sector on contracts awarded by the public sector leads to the private sector being similarly cloaked in corruption. They can only thrive on illicit capital flowing from the public purse and must engage in the corrupt schemes to survive.

There is clearly evidence that senior officials involved in the fight against corruption understand the problem, know what needs to be done and have an appetite to do so. However, when everyone is swimming in a pool of corruption, draining it is not a practical solution. Tackling it requires extensive reforms to address this, with commitment from leaders from the President down and a change to the culture of Nigeria.

This paper draws on the research Musa completed for his PhD at the University of Portsmouth and the following article Zakari, M. B., & Button, M. (2021). Confronting the Monolith: Insider Accounts of the Nature and Techniques of Corruption in Nigeria. Journal of White Collar and Corporate Crime, 2631309X211004567.

References and notes for all articles are now on page 31



Money Mules: Some insights into vulnerabilities and networks

Author:
Dr Michael Levi,
Professor of Criminology, Cardiff University

‘Money mules’ is a phrase that has caught the media, the financial services sector and perhaps the public imagination, in the UK and elsewhere in the world. Mules are people (and also - conceptually - business entities) recruited as conduits for proceeds of crime with the intention of defeating anti-money laundering (AML) and anti-fraud controls. The term makes sense as a metaphor for people carrying sacks of money on their backs: occasional customs or police interceptions of travellers with suitcases containing over $1 million in cash would be the modern form.[1] Cryptocurrency and e-banking worlds have mitigated that particular problem of portability and confiscation risk (once cash has been transformed into them), though most countries outside the UK have no customs confiscation powers if cash is declared on exit and entry.[2]

Depending on where they live and where they want the money to end up, major criminals (including tax and exchange control evaders) have always moved some proceeds of crime. Disguise of proceeds of crime outflows might take place to defeat criminal investigations or civil creditors (or in some countries, extortionist public officials or competitor criminals), but this could be achieved via transfers to high secrecy, beneficially owned companies, or trusts, which are still available in a diminishing number of jurisdictions, including the USA. Beyond that, the need or demand for money mules is an artefact of the controls we have placed on money movement via our AML efforts. Before the UK, US and others began to criminalise money laundering in the 1980s, there was no need for crime entrepreneurs to parcel funds up into sections to make them less suspicious because normally, no-one in an intermediary position in financial services cared or had any legal duty to identify customers or report suspicions. The more business-like the crimes and the organisational context, the easier

Photo by Bermix Studio on Unsplash

transfers out become. There is also the growing, but still not dominant, use of cryptocurrencies (led by Bitcoin) for drugs and human trafficking, constrained by their usability in everyday life and ease of access by counterparties. (Though some cryptocurrencies are becoming normalised, accelerated by recommendations from paid Instagram influencers to buy crypto: in addition to value volatility, a massive fraud problem in the making when some exchange owners disappear with the loot.)

A focus on money mules is understandably a significant part of the contemporary AML control focus. If we could stop proceeds of crime being dispersed in smaller tranches through unsuspected people, the internal bank processes and paradigms of criminal exfiltration would work better and make it easier to identify (and perhaps stop) those criminals that use the muling mechanisms. If there was no risk of formal counteraction – whether freezing assets or criminal justice measures – paying money mules would be a needless expenditure for fraudsters and traffickers. There are also unanticipated impacts on the lives of those who allow their bank accounts to be 'borrowed' by proceeds of crime, articulately highlighted by Cifas and other industry bodies on radio, TV and press outlets. These include the (actually rare) risk of gaining criminal records for money laundering; and denial of future banking and other financial services facilities such as mortgages through Cifas markers put on suspected money mules. We may presume that these consequences are not widely anticipated by either knowing or naïve money mules.

Money muling is a criminal service, and each account has a limited life span before it can no longer be useful. Except where there is a convincing business front, the larger the amounts involved in fraud (or corruption), the more mules may be needed, and therefore intermediaries with access to ready mules can command a premium. In addition to offenders' beliefs about risks, there are also real risks of being picked up and acted against, and the consequences of detection by private and public actors. We need to appreciate the meaning of those risks to different populations.

Money mules are part of fraud as well as of 'pure' money laundering schemes, and this may be connected with the hybridisation of street and cybercrime gangs, in the Netherlands and the UK.[3] Some Dutch mules engage in crimes beyond phishing scams. During a police interrogation, one mule declared that she was asked to change counterfeit 100 Euro bills by buying cheap goods at different locations and collecting the change as 'laundered' cash.

Crimes vary in their need for money muling assistance. For most crimes for gain, there is no need for money muling or indeed any laundering services, since the proceeds are immediately consumed in subsistence or leisure activities rather than being saved or distributed. For others, including some Missing Trader Intra-Community (MTIC) frauds, trade based money laundering and false invoicing techniques predate muling and obviate the need for it. Some 'mule herders' offer their services on internet forums, but contacts between core group members and herders can also be established within offline social networks or offline criminal meeting places. Though internal monitoring makes this risky for them, financial services employees may provide data about "interesting" bank accounts or even increased withdrawal and credit limits, which means reduced numbers of money mules are required to move money originating from phishing attacks.

Mules are important in both offline and online crime. Apart from receiving illegal money, money mules help core members avoid being incriminated and/or being financially imperilled by 'follow the money' investigations,[4] especially those conducted long after the fact, as is the norm with over-pressed investigators in the UK and elsewhere in the world.

Recruiting Money Mules

Launderers typically recruit money mules in two ways: as unwitting accomplices or as willing and knowing accomplices. Social engineering of unwitting mule activities may include inter alia, serving as an intermediary, or transferring money under the guise of an ostensibly benevolent act, such as supporting someone in need overseas, with the mules keeping little or nothing for themselves.[5] In other cases, they may think they are doing a legitimate job, advertised as a work-from-home scheme,[6] also popular during Covid times, when those seeking work via LinkedIn may be targeted.

Complicit mules engage in similar behaviours, but knowing their behaviour is illicit. For instance, they may use their own accounts to conduct wire transfers and keep a fee; use stolen identities to create new accounts from which they can transfer money or access compromised accounts with stolen credentials; collect money from a jackpotted ATM or crypto asset ATM and deliver or deposit those funds to a secure point accessible to the fraudsters with whom they are colluding.

In a recent Dutch study, potential money mules were recruited using the chat function on mobile phones with messages inquiring about people who were interested in making money or more specific questions like 'What kind of [bank] card do you have?' or asking about the colours 'orange' or 'green'—a reference to the colours of the ATM cards from popular banks in the Netherlands. In these messages, money mules were promised large sums of money, sometimes 5,000 or 10,000 Euros or a 30 to 35 per cent cut of all profits if they handed over their ATM cards. The recruitment of money mules also occurred offline. Young people were approached not only at school or at a gym by friends or acquaintances, but also by strangers whilst hanging out on the streets of their local neighbourhoods. Presumably to reduce risks from police and to encourage take-up, only after being approached in person and contact information was exchanged were potential mules contacted through digital messenger services. Offline interactions and encounters remain important even in a 'technological' environment.[7] This pattern is also plausible for the UK, though Cifas reports note the changes in age groups suspected of money muling, by no means just the young. Criminals might be expected to target different age ranges to avoid the banks' money laundering risk models.

In 2019, new asset freezing order powers were used by the UK authorities to clamp down on Chinese accounts used as

Photo by Art Rachen on Unsplash

a conduit for allegedly illicit funds, a concern also expressed in the US and Australia. The extent to which such funds related to cybercrime, organised crime, corruption or simply circumventing Chinese exchange control rules is unknown, either to researchers or to the National Crime Agency (NCA).[8] Almost by definition, the resources exist only to analyse a limited proportion of mules. Launderers often recruit several money mules and have them transact among themselves. Though Western Union and MoneyGram have their own sophisticated data tracking, mules may also transfer funds via other Money Service Bureaus, sometimes disrupting the follow-the-money chain. This strategy makes the money mule a cut-out, a person who becomes the low-hanging fruit that law enforcement arrests when investigations are successful, but who is unable to further identify the 'core' money launderer or the predicate offender(s).[9]

Combating money muling

For reasons of space, I have focused on money muling in the UK and the Netherlands[10], but this is a universal issue, as noted in Europol, US and Australian 'Actions'. The private sector monitoring firms – such as Vocalink's Mule Insights Tactical Solution, plus LexisNexis, BAE Systems et cetera – have extensive systems for identifying patterns of suspected muling and linking Internet Protocol [IP] addresses and other data. But as with all systems, one of the problems is to optimise/minimise false positives and false negatives and to act quickly before the money is gone. All of the banks have their own internal investigative staff for money muling, but technological 'pre-sorting' is vital.

Another area of action is in the Prevent[11] mode, with warning advertising aimed variously at students and any demographic group whose numbers have been rising. In 2021, an Economic and Social Research Council (ESRC) supported initiative 'We Fight Fraud' has developed a lively film, 'Crooks on Campus', accompanied by 'roadshows' on campuses, in an attempt to make students more aware of the harms and the risks to them. Foreign students may be a high risk-taking group, especially as they near the end of their studies and might assume that no harm to them will come from lending their accounts to others. It is commonly held that ethnic groups may be targeted by a combination of pressure, assumptions of harmlessness, and distance from pro-conformist norms, but relaxed attitudes may be more widespread among Generation Z. Evidence of impacts of this warning outreach is not yet available, beyond substantial signups to become, for example, mule marshals, by people who may not have been vulnerable to temptation anyway. Cifas and UK Finance have been engaged in both information sharing efforts within the sector and outreach publicity, but there is not yet any public evaluation of these efforts on money muling.[12] In the past three years, Lloyds Bank alone has blocked £60 million from 88,000 accounts over suspected money muling and other banks have been very active also: but though important, this is a modest proportion of fraud, let alone proceeds of crime generally. We could learn something from those who turn down money muling offers.

There was a predictable political backlash from the Chinese authorities when NCA analysis showed the role of Chinese students in UK money muling. It is an open question: what impact does education about the harms of money muling and the risks of getting a negative credit score and imprisonment have on Generation Z people? They may have few prospects of home ownership anyway and overseas students may not be impacted by UK credit scoring if and when they return home. Money mule recruitment may now be more important since the Confirmation of Payee in online bank transactions has made it harder to scam people using account names that differ from the person/firm they thought they were paying. We will continue to need a range of approaches to attack different segments of the money muling market, and mitigating this problem requires strong cooperation between private, third sector and policing bodies, including targeted warnings and prosecutions for mules, and enhanced communication strategies to increase perceptions of riskiness. Long delayed reforms at Companies House would help to reduce the use of misleading business fronts as corporate mules. We also need more rapid freezing of suspect accounts because once the money has gone, it is a lot harder and more expensive to get it back.

Professor Levi is grateful to the UK Economic and Social Research Council (ESRC) Partnership for Conflict, Crime and Security Research (ES/S008853/1) for funding the underlying research.

References and notes for all articles are now on page 31

Compliance's Knowledge Problem

In 2009, a 23-year-old research assistant in a chemistry laboratory at the University of California at Los Angeles (UCLA) died from burns she sustained when she accidentally mixed two substances and ignited a fire. In the aftermath, the University of California entered into a settlement agreement. The agreement sought to impose terms on the university system to help prevent similar accidents. One of the terms in the settlement was that lab personnel had to be well-informed about dangerous substances. So, the university developed its own organisational rules complete with individual protocols for approximately 200 dangerous substances. Each of these 200 individual protocols were about 20 pages long. Health and safety compliance managers were tasked with ensuring that all faculty, lab assistants, and students entering these labs signed these protocols. That meant that each individual had to sign about 4,000 pages of safety protocols in order to be allowed to do their job.

Authors:
Benjamin van Rooij
Professor of Law and Society, University of Amsterdam, School of Law, and Global Professor of Law University of California, Irvine School of Law and ***Adam Fine****, Assistant Professor of Criminology and Criminal Justice and Law and Behavioural Sciences, Arizona State University*

By introducing these protocols, the University of California developed a massive compliance management system. It did so to ensure that its employees would abide by new safety protocols developed in the wake of the tragic, lethal accident. In doing this, the university provides a good example of how entities respond to compliance problems and liabilities. In the wake of major accidents, scandals, or other major damaging events, public and private organisations typically respond by developing and introducing new rules, and sometimes, new procedures and institutions to implement these changes, often with another set of rules, and sometimes with another layer of implementation actors and protocols. Employees therefore face mounting burdens with new organisational obligations to comply with, potentially hours of training, and additional oversight that impact their everyday activities.

The question therefore is whether the rapid ballooning of rules and implementation practices actually deliver on the promise of keeping us safe from harm or do anything that actually may prevent error or wrongdoing. To answer this question, we must examine why we would expect these systems to impact human behaviour. Let's take the University of California as an example. With the new rules on laboratory safety, everyone entering a laboratory on one of the University's nine large campuses should have read and signed the approximately 4,000 pages of safety protocols. On average, a person reads about 40 pages per hour, so to truly read this text would take 100 hours, a little over four days of full-time reading. And most likely, because these protocols are detailed, reading would likely be slower than average. Let's assume everyone – from student assistants to senior professors – did read every page. Even if they had read the full text, the next question is how much would they be able to remember in the long run. Scientific research has shown that human memory suffers from a so-called forgetting curve, where most newly acquired information gets lost in a matter of weeks, if not days, after it is first acquired, unless the information is reviewed. And in this case, when the sheer amount of information to be studied and remembered is so vast, the chances even of short-term retention, will likely be far lower. Being confronted with this massive volume of safety protocols may even have a negative effect where students, staff, and professors simply become overwhelmed and less receptive to the information about how to handle dangerous substances.

As such, we can seriously question whether having all the people who enter these laboratories read and sign the safety protocols would in fact prevent accidents. From a behavioural point of view, this approach does not make sense.

A different logic seems to have been at play here. Maybe the adopted measures do not truly serve to change future conduct, but instead their logic is about averting legal liability. By having all staff and students who run the risk of being involved in an accident sign these protocols, the university has done what it promised to do under the settlement. And as such, it has delivered on the output; a compliance system. In case an accident does occur, then the

Image: Lysander Yuen on Unsplash

university will face less liability because it did not breach its core responsibility. Even worse, it could argue that the individual staff or student has a higher liability as they were fully informed of all existing dangers. After all, they signed 4,000 pages worth of safety protocol.

This example illustrates some of the core issues on how organisations approach compliance and compliance management. Of course, the example here is extreme in the amount of rules staff and students are supposed to learn, but compliance in any organisation will likely face a similar issue: compliance's knowledge problem. Most organisations will have dozens, if not hundreds or thousands of pages of rules across different regulatory domains that its employees are supposed to know. And knowledge of such rules will likely be extremely limited. In fact, empirical studies generally find that knowledge of the law – whether it is lay people's knowledge of basic rules such as criminal law or family law, or specialised knowledge amongst doctors or school administrators – is shockingly low. Yet organisations continue to grow the bodies of rules that employees must know. They add additional complexity when the people are struggling even with the basics.

Organisations will naturally set policies and procedures that seek to govern the conduct of their staff, for example defining the rules for when expenses can be claimed and setting out the amounts allowable, alongside a clear statement of the possible consequences of transgression. But, in seeking to cover every eventuality, such as the amounts that can be claimed when abroad or for extended periods, such policies can quickly grow in size, become difficult to understand or navigate. When the amounts allowed or updated, or eligibility rules change, there is the risk that the changes will go unnoticed by those affected, increasing the risk for errors or non-compliance.

There are two competing logics here. One is a behavioural logic that focuses on prevention. We call it the ex-ante (Latin, meaning: 'before the event') approach to compliance. Under such logic, the purpose is to reduce harm, and compliance approaches only work if they reduce harmful behaviour in the future. This approach centres on effectiveness, and it focuses on outcomes and impact. Therefore, the increasing burden of compliance is justified if it can truly prevent risks. In the United States, the Foreign Corrupt Practices Act (FCPA) rules and regulations are worthy, if they reduce corruption and bribery. Occupational health and safety compliance systems make sense if they prevent accidents and save lives. And anti-money laundering codes and practices should exist if they truly reduce tax evasion, organised crime, and terrorism.

Second is the legal logic that focuses on liability. We call this the ex-post approach, as it concentrates on reducing or limiting the liabilities once a case of misconduct or an accident occurs. All too often, systems that are allegedly designed to reduce harm end up functioning in an ex-post manner that reduce liability rather than actually change behaviour.

To truly follow a behavioural, ex-ante perspective requires a different type of thinking. It necessitates thinking from the perspective of the people whose behaviour the system tries to change. Let's continue with the Californian laboratory example. If the system designed to prevent accidents in the lab includes a safety training component, the first thing we have to ask is how much time do participants actually have to willingly partake in training on an annual basis? Also, we must understand what the best review frequency is for participants to retain what they learn. Based on that, we can calculate our time budget for both the first-time knowledge transfer and the review sessions. Once we have that, we have to establish what the best manner of knowledge transfer is. Most likely, we will see that pure passive reading is not optimum, so we would need to have some interactive component which would be more time-consuming than just reading. Once we have established this, we can then determine how much content we can introduce in the training and review sessions. We would inevitably find that the amount of space for content would only include a small fraction of the total content of the original 4,000 pages. So, the next step is to prioritise information. Here, we must focus on three practical questions: What are the biggest risks? Which risks originate in a lack of knowledge? And which can be corrected by providing information during training within the available time? Based on this, choices can be made about what information to focus on and a training module can be developed and tested to best transfer the most important knowledge that may actually reduce risk. Returning to the example of an expenses policy, we can seek to use the same principles. Firstly, by understanding that in most cases, an employee's only need for an expense claim will be to occasionally make a simple claim related to a short trip. What do they actually need to know in order to do this? How can the policy be layered so that this essential information is readily available and comprehensible and not lost amongst the complex rules relating to the most unusual claims? Or do we even need to include the complex rules at all? One notable example is Netflix's policy for travel, entertainment, gifts, and other expenses which comprises five words: "act in Netflix's best interest".[13]

If people are both motivated to comply and in a situation where they can comply, then they are very likely to comply. And vice versa - when people are motivated to break rules and are placed in a situation where they can make that choice, they are very likely to violate the rules. We explore this in detail in our 2021 book "The Behavioural Code".

Following a behavioural approach to compliance takes courage and intentional design. It requires that the organisation prioritises prevention over liability. It also means that organisations must learn to gather empirical data about what processes and mechanisms best improve organisational conduct. But for them to do so also requires that regulators follow suit. To truly deliver on safety and prevent harm, regulators must begin supporting organisations that truly try and understand how they can best shape behaviour in their organisation, instead of simply holding them accountable for failing to deliver on paper-level outputs that either do little or even harm the outcomes and impact we all so desire.

References and notes for all articles are now on page 31

We may have got there at last: Reflections on 30 years of fighting fraud

Author:
Duncan Warmington MSc, BSc (HON), GCFS

At the end of March 2022, I shall retire as a Counter Fraud Specialist after 30 years. It has been a very fulfilling and enjoyable career that has changed significantly over the years.

In the early 1980s, central government split the rent allowance element away from the Department for Health and Social Security and created Housing Benefit, which was to be administered by local authorities. This was a canny move on the part of the Thatcher government as five per cent of housing benefit was to be met by local taxation rather than all of it being paid for by central government.

Increasingly, fraud was becoming a concern for the (now) Department for Social Security. As such, they started to bolster counter fraud measures, including increasing the number of fraud investigators. It was not long before the Department turned its concern to fraud within Housing Benefit and Council Tax Benefit. However, local authorities as a whole, were not willing to meet the costs of counter fraud work out of their own budgets. After all, central government funded ninety-five per cent of the local authority administered benefit and as such were suffering the biggest losses.

Subsequently, a payment-by-results scheme was offered to local authorities called Weekly Benefit Savings (WBS). WBS was already well established in the Department for Social Security as a means of measuring their investigative and compliance work. WBS was the amount of benefit stopped multiplied by 32 (32 'allegedly' being the number of weeks, on average, benefit would have continued if it had not been stopped). In simple terms, each local authority was given a WBS target, depending on the amount and number of claims. All WBS over the target could be claimed as a payment for their counter fraud work.

As with all things new there was some reluctance by most, but also some early adopters. One of these was Portsmouth City Council and a film was made about the council promoting the huge amounts of money councils could make if they joined the WBS scheme. This prompted many councils to sign up.

It was at this point that I joined Tonbridge and Malling Borough Council on a short-term six-month contract. My background had been in the army, followed by working for a private company, which included investigating the theft of money and goods. But I knew nothing about benefits. However, I was not alone. This new force of council investigators was made up of people from a variety of backgrounds: council benefit staff; retired police officers; some from the private sector and the odd ex-civil servant.

Image: Prospect Cottage, Dungeness, Kent by Zoltan Tasi on Unsplash

None of us really had a full grasp of what we were supposed to be doing.

In Kent, the investigators decided to meet to share thoughts. That first meeting, held at Maidstone Borough Council, demonstrated that confusion was rife. There was a varied range of investigative methods that were being employed; most worryingly being the diversity of evidence that could get someone's benefit stopped. There was not even agreement on what WBS could or could not be claimed. One might say, it was proper 'wild west'.
As well as meetings taking place in Kent, other meetings were taking place across the country. These meetings eventually led to the setting up of the Local Authority Investigating Officers Group (LAIOG). From LAIOG's inception it was clear that the investigating officers needed three things: training; continuing support; and professional recognition.

In terms of training, help was to come from the Benefits Agency. With the formation of the Benefits Agency, following the merger of the Department for Social Security and the Unemployment Benefit Office, there was the realisation that investigators needed training to meet new professional obligations and standards. In particular, the moving from simply stopping the benefit of fraudsters to the sanction and prosecution of offenders. Ultimately, this training would lead to the creation of the Accredited Counter Fraud Specialist (ACFS) qualification.
I was fortunate enough to be one of the first local authority investigators to be included in this training. This ACFS training programme actually made it into the newspapers because the surveillance element (sadly no longer a part of the basic training) was run by ex-SAS instructors. Being a former soldier, I did think this was a little melodramatic; particularly, as when I turned up for the training, I knew one of the instructors.

The basic ACFS training has always been a good foundation-base for new investigators; this was particularly so when the University of Portsmouth provided the administrative support for an independent oversight board for ACFS training, called the Counter Fraud Professional Accreditation Board.

Once ACFS qualified, I went on to take the ACFS (Manager's) qualification. At this point in my life my children were growing up fast, with all three of them likely to go to university. My wife had a degree, but to say I left school with fewer than a handful of qualifications would be to overstate my academic achievements. I was determined not to be the only one in my family not to have a degree.
It is with my sincerest gratitude that the University of Portsmouth established a distance learning Bachelor of Science degree in counter fraud and criminal justice studies. This was linked to the completion of the ACFS training, with those who had passed ACFS receiving academic credits and having the option to further their studies. It was a wonderful learning and social experience. All of us were mature students drawn from a range of organisations including the Benefits Agency, local government, and the police. Once a year at 'Study School' we could pretend to be proper students.

Once I graduated with a BSc (Hon), I went on to take my master's degree in counter fraud and counter corruption, again at Portsmouth. I would wholeheartedly encourage counter fraud specialists to gain academic qualifications. It is my personal view that the profession needs the academic skills and mindset to think and work at a strategic level. Indeed, going forward counter fraud specialists need to be central in combating fraud at a strategic, tactical, and operational level.

The work of counter fraud specialists was and is changing. For example, data analytics was unheard of when I first started. Also, the types of fraud, its complexity and severity have changed dramatically. It is therefore essential that training and qualifications, such as ACFS, continue to evolve in the same way.

For local authority counter fraud specialists, LAIOG was always there. With its annual conference, local groups and personal networks, local authority counter fraud specialists were well supported and became a force to be reckoned with.

Local government counter fraud specialists enjoyed a professional freedom perhaps not experienced by some of their colleagues elsewhere in the public sector. This allowed for local authority counter fraud specialists to use their knowledge and experience to work in innovative and focussed ways. Such as, in developing policy to meet local need, 'grass roots' development of IT provided by the private sector, and creating organisational and officer-to-officer partnership working with other councils and bodies.

One area that still needs to be addressed for counter fraud specialists are the powers available to them to carry out their duties. For example, benefit investigators in DWP and tenancy fraud investigators at local authorities have substantial powers, allowing them to demand information from employers and financial institutions. However, these powers are not available to counter fraud specialists investigating other fraud types; such as, social care fraud or procurement fraud. This is despite the fact that the monetary value in social care can be significantly greater than either benefit or tenancy fraud and procurement is one of the largest fraud risks. Would it not be great if one day powers were invested in the 'licenced counter fraud specialist', not unlike constable powers in the police?

For me, with my BSc and MSc, I was fortunate enough to get a job with the Audit Commission's newly re-formed Counter Fraud Team. The Audit Commission had the statutory power to require local authorities to report on their counter fraud work, which we used to research and write an annual report called 'Protecting the Public Purse' (PPP). PPP would become the definitive report on counter fraud in local government. The annual survey gathered details of all detected frauds; from which we were able to determine trends and produce comparative data. Areas of best practice were showcased, for example, the excellent work some councils were undertaking into housing tenancy fraud. Their work, and PPP, managed to bring into being the 'Prevention of Social Housing Fraud Act 2013'; making tenancy fraud a criminal offence.[14]

Although I take no personal credit, as it was a team effort, it is a sense of pride that many, if not most, local authority counter fraud teams today would not be in existence if it were not for PPP. As explained earlier, most local authorities first started to invest in counter fraud due to the funds available to them to deal with fraud in the benefits schemes that they administered. Local authorities are, by their nature, independent of one another; it would have been easy for them to work in isolation. But PPP showed the other types of fraud that local authorities fell victim to and highlighted where some authorities had moved their fraud teams into other areas of work. By the time the Department for Work and Pensions (DWP) took back responsibility for benefit fraud investigations from local authorities in 2015 PPP noted a marked increase in the number of local authorities that were now detecting non-benefit fraud too.[15] PPP's impact had, in my view, been influential in many local authorities seeing the need to continue investing in counter fraud work even after they were no longer responsible for benefit fraud cases.

As we are aware, fraud is difficult to measure, with the estimated fraud cost to Government between £29.3bn-£52bn.[16] Even the Audit Commission's annual fraud survey only measured detected fraud and the National Fraud Authority's fraud measurement report, although by far the best we had at the time, was only a calculated guesstimate.[17]

Research suggests that the culture of an organisation is the best way to prevent fraud.[18] The stronger the counter fraud culture, the less likely the loss to fraud and the weaker the culture, the more susceptible the organisation is to fraud. So, one area of work I was greatly involved in at the Audit Commission was building counter fraud culture within organisations. Although we could not determine the true amount lost to fraud, if we could measure an organisation's counter fraud culture we could ascertain its likelihood, or not, of effectively tackling fraud.

To measure that culture, we used staff surveys to find out how 'switched-on' staff in local authorities were to combating fraud. Interestingly, often senior staff would think their organisation was wonderful, but the experience of 'hands-on' staff in the same organisation was very different. We used the data obtained from these surveys to produce comparative data across a range of bodies e.g. council to council, department to department, or pay grade to pay grade.

We then ran counter fraud workshops. These were in part fraud awareness training, but in significantly more depth. However, they were not simply training sessions, but workshops that were intended to be fun, interactive, and engaging. The workshops sought to draw out from attendees where the counter fraud strengths and weaknesses lay in their authority. The workshops were multi-grade, with participants from the very top of the organisation, including elected members, to the 'shop floor'. All engaging, all listening to each other, and all building a common understanding and culture.
Finally, we would put all this together in a report, covering what had been learnt from the survey and workshops, and present it to the very top of the department and organisation. For the 'Tone is set from the Top' and the top needed to hear and act on what their staff were telling them.

Sadly, when the Audit Commission was abolished both PPP and the Commission's counter fraud culture work ended with it. Some may say, 'the baby was thrown out with the bath water'. Thankfully, for me, on leaving the Audit Commission, I joined Kent County Council (KCC) where I was able to continue with the development of 'Changing Fraud Cultures' (CFC). KCC Counter Fraud Team are building their council-wide CFC programme. The programme is also used by other local authorities, such as Kent Fire and Rescue Service and KCC's Local Authority Trading Companies (LATCo's). The amount of survey data is increasing allowing for better comparative data and analysis. Both the workshops and reports are being very well received. Of significant importance, senior managers are sitting up and taking note and action.

I am grateful for the GCFP award I was given for this counter fraud culture work. I encourage all reading this to consider how they might improve their organisation's counter fraud culture. I am sure KCC and GCFP would be happy to speak with you.

Although LAIOG provided an excellent service to local authority counter fraud specialists, the one area it could not make headway with was building a profession. Over the years there have been many attempts to build a profession, but all have failed for one reason or another. One reason was the inability to get the civil service onboard. Without doubt the civil service has the largest amount of counter fraud specialists, albeit that they are spread over a multitude of differing departments and agencies each with their own agendas.

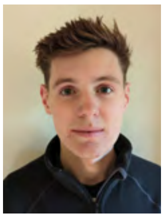
Thirty years after sitting in that meeting room discussing 'what the heck' are we supposed to be doing, we finally have a Government Counter Fraud Profession. As I retire, I cannot begin to tell you how pleased I am. Most probably new people into the profession will no doubt take it all for granted; hopefully they will. But for us old timers, we will appreciate the immense amount of work and effort it has taken Mark Cheeseman, the Cabinet Office staff and all numerous advisors and secondees to bring this about.
It has been my professional dream that counter fraud specialists can have a full and varied career across numerous organisations. For example, start as a counter fraud apprentice in a local authority, move to DWP counter fraud, spend time in the private sector, then back to local government or HMRC, and finish their career as a senior manager in the Serious Fraud Office.

There is still a long way to go; but, with common professional standards and recognition, now there is a chance, just a chance, that this may be possible one day.

References and notes for all articles are now on page 31

COVID Pass fraud

Author:
Will Baker,
Research and Policy Officer, Counter Fraud Centre of Expertise, Cabinet Office



The COVID-19 pandemic has impacted everyone across the globe and led to unprecedented challenges. Her Majesty's Government (HMG) has reacted at pace to support the most vulnerable and deliver essential services, but criminals were quick to adapt their practises to take advantage of the health crisis and target the public increasingly through cyber-enabled means. Criminals have deployed fraud tactics online, through text messaging, email, phone and social media, using COVID-19 and government branding as a hook to steal money, financial details and personal information.[19] To respond to the threat, the Government Counter Fraud Function (GCFF) has continually monitored fraud and engaged with partners to raise awareness of fraud and reduce the harm caused.

Prior to the pandemic, criminals continually targeted the public through text messaging (smishing), email (phishing) and phone (vishing) fraud. Criminals used fake messages as 'bait' to trick members of the public into clicking links to websites which contained malware, or led the victim to submit money, financial details or personal information. This led to direct financial loss to the victim, or resulted in wider fraud and criminality where information was sold across criminal networks to facilitate offences such as banking or identity fraud.

During the pandemic, cybercrime increased exponentially. Which? analysis of Action Fraud data indicates an 83% increase in phone fraud (smishing and vishing from unknown numbers) between April 2020 and March 2021.[20] Moreover, in October 2021, Ofcom research revealed that 'almost 45 million people have been on the receiving end of potential scam texts or calls in the last three months'.[21] A driving factor is criminals using government branding, schemes and policies to trick members of the public, sending fraudulent messaging relating to COVID-19 testing, vaccines and stimulus schemes. Moreover, criminals have used technology to spoof genuine messaging from public service sites, such as Test and Trace, as well as social media to enable fraudulent activities. These tactics are targeted at everyone, but can have the biggest effect on the vulnerable and elderly.

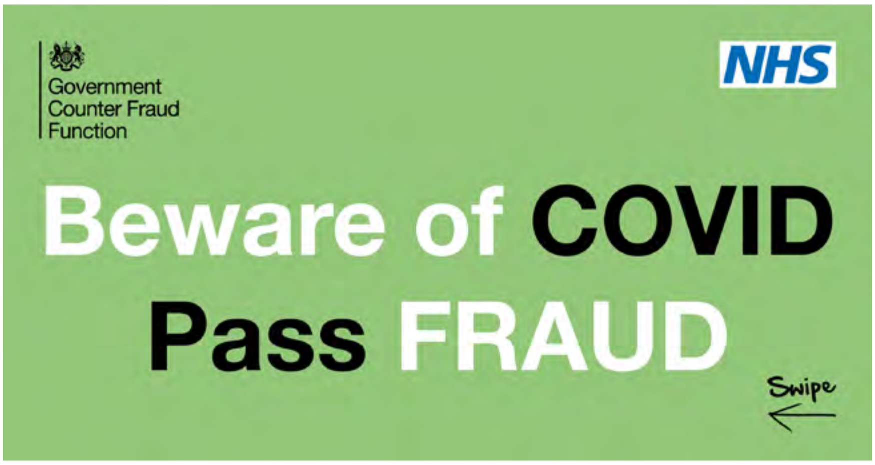
Criminals have continuously adapted their tactics to target the public. At the start of 2020, criminals focused on the vaccination programme to send fake messaging, under the masquerade of being from the NHS, relating to the vaccine and appointments. After the announcement of the NHS COVID Pass to display coronavirus (COVID-19) vaccination details or test results (COVID-19 status), for use to travel abroad or at events and venues in England to prove COVID-19 status[22], fraud has evolved to focus on the NHS COVID Pass. In addition to smishing, phishing and vishing, criminals have offered fake vaccine certificates for sale online and on social media to steal money and personal information.

Issue

The GCFF COVID-19 Intelligence Team (Intel Team) was set up in early 2020 to gather intelligence from across the public and private sector and develop a strategic overview of the threat of fraud against HMG. The Intel Team oversees flows of information from the public, law enforcement, government departments and international forums, which help the GCFF to understand the evolving threat of fraud and collaborate with partners to respond. Organisations including the National Cyber Security Centre (NCSC), Department of Health and Social Care (DHSC) and City of London Police (CoLP) detected a significant increase in fraud reporting relating to the NHS COVID Pass and vaccine certification. Fraud reporting included financial loss to the victim and use of government branding to trick members of the public.

The Campaign

In August 2021, the Intel Team engaged with cross-sector partners, including NSCS, DHSC, CoLP and NHSX[23], to plan and develop a public communications campaign similar to the 'Be Alert to Vaccine Fraud' campaign, launched in January 2021.[24] The purpose of this campaign was to raise awareness of NHS COVID Pass fraud, to provide guidance

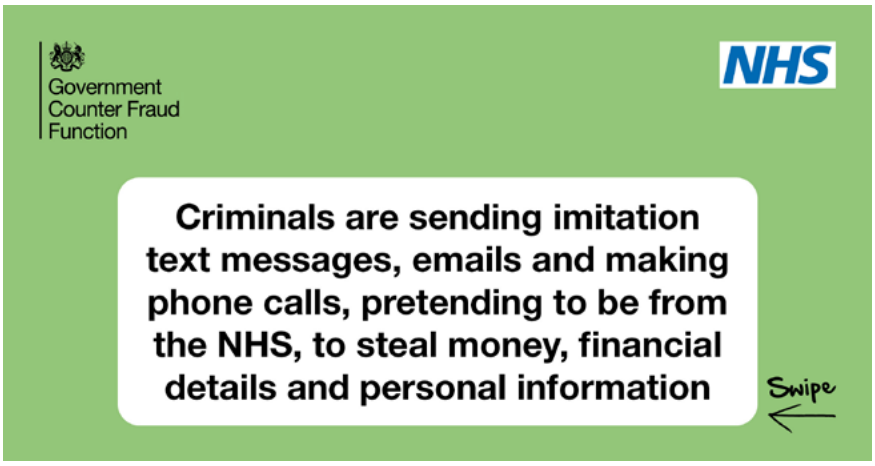


Government
Counter Fraud
Function

NHS

Beware of COVID Pass FRAUD

Swipe ←

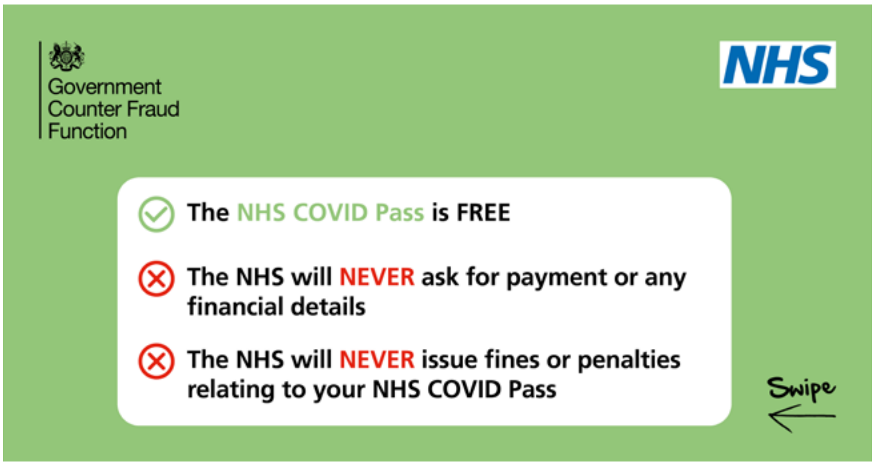


Government
Counter Fraud
Function

NHS

Criminals are sending imitation text messages, emails and making phone calls, pretending to be from the NHS, to steal money, financial details and personal information

Swipe ←

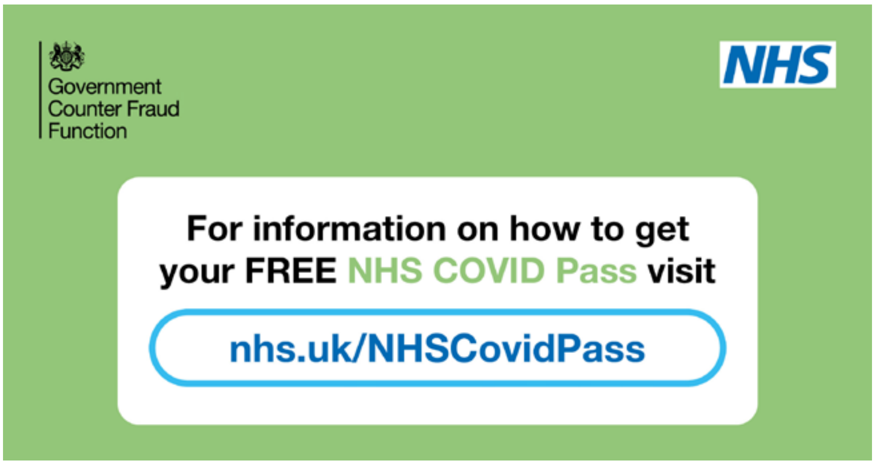


Government
Counter Fraud
Function

NHS

- ✓ **The NHS COVID Pass is FREE**
- ⊗ **The NHS will NEVER ask for payment or any financial details**
- ⊗ **The NHS will NEVER issue fines or penalties relating to your NHS COVID Pass**

Swipe ←



Government
Counter Fraud
Function

NHS

For information on how to get your FREE NHS COVID Pass visit

nhs.uk/NHSCovidPass

on how to access the NHS COVID Pass and to spotlight reporting routes to report suspected fraud.

The Intel Team worked with partners to identify key stakeholders and brought together a small design group in order to develop the focus and priority of the campaign, draft key-messaging and agree on a design. The group swiftly drafted a design to provide clear, concise and simple advice for the public with key messaging including a breakdown of the tactics used by criminals and guidance on how to stay safe from fraud. Particular attention was drawn to the fact that the NHS App and NHS COVID Pass is free, providing a single link to the NHS website to find out information on how to access the pass.

The Intel Team brought together people with experience in intelligence, stakeholder engagement and policy to identify key threats and develop clear messaging. In particular, the network of partners across the public sector, developed during the pandemic, enabled the Intel Team to draw upon wider expertise in counter fraud, cybercrime and public communications. The pandemic has presented challenges, especially due to the nature of remote working whilst delivering the campaign at pace. However, the Intel Team learned from successes and challenges from previous communication campaigns to agree on messaging, engage with partners and continue momentum from the outset.

In addition, the group developed a comprehensive communications strategy. As part of this, communications were circulated to counter fraud leads across government departments, law enforcement agencies and public sector partners. Furthermore, communications were published on GOV.UK as a resource for raising awareness about COVID Pass fraud.[25] Social media assets were developed to summarise key messaging and circulated across social media with wide support from public sector partners. Assets were published on Twitter[26], Instagram, Facebook and LinkedIn and promoted across channels including Cabinet Office, Trading Standards, Local Authorities, NHS and the Foreign Commonwealth and Development Office.

The public sector fraud community has tracked and analysed trends in fraud reporting, including new hooks to trick members of the public, such as smishing messages threatening ‘fines’ or ‘penalties’ for not following a link to download the pass. In response, the Intel Team has developed updated guidance to highlight that the NHS will never issue fines or penalties relating to the NHS COVID Pass.

Success

The campaign has received wide engagement from members of the public across different platforms and key messaging has been further amplified by news outlets across the country. As of 21st September 2021, the NHS App hit a milestone of 16 millions users, currently the most downloaded free app in England, with over 12 million new users since the NHS COVID Pass.[27] Whilst criminals will continue to target the scheme, the campaign has raised awareness of the threat of cybercrime, contributed to the safe roll out and continual use of the NHS COVID Pass across the United Kingdom and internationally, and increased flows of information into the public sector agencies to monitor the threat of fraud.

Lessons learned

- The pandemic has led to unprecedented challenges, including an increase in cybercrime and it is likely that criminals will continue to target the public purse during the economic recovery from COVID-19 and the future.
- Criminals adapted their tactics to defraud members of the public, illustrated through evolving hooks in smishing, phishing and vishing relating to the NHS COVID Pass.
- Criminals are increasingly taking advantage of social media and technology to defraud the public, leading to identity theft, harvesting of personal data and wider criminality.
- Importance of coordinating intelligence and working together to understand the evolving threat of fraud and flagging new tactics used by criminals.
- Importance of forwarding suspicious text messages and emails to the number ‘7726’ or email report@phishing.gov.uk. The 7726 service sends suspicious messages directly to mobile providers, enabling further investigation and helping to prevent others from being exposed to fraud. More information can be found at https://www.ncsc.gov.uk/guidance/suspicious-email-actions.
- Importance of simple and clear messaging for the public to raise awareness of cybercrime and providing guidance on how to avoid fraud.

Mitigating insider risk in remote working

Author:

Centre for the Protection of National Infrastrucure (CPNI)

CPNI Centre for the Protection of National Infrastructure

Remote working, whether working from home (WFH) or another off-site location, can bring many benefits to both employers and employees. Organisations who have recently embraced large-scale remote working have reported raised staff morale, higher levels of staff retention, more diverse recruitment figures and overall cost savings. Equally, employees working remotely are reporting higher levels of job satisfaction, improvements in work-life balance leading to lower levels of stress and financial savings. However, the Centre for Protection of National Infrastructure (CPNI), the lead government technical authority for personnel and people security, recognises that remote working can introduce additional security risks, which if left unchecked, can lead to serious consequences, such as a member of the workforce conducting an insider act. CPNI defines an insider as someone (a permanent, temporary or contract worker) who exploits, or who has the intention to exploit, their legitimate access to an organisation's assets for unauthorised purposes. In this article, CPNI will discuss the personnel security vulnerabilities of remote working and identify ways to reduce the risk of an insider act, such as fraud, being conducted by a member of the workforce.

Preparation for remote working is the key to avoiding future security problems. At the start of the global pandemic in early 2020, there was very little opportunity for organisations to plan in advance of moving, at scale, to remote working arrangements. This led to some ways of remote working being developed to meet immediate operational needs, without full consideration of the security issues. However, it's never too late to put security policies and procedures into place, and the starting point is for an organisation to assess the security risks of remote working and, in turn, identify mitigations to reduce those malicious acts taking place. Conducting a role-based risk assessment will help identify specific positions in the organisation where conducting a fraudulent act may be easier or more damaging. Consideration can then be given when implementing further protective mitigations for these posts.

What are the security risks?

The security risks for remote working are varied. Most line managers will worry that if they have less direct oversight of remote workers it will be difficult to spot poor performance, but fewer managers would consider that remote working could present the opportunity for a malicious worker to conduct an undetected insider act. Many organisations have recognised that there is an increased risk of loss of IT equipment or sensitive company data when staff work remotely. This is most commonly associated with an unintentional or unwitting insider act, where an employee may not realise the risk of having sensitive data in their possession outside the workplace, nor adopt the company policies and standards appropriate for the use of company personal data. By providing staff training, education and support on the safe use of IT, organisations can mitigate the risk of an accidental loss of IT or a data breach. And, that same training and security messaging can be used as a mechanism to communicate

Photo by Pintera Studio on Pixabay

deterrence messages on the range of security systems in place to spot malicious insider activity.

Some security risks created as a consequence of remote working are less commonly acknowledged. A CPNI study of the insider threat found that a frequently recurring theme amongst identified insiders was unhappiness and frustration due to a combination of poor management relationships, unhealthy work/life balances and a perceived lack of recognition. Having effective policies and procedures, supported by good management is an important mitigation for the risk of employee disaffection and the potential for an insider act occurring. The same high standards must apply to managing remote workers as it does to those based on site to prevent the growth of disgruntlement that is frequently seen underpinning insider activity. An organisation should recognise that providing timely, reliable and constructive feedback is more challenging for managers of remote workers and therefore they should be provided with specific management guidance and training for these situations.

Another often overlooked risk related to remote working is the erosion of company culture and departmental or individual morale. If employees with a positive impact on the team environment enter into a remote working agreement, their absence is often felt by the team members left behind, either through missed contact, disruption of the team's activities, or through resentment if they do not have their own remote working agreement. Change to a group's dynamics can unsettle a team, and the group's activities may have to change significantly to accommodate this new practice. Team engagement can be difficult, particularly if staff work in a variety of locations. However, it is important that this is encouraged as it allows colleagues to get to know each other, reduces feelings of isolation, promotes a common purpose within the team, and provides an opportunity for social activities. As with managers, remote workers should keep in contact with colleagues by sharing diaries, e-mails or instant messaging to replicate the 'water cooler' moments they would experience on site.

Writing a remote working policy

Once the security risks for remote working across an organisation have been assessed then appropriate policies can be created. A remote working policy should be robust but flexible and, of course, must comply with UK employment law. An organisation's lawyer should be consulted before finalising and communicating any policy across the workforce.

An organisation's remote working security policy should state whether any jobs or activities within the organisation are not permitted to be undertaken remotely. For example, those involved in financial transactions, processing of sensitive or personal data, and some IT roles. The decision to exclude certain roles and activities should be based on the outcome of conducting a role-based risk assessment to ensure consistency and evidence of decision making. Policies should also set out arrangements for security and storage of documents, access to sensitive data and IT equipment (including password protection); the sending of documents or sensitive data either in hard copy or electronically; disposal of data; sanctions/disciplinary procedures for breaching security policies, loss of data or equipment. A remote working policy should state any prohibited locations for remote working, including outside of the UK.

The role of line managers

For many people, remote working is an enjoyable experience, but some people do report feelings of social isolation and disconnection with their organisation. Those not enjoying the experience of remote working should be supported to avoid disgruntlement. Managers should be trained to identify the signs and symptoms of employees with personal issues, in particular isolation or lack of contact with colleagues, by having regular one to one online meetings. Remote workers who believe that isolation is having a negative impact on their well-being should discuss with their manager how to overcome their difficulties. This could include more frequent visits to the workplace, for example, in line with government policy on remote working. Sensitive handling of such cases will go a long way in ensuring that welfare problems do not escalate unnecessarily into a security issue and all remote workers should have access to an organisation's Welfare Support and Occupational Health Team.

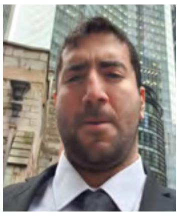
Working hours should be monitored by both the remote worker and their manager to identify instances of both under or over-working. Line managers should also be alert to concerns about excessive working hours for several reasons. Firstly, they have a duty to ensure that remote workers do not contravene the Working Time Regulations and Health and Safety Directives; but it is also important for managers to encourage employees to use their annual leave allowance for welfare reasons. Managers should also be aware of remote employees not wishing to take a break from work or give anyone else oversight of their work whilst they are absent. The CPNI data research study noted several cases of fraud conducted by staff who had sole oversight of financial transactions, and were able to mask their fraudulent activities until such time as they were forced to hand their work to another employee. Managers should be alert to staff who 'log-in' remotely even when they are on leave and excessively 'guard' their work from colleagues.

By following some simple principles, organisations and employees can both enjoy the benefits of a widely adopted remote working arrangement and minimise the potential associated security risks. Assessing and mitigating any identified risk is the foundation of a robust personnel security strategy. Having a clear and well communicated remote working policy will ensure fair but fit for purpose working procedures are adopted consistently across the organisation. Providing staff working remotely with the right equipment, training, and support enables them to work securely with confidence. Providing line managers with specific training to support staff working remotely, both in terms of career development and staff welfare, will improve relationships and minimise the likelihood of an atmosphere of festering disgruntlement that can place a person on a pathway to an insider act.

You can find more information about security risks in remote working at the CPNI website:
https://www.cpni.gov.uk

The taxation of illegal activities: The "Al Capone treatment"

Author:
Raymond Abou-Mansour, LLB (Hons) Law (UCL).
Investigator, HMRC Economic Crime Command



What is the first thing that comes to your mind when you see the words "tax" and "crime" together? Most think of evasion and being punished for it. What usually doesn't come to mind initially is the taxation of crime itself, that is to say, taxing the monies made from illegal activities. That's what I do, I literally tax crime.

Arms dealing, counterfeiting, drug trafficking in narcotics and psychotropic substances, corruption and contraband smuggling, aside from being illegal, all have this in common: they are also taxable activities. The fact that an activity is unlawful or unethical does not stop it being liable to tax. This has been confirmed by a series of cases interpreting the same legislation and its provisions that apply to the rest of us, for both direct and indirect taxes. Notwithstanding the commission of the underlying offence, tax evasion and money-laundering are also committed as offences if amounts made from that original offence (the "predicate"), are not returned to HMRC. We work in this parallel universe to that of an ordinary inspector, where people are guilty of more than tax evasion. And whilst other law enforcement agencies (LEAs) make sure crime doesn't pay, we make sure it does... Tax that is.

So where is the law on this? Judicial precedent on the matter is unequivocal. In Jonas v Bamford [1973] 51 TC 1 it was held "Income is none the less income and taxable as such even though it arises from activities which are wholly illegal". And whilst this is clear, we are then seemingly confronted with a dilemma. By taxing crime, is not the government expressly profiting from it and therefore implicitly condoning it? This argument was famously rejected nearly a century ago in Mann v Nash [1932] 1 KB 752 where the judge stated that this submission raised by the defence was "Mere rhetoric. The state is doing nothing of the kind. It is merely taxing the individual with reference to certain facts. It is not a partner or sharer in the illegality". Indeed, if illegal activities were not taxable, a criminal making money exclusively from illicit sources would not only receive that tax-free thereby being unjustly enriched but would also never be able to be prosecuted

Image: Al Capone's cell at Eastern State Penitentiary, Philadelphia, United States by Ashim D'Silva on Unsplash for tax evasion (as the activity is not taxable, they cannot commit evasion for failing to declare it). This would appear manifestly unfair to the otherwise law-abiding citizen, whose profits from a legal activity are not only taxable but who can also be prosecuted for failing to return them. True equality before the law means equality before taxation because after all, tax is law.

The legislative provisions are in SS317-326 [PART 6] POCA 2002, immediately preceding the money laundering offences in Part 7 (SS327-329 POCA 2002). This gives, for the first time, statutory recognition to the fact that illegal activities were always taxable as confirmed at common law since at least 1886 AD and allows another government department (originally the Asset Recovery Agency, then the Serious Organized Crime Agency and now the National Crime Agency) to also tax them, either in tandem with HMRC or solo.

For example, not only must brothel-keepers and prostitutes pay income tax (see CIR v Aken [1990] STC 497) but they must also pay VAT (see CCE v Polok [2002] EWHC 156). There is nothing new to this; in Ancient Greece, prostitution was also taxable through a tax called the Pornikon (see in 346 BC the Classical Athenian trial "Against Timarchus" by Aeschines at para 119-120).

Fiscally therefore there is no difference between a legitimate business and an illegitimate business, we tax them the same. Criminals, whether suspected or convicted, classify as self-employed entrepreneurs engaged in a taxable trade, profession or vocation, or in an otherwise miscellaneous enterprise, who must declare their finances, even from wrongdoing, to HMRC. This even extends to corporates and other entities. As stated in Martin v HMRC [2015] UKUT 0161 (TCC) "HMRC would not be concerned, in assessing tax, whether the income was derived from criminal activity" and in this respect, we don't just collect tax, we dispense justice by using it against them. The executive policy behind this is found in the Cabinet Office Performance and Innovation Unit Report (2000) "Recovering the Proceeds of Crime" in Chapter 10, a Report which crucially led to the enactment of POCA 2002, the main regime for anti-money laundering in the UK.

But what about this in practice? Civil tax investigators pursue and catch criminals based on a very simple principle: we look at both wealth and lifestyle and ask does the individual appear to have more than their declared income would suggest they should be able to earn?

And what about the accounting? A criminal's accounts and the computation of the profit can never give a "true and fair view" as required by Generally Accepted Accounting Practice, (which are the binding standards for the accounting sector and are prescribed by tax law: S25 ITTOIA05 + S46 CTA 2009) without incriminating them, as they would show the illegal activity and expose them to prosecution. It would be quite ironic for a counterfeiter to issue real invoices and receipts for the fake goods and services supplied. Criminals therefore don't keep books and records of their illegal activities due to the very nature of what they are doing but if they do, they either withhold them or destroy them, as these could be used as evidence against them. As such, its usually us that decides what they pay using our court tested methods, including the option to audit them. As is true of life generally, in accounting everything must balance. To use accountancy terminology, we act as the contra-entry that rebalances the imbalance; the legal debit to the illegal credit.

What then if the perpetrator claims they do nothing illegal, such as a drug trafficker claiming he is "a pharmacist"? That wouldn't matter because pharmacists must pay tax too. It does not impact us how they attempt to hide their occupation even if they do masquerade it as legal, as long as their declared income (if any) mismatches with their expenditure or capital, that would be enough for us to investigate.

But before we investigate to tax them, first and foremost a criminal investigation and the criminal justice system and its processes must have at the very least been contemplated relating to the predicate offence as well as confiscation or forfeiture of the benefit made from it (as mandated in S2A(4) POCA 2002). Confiscation is the first option and requires a conviction. Tax is the last resort where all other measures have failed, it does not need a conviction and may even lead to one. Our compliance and enforcement powers are wide ranging and have dual use to not only disrupt them but also bear yield for the Exchequer. The following powers can be used against any defaulting taxpayer. The advantages of these in a proceeds of crime context will be obvious:

1. We can issue assessments (tax bills) based on our opinion (i.e. not fact) of the amount of tax, duties and contributions payable. We do not need to be exact (see S29 TMA 1970).
2. Interest is chargeable from the date the tax should have been paid. Tax is a Crown debt, and as is characteristic of debt it carries interest (S86 TMA 1970).
3. Penalties are chargeable of up to 100% of the tax in UK cases and 200% with an overseas connection (SCH 24 FA 2007, SCH 41 FA2008). Due to statutory prohibition on claims for deductions, allowances or exemptions for illicit outgoings (SS55 & 870 ITTOIA 2005/S1304 CTA 2009) and the higher rates, this means they may end up owing more than they made.
4. Our investigations and the resulting tax bill span a sliding scale from a minimum of 1 year to a maximum of 20 years (S36 TMA 1970). That's potentially 20 years' worth of tax, interest and penalties.
5. The investigations have global coverage. Citizenship, nationality, domicile and residency are no restrictions to taxing them if the proceeds of their crimes were made in the UK (Whitney v IRC (1924-1926) 10 TC 88).
6. Very importantly, the burden of proof is on the taxpayer. Once the conditions and criteria for making an assessment are achieved, the tax bill remains right unless and until it is shown wrong by the taxpayer themselves. They would also have to supplant it with the right figure, it would not be enough for them to just show its wrong (S50(6) TMA 1970). As stated in Brady (HMIT) v Group Lotus Car Companies plc [1987] BTC 480 "however unacceptable the idea may be to the ordinary member of the public, it has been clear law binding on this court for sixty years that an

inspector of taxes has only to raise an assessment to impose on the taxpayer the burden of proving that it is wrong." In a proceeds of crime context, "The assessment is made. The taxpayer is free to appeal the assessment and to adduce evidence to demonstrate that it is incorrect by providing evidence of his taxable profits, whether lawful or unlawful" Higgins v NCA [2018] UKUT 14 (TCC). They would also be exposed in an open forum for the world to see and indeed on appeal the court has discretion to increase the bill further than what we put it at.

7. HMRC can use any ancillary and expedient ways and means to investigate and raise the tax bill and make inferences (SS5-9 CRCA 2005).
8. The costs both of representation during the investigation and any appeal are not tax deductible. Accountants are not covered by legal professional privilege and can be subject to disciplinary and even money laundering offences if they attempt to deceive us.
9. We can target anyone and anything not just the main perpetrators. We can go after both convicted and suspected criminals but also even their friends and family who may have been accomplices that are aiding and abetting them. This enables us to find their weak spots and dismantle entire groups.
10. There is no need to even investigate. An assessment can be issued at any point even on initial contact as long as we have something to base it on. This makes sense of course as most people are taxed without having to be investigated first! So, the investigation is not a prerequisite for taxation (Van Boeckel v Customs and Excise [1981] 2 All ER 505). We can therefore support law enforcement actions strategically and tactically in this way and we do not need court approval to give them the bill unlike confiscation or forfeiture.
11. If we haven't started a criminal investigation ourselves, our civil investigation can always escalate to a criminal investigation if offences are discovered during the civil investigation (R v CIR (ex parte Allen) (2001) 69 TC 442).

So, when do we tax crime? As the UK's tax authority, it's only right that we focus our law enforcement powers primarily on tackling fiscal crime and disrupting the illicit financial flows that go with it. We do, however, work with our LEA partners and tax the proceeds of crime in a number of cases where the predicate offence is non-fiscal. These tend to be cases where the threat posed to the country is severe, including cases of terrorism, and where all other avenues have been exhausted and where we can effectively target high priority criminal nominals. This approach, of course, has a famous precedent.

Al Capone, also known as Scarface, the notorious mobster boss of the Chicago mafia during the American prohibition era, and the most infamous gangster of all time, committed serious organised crimes ranging from racketeering and bootlegging to murder. Neither the CIA nor the FBI brought down public enemy number one. It was the IRS, the tax man, that prosecuted and convicted him of the only crime they could get him on, tax evasion on his illegally earned income, leading to his imprisonment in Alcatraz. We operate on the same logic but for Her Majesty. In the end, as stated by Benjamin Franklin, one of the founding fathers of the US (a state whose independence was itself triggered by a UK taxation dispute; the Boston Tea Party) and the face that adorns one of the most recognizable signs of wealth on the planet, the $100 bill, "in this world nothing can be said to be certain, except death and taxes".

If you wish to refer cases to us, please report it to: https://www.gov.uk/government/organisations/hm-revenue-customs/contact/report-fraud-to-hmrc

Stop, hang up, call 159

Author:
Simon Miller,
Stop Scams UK

In September 2021 Stop Scams UK, a collaboration of businesses drawn from across the banking, technology and telecoms sectors with the explicit purpose of stopping scams at source, launched 159, a memorable short code number that connects the users of 70% of the UK's retail bank current account holders directly safely and securely with their bank. The messaging behind 159 is clear, if you have received an unexpected or suspicious call from someone claiming to be from your bank: stop, hang up and then call 159.

We are very proud of the work that has gone into 159. It has been an extraordinary collaborative effort between banks, telecoms firms and technology companies. It shows what can be achieved when businesses work together. 159 has been launched as a pilot, if it is as successful as we think it will be, Stop Scams UK will ask Ofcom to make 159 a mandatory number, offered by all telephone providers, similar to 101, 111 or 999.

Why have we done this? Well, the answer is simple: scams in the UK are increasing exponentially and causing UK consumers and businesses real and growing harm. This must be stopped if we are to keep consumers safe and ensure that scams do not undermine trust in our systems and damage the UK economy.

According to figures published by UK Finance, UK banks recorded over £1.26bn of reported banking fraud in 2020[28]. Authorised push payment fraud - a type of scam where victims are manipulated by criminals, often through social engineering, into making real-time payments - accounted for 38% of that, up from 36% the year before. Remote banking frauds also increased by 4%. In the first six months of 2021 alone, reported APP Fraud was 60% above the equivalent level for 2020 with the losses incurred by consumers and businesses 71% higher.

To put this in money terms, criminal gangs stole over £470m from individuals and small businesses last year alone by pretending to be a bank or other authority figure, encouraging customers to make a payment or transfer money. But it is not just the money[29]. Scam journeys cross multiple sectors and platforms. They combine websites, text messages and phone calls, as well as complex and nefarious 'social engineering' scripts to scam people. Stopping them will require intervention at multiple points in the scam journey and for businesses across each of the banking, technology and telecoms sectors to work together.

Policy makers have recognised that collaboration across sectors is needed for solutions to be truly effective and this is core to each of the sector fraud charters that cover accounting, banking and telecoms which has been agreed by the Home Office with Industry. Stop Scams UK exists to help make this collaboration happen.

Stop Scams UK started life in 2019, when a small team led by Ruth Evans (our Chair) met to explore opportunities to work across sectors. That team was drawn from representatives of Barclays, BT, the Financial Conduct Authority, Grant Thornton, Ofcom and UK Finance. The early work established that there was a clear need, as well as an opportunity, for a new cross-sector approach to helping firms protect their customers based on proactive collaboration, and the sharing of insights and best-practice.

Because scam journeys are complex, we know we have to have a cross-sector approach, but at the same time be sector-neutral. We also have to be representative of those sectors where scams are most prevalent. This gives us real clarity of purpose; to bring together responsible businesses through the development and realisation of industry-led solutions to the harm caused by scams. 159 is the first such example of this.

Photo by Tim Mossholder on Unsplash

We know that although businesses, industry bodies and regulators are making huge efforts to limit the harm caused by scams, including some powerful examples of effective collaboration through CIFAS and UK Finance, some firms and sectors struggle to work together. The banking and telecoms sectors, for instance, and the businesses within them, were not only set up to be highly competitive but they are also highly regulated. As a consequence, it means that some can find it difficult to engage with other businesses and across sectors. We have a remit from our members to facilitate this engagement.

We have not been set up as a trade association with a single industry view, but as a peer to peer not for profit organisation, established to provide a safe space for collaboration and to enable businesses to make a difference and collaborate.

Stop Scams UK has now been formally constituted for a year. Our membership includes all major UK high street banks (accounting for over 80% of UK current accounts) and some of the UK's largest telecoms firms. We also have growing representation from the technology sector, with Google and Microsoft joining earlier this year.

159 is our first major initiative. It has been launched as a pilot but it is clear already that it has the potential to be a powerful consumer tool. Calling 159 could become a reflex action and response to suspicious or unexpected calls; it is a practical way of enabling people to stop, challenge and protect both themselves and their money. It's a simple step that could be the difference between them falling victim to a scam, with all the potential harm and practical difficulties that entails, or avoiding it altogether.

Over 4,500 calls were made to 159 in its first week of operation and over 15,000 calls in the first month and each month since. If the average bank impersonation scam costs the consumer in excess of £3,000[30], 159 has already potentially saved customers a lot of money. This has been done with only the smallest amount of publicity using basic technology.

2022 is going to be a critical year for Stop Scams UK. Our immediate priority is to take forward the development of 159. Currently, it can only accommodate as many banks as there are touch pads on a telephone.

Our immediate focus will be to replace the auto-attendant on the BT interconnect with an intelligent voice response service, providing us with an opportunity to increase the number of participating banks. This will not only allow for the expansion of the service but open up new opportunities for data capture and data sharing, and an ability to triage calls. An enhanced capability to capture data could also enable the generation of new insight on both the scam journey, possibly including scam call tracing but also new insight into the scammers and their modus operandi.

This investment will help put the service on a stable footing and help drive it forward to its next phase. We also hope it will enable the expansion of the service to other potential destination participants such as HMRC, Royal Mail and TV Licensing as well as other organisations at risk of scams and other forms of impersonation fraud.

The data that the service will generate, particularly once the changes outlined above are implemented, will drive the insight and performance information needed to be able to kickstart the Ofcom consultation process to make 159 a mandatory number.

As we take forward 159, Stop Scams UK will work with key stakeholders in the anti-scam space to ensure that the service and products we offer add value to and complement existing initiatives. Part of this will include exploring whether and how the data generated through 159 can be shared with regulators and others, such as the National Cyber Security Centre and law enforcement agencies so it contributes to their work to combat scams and keep UK consumers and citizens protected.

However, Stop Scams UK is about much more than the 159 campaign. Our strategy for 2022, agreed by our Board in November 2021 includes a focus on the delivery of a number of research and development projects to enable better information sharing between businesses and specific harmful URL blocking across sectors.

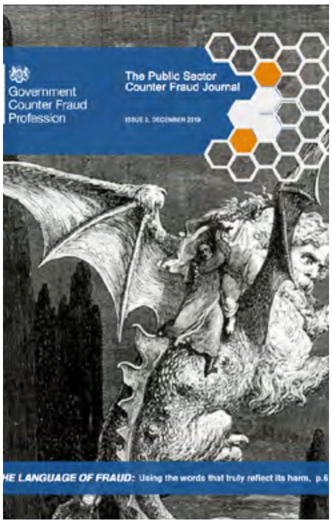
A major part of this work will be to define the role of Stop Scams UK in the ever-changing, scams landscape, recognising existing and emerging workstreams and responsibilities, including the links with and to the Government's Sector Fraud Charters and other regulatory initiatives. Above all, we need to make certain that our work adds clear, new value to efforts to stop scams.

This will all be in addition to our existing workstreams, particularly our technical collaborations through which we enable our members to develop innovative solutions to disrupt scam journeys before they can cause harm. We believe these benefits could not be realised either by individual firms or within single sectors alone. These services protect consumers from criminal web content and data harvesting, and work to enable better information sharing on risk signals. Future collaborations will support strategies to identify, develop, scope and evaluate concepts for future projects.

2021 has been a big year for Stop Scams UK. 2022 will be even bigger. We know (as do our members) that there is still a mountain to climb if we are serious in our endeavours to keep consumers protected. But we are clear that we have a vital and important role, and given our membership is across three key sectors, we have a unique role in the fight to stop scams.

Stops Scams UK's members are: Barclays, BT, Gamma, Google, HSBC, Lloyds, Microsoft, NatWest, Santander, Starling, TalkTalk, Three, and TSB.

Previous issues


Government Counter Fraud Profession
The Public Sector Counter Fraud Journal
ISSUE 3, DECEMBER 2019
HE LANGUAGE OF FRAUD: Using the words that truly reflect its harm, p.6

Issue 3

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

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

Government Counter Fraud Profession
The Public Sector Counter Fraud Journal
ISSUE 4, MARCH 2020
SASTER CRIME: Protecting emergency relief efforts from fraud risk, see page 7

Issue 4

- Countering fraud in disasters
- Fraudsters are people too!
- Preventing and detecting fraud using machine learning
- International collaboration

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

Government Counter Fraud Profession
The Public Sector Counter Fraud Journal
ISSUE 5, JUNE 2020
NHS
COVID-19: Staying alert to the risk of fraud during the pandemic

Issue 5

- COVID-19 response
- Insurance fraud
- Career change
- Coronavirus, fraud risk and the use of the word “scam”
- Digital detectives in the NHS
- Black swans

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

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

Issue 6

- Measuring the iceberg: the Fraud Measurement and Assurance Programme
- Can risk be your friend?
- Fraud fighters unite to defend the UK from COVID-19 crime

Download:
https://bit.ly/journal-issue-6

Government Counter Fraud Profession
The Public Sector Counter Fraud Journal
ISSUE 7, FEBRUARY 2021
Using social norms to prevent fraud and corruption

Issue 7

- Bribery and corruption
- Following the money
- Innovating amid a crisis
- Energy theft

Download:
https://bit.ly/journal-issue-7

Government Counter Fraud Profession
The Public Sector Counter Fraud Journal
ISSUE 8, JULY 2021
The Fraud Triangle: its origins and relevance

Issue 8

- Fraud triangle
- Human Risk
- New disclosure culture
- Mortgage fraud

Download:
https://bit.ly/journal-issue-8A

Endnotes

[1] See, for example, 'Investigation into Dubai money laundering ring continues as £5.5m cash courier Tara Hanlon jailed.' https://www.essexnewsandinvestigations.com/single-post/investigation-into-dubai-money-laundering-ring-continues-as-5-5m-cash-courier-tara-hanlon-jailed (accessed 29/11/2021);

https://www.nationalcrimeagency.gov.uk/news/closed-case-plane-passenger-with-1-5m-in-baggage-ordered-to-give-it-up (accessed 29/11/2021).

[2] See Johnson, J. 'Head of money-laundering unit resigns over suspected money-laundering', The Telegraph, 9 November 2021.

[3] Roks, R., Leukfeldt, R. and Densley, J., 2021. The hybridization of street offending in the Netherlands. The British Journal of Criminology, 61(4), pp.926-945; Soudijn, M.R. and Zegers, B.C.T., 2012. Cybercrime and virtual offender convergence settings. Trends in organized crime, 15(2), pp.111-129.. Berry, M., 2020. Organised crime in Red City: An ethnographic study of drugs, vice and violence. PhD Thesis, Cardiff University. Other UK work is currently under review.

[4] Leukfeldt, R., Lavorgna, A. and Kleemans, E., 2017. Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime. European Journal on Criminal Policy and Research, 23(3), pp.287-300.

[5] Button, M. and Cross, C., 2017. Cyber frauds, scams and their victims. Routledge.

[6] Aston, M., McCombie, S., Reardon, B., and Watters, P. (2009, July). A preliminary profiling of internet money mules: an Australian perspective. In 2009 Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing (pp. 482-487). IEEE.

[7] Roks et al., op cit. n4. See also Soudijn and Zeegers, n.4, who note that distant mule herders have little control over mules recruited on the Internet. They suggest using undercover fake 'mules' to create uncertainty in the criminal market by not passing on moneys to the next stage, despite the detailed instructions they receive from herders. This tactic might be too dangerous in the hybrid cases of local recruitment.

[8] https://www.scmp.com/news/china/society/article/2189065/warnings-issued-after-britain-freezes-chinese-students-bank; https://www.universityworldnews.com/post.php?story=20190307200521986. See more generally, https://www.cifas.org.uk/newsroom/new-data-reveals-stark-increase-young-people-acting-money-mules; https://www.europol.europa.eu/newsroom/news/over-1500-money-mules-identified-in-worldwide-money-laundering-sting; https://www.bbc.co.uk/news/uk-england-45797603 (all accessed 30 November 2021). See also the thoughtful NCA review of Chinese underground banking: https://www.nationalcrimeagency.gov.uk/who-we-are/publications/445-chinese-underground-banking/file.

[9] Gundur, R.V., Levi, M., Topalli, V., Ouellet, M., Stolyarova, M., Chang, L. and Mejía, D., 2021. Evaluating Criminal Transactional Methods in Cyberspace as Understood in an International Context. CrimRxiv, https://www.crimrxiv.com/pub/48bmtkg0/release/3; Moiseienko, A. and Kraft, O., 2018. From Money Mules to Chain-Hopping: Targeting the Finances of Cybercrime, RUSI Occasional Paper.

[10] See UK Finance's https://www.moneymules.co.uk/

[11] 'Prevent' is one of the 4Ps - See HM Government, 'Serious and Organised Crime Strategy 2018' https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752850/SOC-2018-web.pdf (accessed 21/12/2021). Though it discusses economic crime prevention extensively, the Economic Crime Plan does not relate to the Prevent approach to turning people away from criminal pathways.

[12] https://www.lloydsbankinggroup.com/insights/taking-on-the-fraudsters-together.html

[13] https://jobs.netflix.com/culture

[14] https://www.legislation.gov.uk/ukpga/2013/3/contents

[15] You can read the final PPP published by the Audit Commission here: https://webarchive.nationalarchives.gov.uk/ukgwa/20150421134146/http:/www.audit-commission.gov.uk/wp-content/uploads/2014/10/Protecting-the-Public-Purse-2014-Fighting-Fraud-against-Local-Government-online.pdf

[16] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/961505/2609-Executive-Summary-Fraud-Landscape-Bulletin-V7.pdf

[17] https://www.gov.uk/government/statistics/annual-fraud-indicator

[18] See, for example: https://www.thecaq.org/wp-content/uploads/2020/03/afc_assessing_corporate_culture_a_proactive_approach_to_deter_misconduct.pdf

[19] https://www.actionfraud.police.uk/report-phishing

[20] https://www.which.co.uk/news/2021/07/scams-rocket-by-33-during-pandemic/

[21] https://www.ofcom.org.uk/news-centre/2021/45-million-people-targeted-by-scams

[22] https://www.nhs.uk/conditions/coronavirus-covid-19/covid-pass/

[23] NHSX is a joint unit of NHS England and the Department of Health and Social Care, supporting local NHS and care organisations to digitise their services, connect the health and social care systems through technology and transform the way patients' care is delivered at home, in the community and in hospital.

[24] https://www.gov.uk/government/publications/resources-for-raising-awareness-about-vaccine-fraud

[25] https://www.gov.uk/government/publications/resources-for-raising-awareness-about-covid-pass-fraud

[26] https://twitter.com/cabinetofficeuk/status/1442428804673179648?s=20

[27] https://www.nhsx.nhs.uk/news/milestone-hit-with-over-16-million-nhs-app-users/

[28] https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202021-%20FINAL.pdf

[29] https://www.ukfinance.org.uk/system/files/Half-year-fraud-update-2021-FINAL.pdf

[30] https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202021-%20FINAL.pdf

Government
Counter Fraud
Profession

Contact us:

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