



Government  
Counter Fraud  
Profession

# The Public Sector Counter Fraud Journal

ISSUE 4, MARCH 2020



**DISASTER CRIME:** Protecting emergency relief efforts from fraud risk, see page 7







# CONTENTS

- 5 - Editor's Letter**
- 6 - Designing an effective response to fraud arising from disasters**
- 9 - Building sustainable capability for the Counter Fraud Function**
- 11 - Fraudsters are people too!**
- 14 - They're not lovable rogues, they're ruthless criminals**
- 16 - Mass-marketing fraud susceptibility and risk**
- 18 - Preventing and detecting fraud using machine learning**
- 20 - Tackling Economic Crime Awards**
- 22 - Award-winning collaboration**
- 24 - On the right track**
- 26 - How an apprenticeship can boost your counter fraud career**
- 28 - Why businesses must be just as alert to fraud as consumers**
- 30 - Fighting public sector fraud through international collaboration**



---

# Editorial Board



**Toni Sless**  
Chair and Founder  
Fraud Women's Network



**Jackie Raja**  
GCFP Development Lead  
Department for Work and  
Pensions



**Professor Mark Button**  
Director of the Centre for  
Counter Fraud Studies



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



**David Kirk**  
Consultant Barrister  
RS Legal Strategy Ltd



**Maria Kenworthy**  
Investigator  
Ministry of Justice  
Counter Fraud and  
Investigations



**Mick Hayes**  
National Operations Manager  
NHS Counter Fraud Authority



---

# Editor's letter

*This issue's letter is again provided by David Kirk, a member of the Journal's Editorial Board. David has practiced as a barrister and solicitor for both prosecution and defence, specialising in economic crime, since the early 1980s*

This fourth edition of the Journal, with its wide range of topics, feels very much like: 'now let's get down to the serious business of identifying and preventing the serious economic crime that features so high on the government's risk list.' No easy task, of course, but one that can be made slightly easier when we stop pretending that fraud is something that happens to others, and recognising the enormous scale of the problem, and the serious damage it causes across the board. Government, businesses of all sizes, and individuals, rich and poor, suffer from the fraud plague in measures that are different only in scale.

The true cost of fraud has always been a bit of a finger in the air exercise. Numbers are bandied about which are as terrifying in their size as they are difficult to prove. Dr Hanoch and Professor Wood quote the Home Office as reporting that the annual figure at £110 billion, "roughly equal to the cost of the NHS in England". Or to use a more topical comparison, the cost of HS2, as estimated this week. Their description of the types of activity encompassed under the heading of Mass Marketing Fraud will strike a chord with almost every reader – we have all received those calls, and fought off those attempts to part us from our assets.

The practical measures that can be taken to reduce fraud risk require excellent (not just good) systems and controls,

intelligent equipment, and well-trained staff with inquisitive minds. Nick Jennings's account of the small beginnings, and subsequent development of the award winning Hertfordshire Shared Anti-Fraud Service is a brilliant reminder of how programmes that really work and make a difference can be built by determined and funded manpower. I have also seen this working at first hand, in my capacity as Chair of the Fraud Advisory Panel, working closely with the Charity Commission – a fellow finalist in the "Tackling Economic Crime Awards" – to reduce the level of fraud committed in the charity sector.

The extent to which fraud is mean, callous and very damaging, just as other criminal activity is, is exposed in Nick Sellars' article on responding to fraudsters who take advantage of disasters to make fraudulent claims. Just as fraud against charities seems utterly disgraceful, in addition to being criminal, taking advantage of a disaster to make a dishonest profit is beyond all comprehension. It is of course true, as Christopher Haycock says, that fraudsters are people too, and we all need to understand people better in order to identify risk, but the complications involved in probing the character of every employee, or claimant, and challenging people's integrity in what will often be seen as tragic circumstances, can be difficult, to put it mildly.

But this is what the GCFP has been set up to achieve, and every member of the Profession has an opportunity to engage in this fascinating – and sometimes frustrating! – work. Apprenticeships will soon be available, as Maria Kenworthy sets out, and they certainly can boost your career. The GCFP needs you.

**David Kirk, Consultant Barrister, RS Legal Strategy Ltd**

## Get Involved

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

*Please email us via: [pscfjournal@cabinetoffice.gov.uk](mailto:pscfjournal@cabinetoffice.gov.uk)*







*Smoke and flames in Australia, by the European Space Agency, is licensed under CC-BY 2.0*

*Ferocious bushfires have been sweeping across Australia since September 2019, fuelled by record-breaking temperatures, drought and wind. The smoke, flames and burn scars can be seen clearly in the image, which was captured on 31 December 2019.*



# Designing an effective response to fraud arising from disasters

In September 2019, many rural communities and regions in Australia began to be affected by what would become a summer of devastating bushfires. By Christmas, smoke from bushfires had reached dangerous levels in Canberra and Sydney. On New Year's Eve and the days following, fire fronts trapped thousands of summer tourists and residents at the water's edge in small and mid-sized towns in New South Wales and Victoria. Fires tore through the hills East of Adelaide, and across South Australia. The main highway linking Perth to the Eastern States was impassable for more than a week. By mid-January 2020, some 27 lives had been lost, more than 2,000 homes destroyed, over 10 million hectares of forest and farmland burned and over one billion invertebrates killed. Tens of thousands of people have been displaced from their homes. Public infrastructure, including thousands of kilometres of roadways, fencing, electricity lines and reservoirs have been damaged. The Australian Defence Force and the Army Reserve have been mobilized to assist in the response.

Within ten days of the New Year's Eve fires, Prime Minister Morrison announced a tax-payer funded A\$2 billion bushfire recovery fund, and a new national agency to administer its distribution. Immediate grants of A\$1 million to local councils were also approved and paid within 24 hours to underwrite immediate clean-up priorities, to be reconciled at a later date (essentially a trusted-trader scheme). A similar low-documentation scheme to get cash and other support from government agencies direct to displaced individuals is also now in place.

In a heart-warming response, hundreds of millions of dollars have been donated from individuals (including celebrities) around the world to charities and firefighting organisations through ad-hoc on-line fundraising. Sadly, but not unsurprisingly, within days of the first deaths of firefighters and the loss of homes, online scammers sought to cash-in on the tragedy, prompting the government and media to warn of fraudulent fundraisers. As fraud professionals will know, the worst may be yet to come.

## Disaster fraud

It is predicted that our changing climate will significantly increase the frequency and scale of disasters like catastrophic bushfire, flood and wind events. One of the

*About the author:*  
**Nick Sellars,**  
*Special Integrity  
Advisor, Integrity  
Partners Australia  
Pty Ltd*

*Nick is a former  
senior public servant  
in the Australian  
Government, now in  
private practice.*



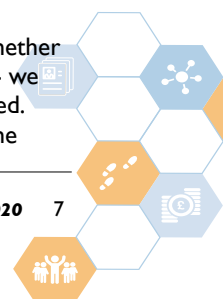
strategic questions that arises is how will all levels of government be strengthening our logistical responses to ensure that we don't also have a governance (and associated financial) disaster?

Disaster fraud is real: from charity fraud, false insurance and grant claims, through to major procurement corruption. As terrible as these frauds are, they demonstrate how some risks tend to group around certain factors, thereby enabling fraud policy-makers to design an impactful, thematic response.

Each natural disaster event brings its own distinctive characteristics. As a generality, thankfully, these events don't tend to happen in the same geographical region too often. However, this cycle means a need to build a response capability every time, including in the governance and anti-fraud space. Such disasters can be unpredictable and unprecedented in their scale. While disaster recovery money from government can flow quite quickly, as the current Australian experience shows, there isn't always the skill set on the ground to be able to deliver relief outcomes in the time frames needed (at least not with the level of competence and probity we might usually expect).

For instance, public procurement processes are one of the response capabilities that get pushed in to overdrive every time there is a need to recover quickly and rebuild following a major flood, wind event, fire or other disaster. In the initial recovery phases, the need to develop and deliver fast infrastructure outcomes can reduce the supplier pool and reduce purchasing bargaining power. Even so, the risk of being "ripped off" at that point is probably comparatively low (despite the governance arrangements that might be lacking). However, in the medium term, the increased scale of rebuilding and high volume of transactions can lead to reduced oversight, cosy relationships forming and a much higher risk of collusive contract manipulation. The risk is that recovery dollars are wasted - essentially paying too much because of pressure to deliver a result, but also through unscrupulous operators and decision-makers taking advantage of a significant corruption opportunity (for example, rigged tendering).

Just as storm water will find its way into buildings - whether through cracks in the wall, or through a torn off roof - we know fraud will follow and find money left unsupervised. There is a lot of money in disaster recovery, and for the







The aftermath of the bushfires in Sarsfield, Australia in January 2020  
Image: Peter Mackey CC BY-ND 2.0

reasons outlined above, it is often under-supervised.

### **An effective response**

But just how can we balance the required agility and pace of response with an effective means of ensuring the risk of fraud is reduced as far as possible?

One answer is the recovery taskforce model, and ensuring governance (including purchasing and probity skills) form part of the standard response toolkit to support governments and, more particularly, local government where capability may be low. An even more mature approach can include a range of jurisdiction-wide, pre-approved supplier tender panels, so that valuable response time is not tied up in red tape, while reputable delivery capability is sourced and procured on a competitive basis.

With so much at stake, the USA has responded to this risk by establishing a standing capability to deal with criminals who would seek to exploit the opportunities these disasters present: the National Center for Disaster Fraud (NCDF), located within the US Department of Justice. The NCDF has a well-targeted mission statement: it detects and investigates disaster fraud. It coordinates and supports fraud responses nationally, providing outreach and training, educates the public about disaster fraud risk and provides policy leadership. Since NCDF began in 2005 it has received 95,000 complaints received in relation to 100 natural and man-made disasters over 50 states. What an amazing policy response. The scale of the US problem is bigger than Australia's, due to population size differences, so there is arguably more potential for fraud to occur.

However, the sophistication of the response has as much to do with NCDF's political underpinnings - imagine the

despair of being a victim of Hurricane Katrina (1,800 lives lost; US\$100 billion in damage), only for communities such as New Orleans to become victims a second time as a result of local government corruption found to be compromising the response to Katrina. This thematic response inherently builds specialisation and efficiency of professional practice in

a way that can reach across silos; multi-party political and community support models that build trust in government; articulates public value in a way that is hard to argue with (rebuilding communities following a disaster, fairly); run by experts in the field.

### **Options for Australia**

So, could the NCDF model suit Australia, given a worsening prognosis for disasters? Well, as they say in the corruption investigation handbook: if you don't look, you don't find. Thematic risk is a good place to start.

I see that an exploration of disaster fraud could start off as a very useful focus point of Australia's new Commonwealth Fraud Control Centre, presently being established within the Attorney-General's Department (AGD). It would be a nice way to stretch into some non-traditional spaces (e.g. emergency management augmentation) and be a catalyst for engaging with the public and across layers of government to achieve a common purpose. AGD is good at all those things, and the leadership focus and innovation would likely be welcomed by stakeholders. If it helps local communities to recover from disasters, fairly, then that, surely, is a good thing.

**For more information on fraud in emergency management and recovery see the article on page 30 regarding the work of the International Public Sector Fraud Forum**



# Building sustainable capability for the Counter Fraud Function



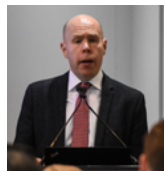
The GCFP team meet members of the Profession at Counter Fraud 2020

**O**ur Government Counter Fraud Profession continues to grow. Whether you are already among our community of over 6,000 members who have already joined, or someone who aspires to be one in the future, have you considered what membership actually means?

Fraud is a hidden, complex and evolving crime. Tackling it effectively does not necessarily mean more investigations are required. Investigation and enforcement, through both the civil and criminal routes, remains invaluable, but by the time an investigation has started the fraud has already happened and the harm has been done, whether that is to victims, communities, the public purse, businesses or charities. We need to better understand fraud, its true dimensions, seek to prevent it and use insights to determine the appropriate response.

The National Audit Office, in its 2016 Fraud Landscape Review, reported that “Departments’ capacity and capability to manage fraud is mixed”. The Counter Fraud Profession now exists to build capability across the Counter Fraud Function and has already made significant progress. Central to this is the understanding that the counter fraud

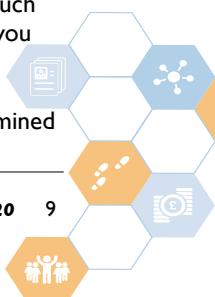
Author:  
**Chris Freeman**  
Head of Engagement  
and Membership,  
Government Counter  
Fraud Profession



community does not solely consist of investigators. The Profession, therefore, is built to recognise the diversity of skills to holistically deal with fraud as it is now and in future, as it continues to change. This has included developing new Profession Standards in the areas of Fraud Measurement and Assurance, Fraud Risk Assessment and Data and Analytics, moving towards a more proactive approach to fraud.

As a member of the Government Counter Fraud Profession you are recognised as having a level of training, knowledge and skills that meet the Counter Fraud Profession Standards, meeting an exacting standard for counter fraud occupational competence as defined by the Profession Standards Framework, which may or may not also include qualifications. This is where the Profession differs from its antecedents: a qualification is the first step but it is essential that having completed one you apply that knowledge in order to attain practitioner status. To retain recognition as a practitioner you must then continue to maintain and develop your skills. As such membership signifies that you are up-to-date and that you are active as a practitioner.

When the Board was first formed it was quickly determined that the Profession should recognise a number of core





disciplines and sub disciplines, with separate Profession Standards for each. The development of standards, however, is a substantial task in itself. The Profession Standards include a skills matrix, which identify the key components required by someone working in that discipline. They also have product and process guides - models of how the work should be done.

With the diversity of counter fraud work undertaken within government finding that common ground to put into the Standards was a major undertaking.

When talking about the Profession we frequently say it was 'built by experts, for experts'. It was essential that the Standards were not merely a reflection of current practice, which may not necessarily be the right way to do things; by bringing together the right experts from the public and private sectors and academia it was possible to define the right practices and build the Standards to reflect this.

One of the best parts of my role is meeting with practitioners from across the counter fraud community. Engagement is a vital part of my job, delivering presentations and using workshops to gather ideas and insights. I continue to be surprised by the variety of counter fraud work

within those limited bounds, but as already discussed, to do so would be ignorant of the real reasons the Profession was needed.

During 2019 the Profession launched the Fraud Risk Assessment Standards. There was a recognition that, again, capability in that particular area was mixed. The Profession also developed training based on the Standard, successful completion of which results in the first qualifications awarded by the Profession and also membership. Now we are developing standards on Fraud Measurement and Assurance and also Data and Analytics for Fraud; this work will continue into 2020.

This year we will be focusing on the establishment of a Learning Environment Advisory Panel (LEAP), which will be integral to the Profession's aim of becoming an awarding body for counter fraud qualifications.

We have already expanded the Profession beyond central government, with both City of London Police and the Eastern Region Special Operations Unit (ERSOU) gaining membership in 2019 and continue in 2020 to work with groups from local government to build options for local authorities to join too. We will also be developing options



GCFP Head of Engagement and Membership Chris Freeman speaking at Counter Fraud 2020

undertaken, with high-volume but low value fraud being common to one organisation to single cases running to millions of pounds and taking years to conclude the staple of others. What is common to all, however, is the passion that practitioners have for their work. I am also asked, constantly, about the progress we are making and what is planned for the future. There is a definite hunger for the Profession to do more and to widen its remit further.

The decision to launch the Profession in October 2018 by opening to members in the Intelligence and Analysis and Investigations disciplines was a recognition by the Board that the majority of people working in the Counter Fraud Function would be found in those disciplines. It would have been easy to stop at that point and just grow the Profession

for individual membership, which will mean those working in organisations not able to meet the requirements for collective membership will still be able to join the Profession.

During 2020 there will be more opportunities for members to continue to build their community together, through practitioner events and our annual conference too.

It's a really exciting time to be part of the Profession; we are, collectively, really ambitious. But we must also temper this to ensure that what we build is of the highest quality and sustainable. I don't yet know what the Profession will look like in 2030, but with the drive and enthusiasm of those in the Counter Fraud Function it's clear that we can, working collaboratively, achieve great things together. †





# Fraudsters are people too!

**T**his is not going to be 1500 words of excuses for those who commit fraud. What I hope to do here is to present an alternative view, which may help organisations, and specifically public sector organisations, better understand those within the organisation, who may find themselves involved on the wrong end of a fraud investigation.

Classical theories of criminality espoused by Jeremy Bentham (1747 – 1832) and Cesare Beccaria (1738 – 1794) suggested that crime was a function of the offender's weak will or over-stimulation (see Farrer 2019, Williams and McShane 2010). It was thought that external control of the offender, by way of punishment, was key to correcting this deficient personality. Even more recently in our history, Cesare Lombroso (1835 – 1909) really did follow the social Darwinian line that criminals were degenerates, whose criminality was literally written all over their faces and evidenced by “sub-normal” physiognomy (Ellwood 1912). While we are probably less inclined to follow the social Darwinian doctrine, we do however still see remnants of these philosophies today. The belief that fraudsters are somehow different or bad still receives support from some engaged in the counter-fraud professions.

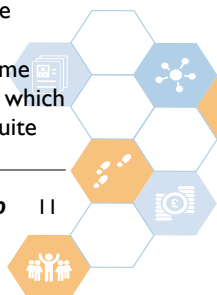
*About the author:*  
**Christopher G Haycock** MA, MSc, BA (Hons), PGCE, PGCert, DipHE, SFHEA, ACFE, CFS

*Chris is a Senior Fellow of the Higher Education Academy and the Course Director for the MSc Fraud Investigation Management course at the School of Psychology, Social and Behavioural Science at Coventry University.*



This professional-client tension is common among many sectors, but we find that it is also echoed from a public perspective too. The tenets of the classical theories remain alive today, in calls for increasingly harsh prison sentences in the expectation that this will reduce crime. Society has always expected the criminal justice process, and principally prisons, to correct offending behaviour in the individual. After centuries where prisons fail at this task, modern criminology theory and the fraud investigation profession more generally, are coming around to the idea that fraud is an issue for the whole of society to address, and a more holistic approach to the fraud threat is required.

Explanations for crime today are more likely to consider the individual within their environment, not to provide excuses or acceptance of the criminal actions, but to understand their actions. Attributing fraud to modern society in a similar way, may then seem fairly reasonable. Where there are transactions which involve money, money equivalents, things in action or other assets, there will be fraud. So, the argument goes that if the cultural environment gives rise to the transactions then surely that same environment must be responsible for the frauds which may take place within it. However, fraud is not quite





the same as other acquisitional offences. To begin with fraud is a civil tort as well as a crime; a fraud requires another person to willingly provide the asset and those who commit fraud do not conveniently fit the canonical explanations of crime based on background and social position.

There are fraudsters who see crime as a way of life, who do not possess qualifications and experience with which to barter for wages, fraud is simply their means of achieving their hopes and aspirations. Fraud is, however, a special case, as we also see many frauds committed by individuals who have access to these assets and are employed. "Insider fraud" cost UK businesses £40million in 2016-2017 (RSM 2017) and £88million in 2018-2019 (Taylor-Whiffen 2019). The Association of Certified Fraud Examiners (ACFE) (2018) found that only 4% of perpetrators had any previous convictions, and fraud by those

who had been with the company the longest often accounted for the highest losses. We see many cases where the fraudsters are in fact managers, owners and chief officers of organisations. The public sector is not immune to this either. While there are issues with devising accurate values for these losses, Gee, Button and Brookes (2010)

put them as high as £74.2 million per annum (after adjusting for "expected figures"). Not a huge number in terms of public body budgets, but when viewed in terms of the 1,400 nurses it could fund each year (Curtis and Burns 2018) or the more than twelve thousand children it could put through school each year (Sibieta 2018), it becomes evident that there are many other valuable and needed areas where this public money could, and should, be spent. We just need to understand the motivation sufficiently in order to deter it.

The fraud triangle (Cressey 1973) and Wolfe and Hermonson's (2004) diamond model are concepts which are often used to explain fraud. However, contrary to popular belief, they are not an investigative tool, nor are they an explanation of fraud. These models are simply an acknowledgement that any behaviour, not just fraud, requires certain ingredients to be present before that behaviour takes place. People are not geometric, they are far more complex. On their own, neither of these models will add much to a forensic enquiry, although they do have their uses. They are both useful tools from a risk assessment perspective, to identify red flags. Understanding that a perpetrator, and specifically in this case an employee, must have all three ingredients present before they will commit a fraud against their employer, helps put the opportunity (here I include capacity with opportunity) part of the models into context. As a business traditionally could not readily control all the pressures that a person might experience to commit fraud, as this is often outside the organisations domain, nor the means by which a fraudulent act might be justified in the employee's mind, as this is contained within the ultimate sanctum of the conscience, it leaves only opportunity. This could be fairly easily controlled through robust processes and oversight. The ACFE in the USA (ACFE 2018) found from their Annual Report to Nations research that over half

of the frauds their members reported were due largely to poor internal controls, and for this reason opportunity is typically the only element that a business would consider addressing. If, however, we could have a more direct effect on how fraud might be justified, by understanding how a person might rationalise a fraudulent act or a more supportive approach to the potential pressures to commit fraud, then a more effective counter fraud activity can be planned, the model now becomes very useful from a risk assessment and asset protection perspective. The challenge therefore is now to discover what influences justification or pressure.

Current sociological and criminological theory may help here. The theoretical consensus has moved to a more holistic explanation for crime where the offender is no longer seen as abhorrent, deviant or different, but as an individual working under the usual and unusual pressures

of life (see Youngs and Canter 2012). By considering the person's "self narrative" (ibid) a better understanding can be had for the various aspects of the person's personality which might, under unusual circumstances lead to their committing a fraud. This perspective can be used to better understand not only why a particular person

may commit a particular fraud but also why a senior executive may commit fraud, as they do not usually fit the more traditional explanations of criminality. Often in these cases there is a self-narrative of a person who believes they must save the business, or conversely one who might see themselves as being entitled to certain perks because of their position, etc. Having a better knowledge of a person's "narrative", managers and investigators will have a better understanding of whether a particular person becomes bitter, entitled or turns to addictive behaviours when under stress (Hathaway and McKinley 1940). With support for staff the organisation can be better placed to deal with, not only staff going through divorce, addiction, bereavement or any of the other life changing events that visit us all on occasion, but also those in positions of power and authority who so often suffer least from oversight and control but potentially more from the forces affecting their businesses.

There are a number of personality tests in circulation such as The Minnesota Multiphasic Personality Inventory, 2nd Edition (Green 2000). Often these are only advised to be carried out by trained practitioners and the results can often be subjective. As investigators and certainly those who regularly conduct interviews, speaking with staff and colleagues will help give some understanding of who your colleagues are and what is going on in their lives. Speak to managers and general staff regularly, in the canteen, in the corridors and at social functions, not to pry but to know the people behind the operative.

One's narrative, or story, contributes immensely to one's identity. How someone sees themselves relates directly to whether they would justify committing a criminal act against their company. If the organisation were able to manage the justification element of fraud, together with the opportunity element, they might be better placed to manage that

***If the organisation were able to manage the justification element of fraud, together with the opportunity element, they might be better placed to manage that previously unseen threat.***

previously unseen threat. Like any counter fraud activity this is not a silver bullet, there would need to be a concerted programme of education and training for all staff to navigate these life events and support, counselling and assistance for those who are experiencing problems currently. While the associated costs of this would depend on a multitude of factors about level of service and method of delivery, the sums involved in public sector fraud are such that even if each agency invested a fraction of the savings made and a system of shared and combined services were adopted there is real potential to reduce the amount of public money lost to fraud.

Understanding the workforce and being familiar with their position and opportunities to commit fraud along with the associated services of support and programmes of diversion, could mean that any negative changes in a person's lifestyle pressures can be factored into the risk assessments and counter-fraud policies to protect the organisation's assets. People who commit fraud are people first, and fraudsters second. Timely and appropriate intervention can prevent many people turning to fraud. <sup>1</sup>

## References:

- Association of Certified Fraud Examiners (2018) Report to the Nations. ACFE available at <https://s3-us-west-2.amazonaws.com/acfe-public/2018-report-to-the-nations.pdf> Last accessed January 2020
- Cressey, D. (1973) *Other People's Money: A Study in the Social Psychology of Embezzlement*. Montclair, N.J.: Patterson Smith.
- Curtis, L.A. and Burns, A. (2018) *Unit Costs of Health and Social Care 2018*. Project report. University of Kent. Canterbury. Available at <https://doi.org/10.22024/UniKent/01.02.70995>. Last Accessed January 2020.
- Ellwood, C.A (1912) Lombroso's Theory of Crime. *Journal of the American Institute of Criminal Law and Criminology* Vol. 2, No. 5 pp. 716-723. Northwestern University Pritzker School of Law: Chicago.
- Farrer, J.A (2019) *Crimes and Punishments: Including a New Translation of Beccaria's 'Dei Delitti e delle Pene'* Good Press: Glasgow.
- Gee, J. Button, M. Brooks, G. (2010). The financial cost of UK public sector fraud: a less painful way to reduce public expenditure. McIntyre Hudson: London. Available at [https://www.researchgate.net/publication/277053555\\_The\\_financial\\_cost\\_of\\_UK\\_public\\_sector\\_fraud\\_a\\_less\\_painful\\_way\\_to\\_reduce\\_public\\_expenditure](https://www.researchgate.net/publication/277053555_The_financial_cost_of_UK_public_sector_fraud_a_less_painful_way_to_reduce_public_expenditure). Last Accessed January 2020
- Greene, R. L. (2000). *The MMPI-2: An interpretive manual* (2nd ed.). Allyn & Bacon.
- Hathaway, S.R, McKinley, J.C (1940) A multiphasic personality schedule (Minnesota): Construction of the schedule. *The Journal of Psychology*, Taylor & Francis
- Sibieta, L. (2018) Seven charts on the £73,000 cost of educating a child Institute of Fiscal Studies. Available online at <https://www.ifs.org.uk/publications/13710> Last accessed January 2020
- Taylor-Whiffen, P (2019) *The lowdown on employee fraud*. Natwest: London. Available from <https://www.natwestbusinesshub.com/content/the-lowdown-on-employee-fraud> Published: 24 January 2019 Updated: 27 November 2019. Last accessed January 2020
- Williams III, F.P. McShane, M.D (2010) *Criminology Theory: Selected Classic Readings*. Routledge: New York.
- Wolfe, D.T., Hermanson, D. (2004) The Fraud Diamond: Considering the Four Elements of Fraud. *CPA Journal* 74.12: 38-42.
- Youngs, D. Canter, D.V (2012) Narrative roles in criminal action: An integrative framework for differentiating offenders. *Legal and Criminological Psychology*, Wiley Online Library. Available at [https://www.safelylit.org/citations/index.php?fuseaction=citations.viewdetails&citationIds\[\]=citjournalarticle\\_372291\\_20](https://www.safelylit.org/citations/index.php?fuseaction=citations.viewdetails&citationIds[]=citjournalarticle_372291_20)





# They're not loveable rogues. They're ruthless criminals.

Some of us will have fond memories of BBC TV comedies such as *Porridge* or *Only Fools and Horses*, where endearing characters like Norman Stanley Fletcher and Derek Trotter encouraged us to laugh at their questionable endeavours.

However, National Trading Standards (NTS) investigators can show you a very different – often sinister – face to these crimes in 2020. As we and local Trading Standards colleagues close in on fraudulent and criminal activity, criminals are forced to adapt and often resort to new, more advanced techniques. Officers are seeing scams and fraud become more advanced, in many cases being operated by organised criminal gangs, while developments in technology enable criminals to adopt increasingly sophisticated targeting techniques to prey on some of the most vulnerable in our society – or people particularly susceptible to scams.

An older neighbour who lives alone who responds to lottery schemes that arrive by post, whose address has in fact been targeted by multiple clairvoyant scams. A 17-year-old who has just passed their driving theory test and eagerly books their practical test online. An avid music fan desperate to see their favourite artist perform, searching high and low for tickets. A refugee who is looking for work to send money home to their family. All are being targeted by ruthless criminals looking to line their pockets.

## Doorstep crime and modern slavery

Organised crime groups are playing an increased role in doorstep crimes and other scams. There are gangs operating in the UK who target vulnerable men from deprived areas – such as those with alcohol and drug dependencies, homeless people or immigrants – to carry out substandard, unnecessary repairs and so-called improvements to people's properties. These workers are often entrapped into cycles of escalating debt, paid far less than the minimum wage, if at all, and work in unsafe conditions.

Recent estimates from the National Crime Agency (NCA) have identified at least 181,000 people involved in serious and organised crime in the UK – more than twice the strength of the regular British Army. While the NCA leads on serious and organised crime within the UK, more cross cutting issues are straying into Trading Standards' area of expertise.

Author:  
**Lord Toby Harris,**  
Chair of National  
Trading Standards



Recent high-profile cases have illustrated the dangerous approaches sometimes taken by criminal gangs to smuggle immigrant workers into the country. The numbers are thought to be growing: referrals of potential victims of modern slavery increased by 36% in 2018 compared with the year before – a rise of more than 80% since 2016.

Sometimes shoddy or unsafe maintenance and improvement work, from poorly patched driveways to overpriced, ineffective solar panels, is carried out by enslaved labourers. Then unsuspecting householders – often older people or people living with a disability – are bullied into paying hugely inflated prices, often losing their life savings in the process. Would the kind of people who would risk lives by transporting human beings in an airless shipping container think twice about frogmarching a vulnerable householder to a cash machine?

The crimes have two sets of victims: the enslaved or exploited workforce and vulnerable householders.

## Mass marketing fraud

Of course, organised criminal activity isn't just on doorsteps. Our NTS Scams Team tackles fraud that comes through the letterbox too. Each year, mass marketing mail scams, which often target the vulnerable or disadvantaged, cause between £5 billion to £10 billion worth of harm to UK consumers. Many criminal groups run their fraudulent activity from overseas but their mailings land in UK letterboxes, making enforcement particularly complex. To help protect consumers, the NTS Scams Team works to disrupt scam mail sent by fraudsters – such as fake lotteries, misleading prize draws and clairvoyant scams – to help reduce instances of scam mail from reaching people's letterboxes. By working in partnership with agencies both in the UK and internationally, we have been able to identify scams and disrupt criminal groups' activity to the extent that some organisations have stopped sending scam mail to UK addresses altogether.

In 2018/19 alone, more than 1.5 million mailings were stopped by the team. So it's no surprise that criminals are trying to find ways around the preventative measures already in place, such as disguising the mail, or sending from the UK into foreign jurisdictions and vice versa. International collaboration has ensured that mailings destined for the UK have been stopped in a number of different countries including Singapore, the US, Canada, Switzerland and Belgium.

Intelligence gathered by NTS investigators also resulted in high profile prosecutions and asset seizures in the USA. We have our own not-so-secret weapon too – over 350,000 people have signed up to be Friends against Scams. They receive online or face to face training, improving their resilience against becoming victims of scams and helping identify suspected criminal activity.

Previous victims of scams can also graduate to become a Scam Marshall and provide NTS with useful intelligence about the criminals' latest ruses. A number of responsible utility companies recently signed up to Utilities Against Scams and recruit SCAMchampions from among their workforce. Uniquely placed as they have daily contact – face to face or over the phone – with their customers, they can support those who may be targeted by unscrupulous callers, spot tell-tale signs and act upon them.

Some local authorities, other public bodies, banks, consumer-facing businesses and community groups also support Friends against Scams by encouraging employees and volunteers to undertake e-learning modules which help them to spot potential victims of scams and give them tools to make their communities more resilient. You can find out more about this successful initiative at [www.friendsagainstscams.org.uk](http://www.friendsagainstscams.org.uk)

### Online crime and fraud

Online crime is not new, but it continues to become increasingly targeted and large numbers of people are at risk – including those who consider themselves to be tech-savvy and vigilant around scams.

Examples include:

- 'Copycat' adverts on social media – the popularity of social media sites as selling platforms allows counterfeiters to increase their reach when selling unsafe, counterfeit or stolen goods by targeting time-poor consumers with lookalike adverts in their feeds.
- 'Copycat' government websites – which are often designed to mimic government services – many of which are free – and charge a premium. Examples include renewing driving licenses, applying for new passports, renewing European Health Insurance Cards, tax returns and other government services.
- Misleading search engine adverts – a rising trend of misleading adverts appear at the top of search engine results which encourage users to call them for services like technical support and IT issues. With more searches being made by smartphone, users act on these adverts immediately and call through to fraudulent phone lines.
- Subscription traps – often linked to free trials, these scams lure consumers with enticing offers before locking trialists in to costly repeat payments.
- Connected devices and the 'Internet of Things' – increasing numbers of household consumer devices – including smart speakers, connected TVs to internet-connected ovens and other home appliances – connect to the internet by default, increasing the risk of devices being exploited to cause consumer harm. Sometimes users may even fail to change their passwords from the factory setting, creating an easy opportunity.

More recently, we've seen warnings issued to consumers trying to make online donations towards the efforts to tackle the bushfires in Australia. Scammers often capitalise on such spikes in payments, shamelessly exploiting people's goodwill and diverting funds from charitable causes.

Another example was seen when consumers who were left out of pocket by Thomas Cook collapsing applied for refunds. Similar warnings were issued about criminals setting up fake Thomas Cook refund websites to collect consumers' bank details.

### Effective performance despite constrained resources

National Trading Standards, alongside our Trading Standards partners at local authorities across England and Wales, continue to clamp down on criminals and generate value for the taxpayer. Funding for trading standards and consumer protection work has been halved in the last decade, resulting in a similar reduction in the number of Trading Standards Officers. The average spend per head of population in 2017 was £1.69 PER YEAR – that's the equivalent of ½ a cup of coffee in a London coffee shop or three own brand toilet rolls! For this budget, local trading standards operations are collectively tackling over £15 billion in consumer and business detriment, supporting legitimate local businesses from being undercut by dodgy dealers and con artists, and protecting the most vulnerable in our communities from scams and exploitation by criminals.

Funding invested in Trading Standards produces consistent results. For our own organisation, every pound received by National Trading Standards has delivered around £12 of benefit, including preventing over £800 million in consumer detriment since we were established six years ago. As acknowledged by the National Audit Office, the model of national commissioning from local authority-based teams delivers results. For us to continue to disrupt, investigate, prosecute and keep people safe, all parts of the system need to be adequately resourced.

There are many other aspects to NTS work and to consumer protection. Preventing £92.8 million worth of detriment by stopping unsafe and non-compliant goods from entering the UK supply chain. Serving prohibition notices on incompetent or unscrupulous estate agents. Prosecuting retailers caught selling knives to under 18's. Putting the brakes on the old-school crime of car mileage clocking.

Our work is just one small element of trading standards and consumer protection activity. The bulk of trading standards work is carried out by local authorities while Citizens Advice, the Advertising Standards Authority, the Competition and Markets Authority, the Financial Conduct Authority and many other organisations – all play crucial roles to help protect consumers, businesses and communities from scams. There is more to do, much more, and we remain committed to protecting consumers, raising awareness, disrupting and combating criminal activity and prosecuting the criminals themselves in the new decade.

A rose-tinted view of Jack-the-lad rogues and hapless incompetent dodgy dealers, forged by TV series from three decades ago, shouldn't get in the way of protecting ourselves, friends and neighbours from the altogether more unpleasant and unscrupulous 2020's criminal.

**An in-depth look at mass-marketing fraud can be found on page 16**





# Mass marketing fraud: susceptibility and risk

**You have almost certainly received letters informing you of prizes you won, e-mails prompting you to click on certain links or to reply with your personal information, or calls asking you if you were involved in an accident. Of course many of these letters, emails and calls come from criminals intent on stealing your money, identity or data. Often these attempts are easy to spot, but clearly some people must fall prey or criminals would not continue to attempt them.**

According to a report by the Home Office, approximately 1 in 17 adults in England and Wales were a victim of fraud, and about 50% of businesses experienced fraud. The cost of fraud is estimated to be around £110 billion a year, roughly equal to the cost of the NHS in England.

There are many types of frauds, ranging from pension scams, identity theft, cyber fraud, credit and debit fraud, to name but a few. One type of fraud which has received a lot of attention is mass marketing fraud (MMF). MMF refers to any type of fraud scheme that employs one or more mass-communication techniques or technology, including the internet, to present fraudulent solicitations. Overall, MMF fits into three categories: advance fee fraud schemes; bank and financial account schemes; fake investment opportunities.

Advance-fee fraud schemes are a type of scam that is based on the concept that the victim is promised a substantial benefit but must first pay a small amount in order to access that benefit. A report by the RAND corporation suggests that Mass Marketing fraud costs each UK victim an average of almost £7,000 during their lifetime, with about 1% of victims losing more than £100,000. Scammers, moreover, target everyone; they do not discriminate between people. What seems to impact the likelihood of falling prey to scams is the level of engagement, the type of scam, and method of contact.

## Who is behind these types of scams?

Unlike many other crimes, fraud is increasingly

transnational, making it very difficult to identify the scammers, let alone bring them to justice. For example, a call appearing to come from a domestic telephone number may in fact originate from a call centre in India or Nigeria. Perpetrators are adaptive, quickly moving from one region to another as easily as shifting from one tactic to another; appearing to represent government bodies, technology scams, or asking if you have been involved in an accident and wish to claim compensation. Some advance fee scams are well known, with '419 scams' linked to scams originating from Nigeria (419 is the section of the Nigerian criminal code outlawing the practice) and '876 scams', based on the local telephone area code in Jamaica where some calls have typically originated. However, these scams have a presence in all regions of the world, including the UK.

## Our Research

In a recent article, 'Call to Claim Your Prize: Perceived Benefits and Risk Drive Intention to Comply in a Mass Marketing Scam', we, along with our co-authors, examined factors that we suspected increased risks of falling victim to mass-marketing scams through analysis of previous cases and experiments. Some of our findings question common assumptions about fraud. For example, we didn't necessarily see older adults at greater risk of advance-fee scams pitches.

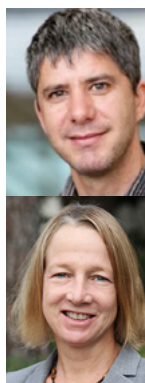
In order to study consumer susceptibility to mass-marketing scams we reviewed 25 "successful" mass-marketing scam solicitations obtained from the Los Angeles Postal Inspector's Office. We analysed the content of these solicitations and noted commonalities. For example, many of them included some type of familiar brand name to increase their credibility and authority.

Scammers frequently use persuasion techniques to increase trust and motivation in victims: spoofing area codes to increase recognition or familiarity; impersonating well-known legitimate businesses to evoke authority; adding pressure such as "act now" or creating illusions of scarcity to prompt action by victims.

Some of the scam letters analysed were quite colourful and included images of money, prizes and 'winners'. Others were much more businesslike and included legal-sounding text in an effort to increase credibility.

Based on this review we developed a prototype letter. We created four versions that manipulated authority (we obtained your name from Costco or

Authors:  
**Dr. Yaniv Hanoch**,  
*Associate professor at the Business School, University of Southampton and*  
**Professor Stacey Wood**, *Professor of Psychology, Molly Mason Jones Chair in Psychology, Scripps College, CA, USA*



# VERIFICATIONS SERVICE

✓ Identity of declared winner

**VERIFIED**

✓ Protected service proposed

**VERIFIED**

✓ Your first prize: a valuable package

**VERIFIED**

✓ Your second prize: monthly income of \$ 1,600.00 for six months.

**VERIFIED**

✓ Your third prize: the bank check for \$ 14,400.00

**VERIFIED**

✓ Letter of confirmation from the President of the A.P.M.E. Board of Directors

**VERIFIED**

✓ Official certificate enclosed for more than \$ 24,000.00

**VERIFIED**

Target versus “from our vendors”), and scarcity (“act by 30th June” versus “respond soon”) in order to determine what persuasion factors motivated consumers to respond or refrain from responding.

In one experiment we asked 211 participants to read a one-page solicitation, informing the consumer they are “already a winner”, and asking them how likely they would be to contact the “activation number”. We found many participants (48%) indicated some willingness to contact the “activation number”. As a group these consumers tended to have fewer years of education and be younger than non-responders. These participants tended to rate the risks of contact as low and the benefits as high.

In a second experiment, we increased the risk by adding an “activation fee”, a common tactic in mass-marketing scams. Even with an activation fee, 25% of our sample indicated some willingness to contact the number provided. Similar to the first experiment, individuals who rated the solicitation as having high benefits were more likely to signal intention to contact.

Our research indicated that what consumers pay most attention to appears to be their assessment of the benefit offered and the perceived risk of responding.

## Why do individual respond to scams?

We asked individuals in our studies about risks involved in these solicitations. Most (about 60%) identified the possibility that these solicitations are likely to be a scam. However, they viewed the opportunity as potentially beneficial as well. In some ways, these advance fee scams may act as unofficial lotteries, with a low cost of entry and a high chance of failure. However, while consumers are wary, they don't completely write-off the possibility of a big payoff.

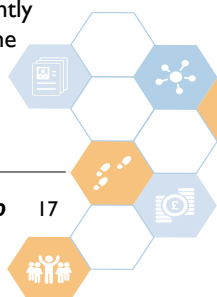
Unfortunately, consumers overestimate their ability to “shut it down” if the offer turns out to be a scam. Once potential “suckers” are identified by responding to any of these letters, phone calls or clicking on fraudulent ads, they may be relentlessly targeted by phone, email and mail. After a response, their names are sold to other scammers, who view the individual as a good target for further attempts. In other cases, victims are groomed to become “money mules” for the scammers, assisting with money laundering in exchange for the ability to continue to be involved in the “sweepstakes” or to recover losses from the scam.

## What to do about scams?

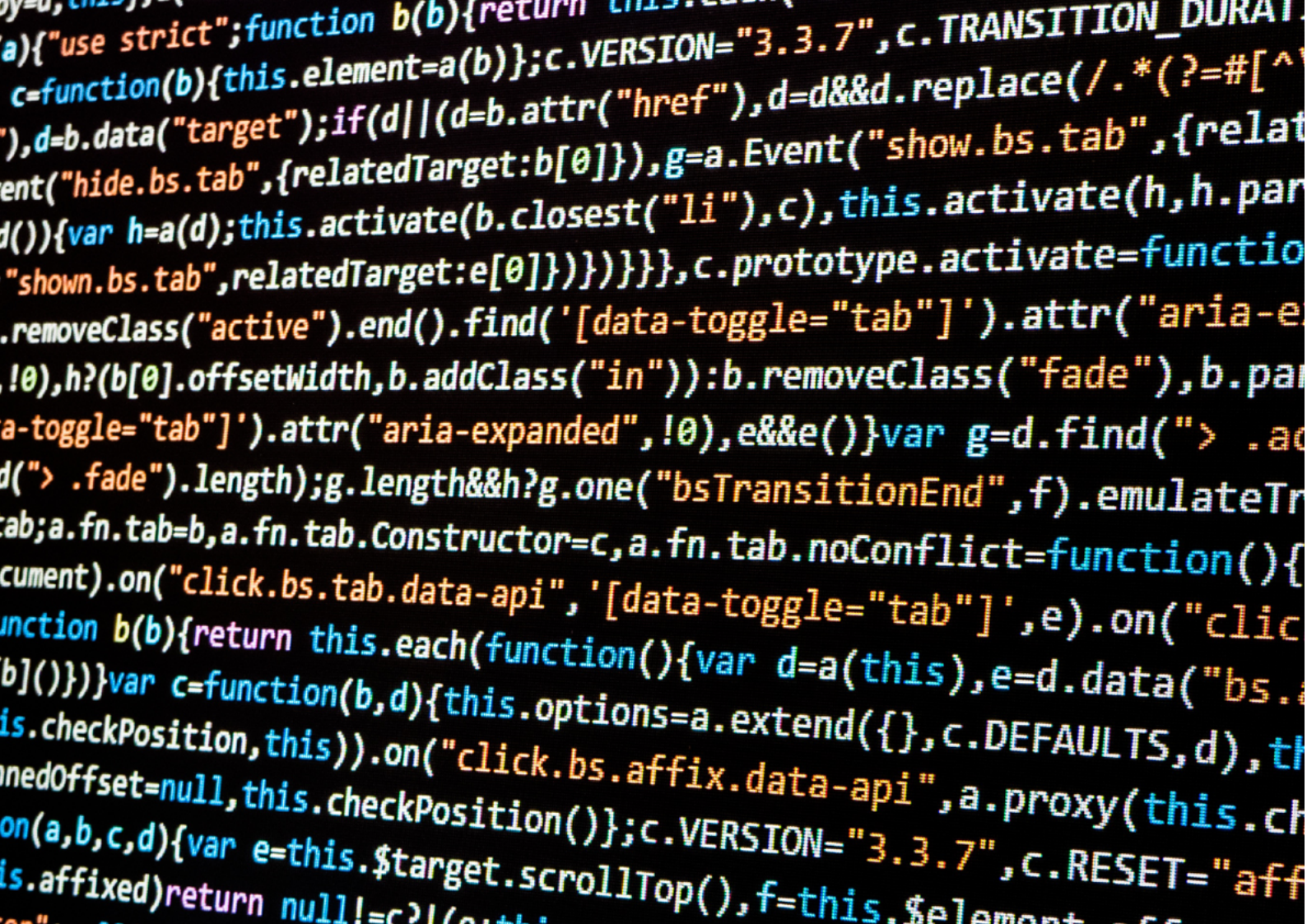
In terms of individual behaviour, there are some apps being developed to assist in screening calls. It is also important to resist clicking and responding to suspicious material in any way.

Initially we thought that scammed consumers would be those who superficially processed the information and “missed” red flags. We suspect it is actually the opposite, that is consumers who quickly identify a solicitation, as a risk and dispose of it without spending much time on the scam are less vulnerable than those that open the email or letter. These are just a few suggestions.

Given the prevalence and financial, emotional and health costs of fraud, there is an urgent need to develop better means to reduce the rate of victimhood. These could only be achieved, we believe, by uniting efforts from a wide spectrum of sources. Law enforcement agencies, advocate groups, government departments, and academics need to urgently work together to find better means to tackle one of the leading crimes of the 21st century. <sup>1</sup>







# Preventing and detecting fraud using machine learning

**Machine Learning (ML) is a powerful tool, providing the ability to learn from data without programming explicit instructions.**

**T**raditional rule-based systems are manually created to define a set of 'rules' that indicate potential fraud. An example of a rule would be to flag a transaction if it is above a threshold and from a location that the customer hasn't bought from previously. This, however, relies on having the capability to define those rules in order for the detection to happen - knowing what to look for. In the case of payments, these rule-based systems are now creaking at the seams as

the number of payments transactions has grown dramatically, driven by:

- Increasing numbers of mobile customer payments;
- Customers moving from cash-based payments to digital payments;
- Instant payments requiring payment transactions to be settled in a matter of seconds.

This tsunami of payments volumes means that there is an even greater opportunity for fraud to take place. In this article we look at the advantages of ML and why it is now a vital tool for both preventing and detecting fraud.

Author:  
**Tamsin Crossland,**  
Icon Solutions



## How Machine Learning helps

Rule-based systems are struggling to keep up in this open, digital world. Through ML, however, computers can identify patterns, imperceptible to humans, in massive datasets, running to millions or perhaps billions of data points. These can be used to automatically detect new fraud patterns.

ML will 'train' a model from data, which can then be applied to a business problem, such as fraud detection. This involves feeding in sets of data to build the model, for example loading data from transactions where some are known to be legitimate and some fraudulent and by telling the model which is which. The model looks for correlations between user behaviour and the likelihood of fraud by comparing the many variables in the known fraudulent and known genuine transactions.

The diagram (right), a correlation matrix, gives a graphical example of how data can be analysed prior to training the model. In this case there were 28 variables in the data set, each shown on the axis with a V number. These variables could be, for example, the value of the transaction; the location from which it was made; the type of product purchased; information known about the user or indeed any other data captured as part of the transaction.

Looking at the bottom row (fraud) of the correlation matrix, it is possible to identify which features are most influential:

- the darker blue elements are positively correlated; if V2, V4 or V11 have a higher value it is more likely that the transaction is a fraudulent one.
- the darker red ones are negatively correlated, so lower the value of V3, V12 or V14 the more likely that the transaction is a fraudulent one.

### Using the outcomes

So far we have looked at the training of the model, but of course, during training, the model already knows which transactions are fraudulent as they are labelled. After training it can then be applied to determine whether future transactions are likely to be fraudulent or not.

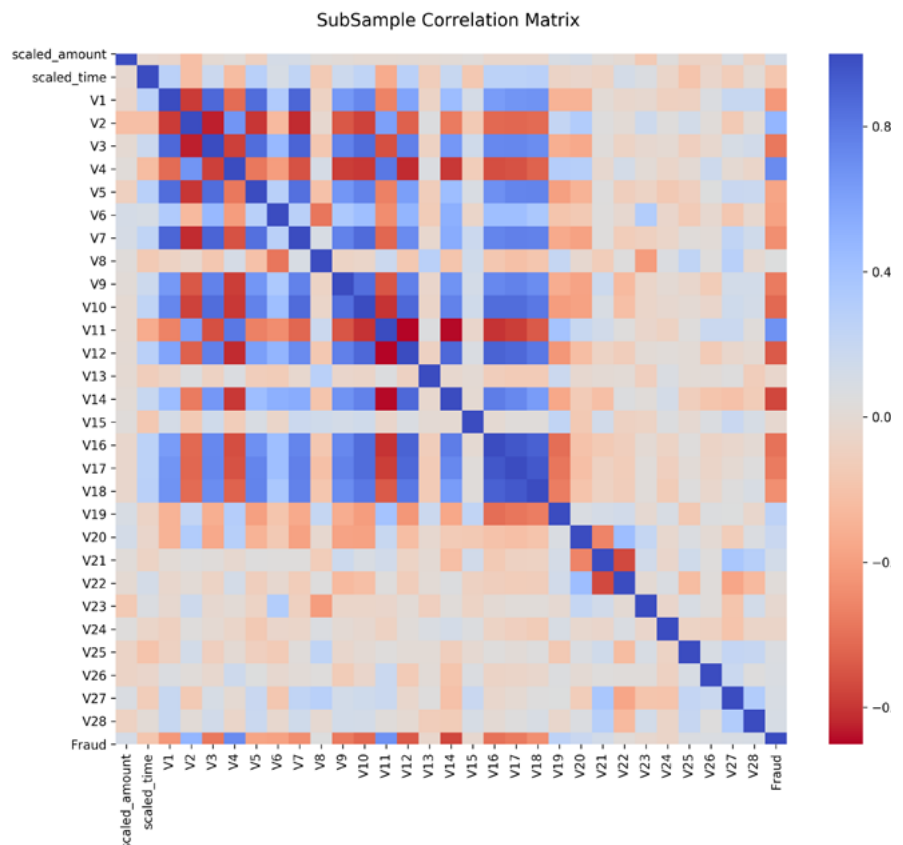
### Positively false, or a false positive?

ML is certainly not perfect. Output will include correctly-identified fraudulent transactions, or 'true positives', but may also incorrectly classify a transaction as fraudulent, when

actually it was genuine, known as 'false positives'. The model may also miss some fraudulent transactions ('false negatives').

In the case of 'false positives' this can lead to negative experiences for customers; most people don't like being told that they are being flagged as a potential fraudster! Depending upon business requirements, an organisation may prefer to tolerate more fraud to avoid the negative customer experiences.

Key to a well-functioning model, therefore, is having sufficient data for the training stage and that the data used is of a high-quality. Given that the proportion of transactions that are fraudulent is relatively low, compared to those which are



genuine, this can be a challenge. There are, however, analytical techniques which can be used to generate better-balanced data sets in order to train models and attain a high degree of accuracy in detecting fraud in transactions.

### The potential is clear

ML offers the potential to detect new fraud patterns as they emerge and to handle the tsunami of digital payments that we are seeing as people around the world make more and more digital payments. ML can pick up the baton of applying AI to detect fraud that rule-based systems have successfully achieved over the past 30 years.

**For more information on the use of artificial intelligence to combat public sector fraud see the article on page 31 regarding the work of the International Public Sector Fraud Forum**







TECAs 2019 Winners from the public and private sectors

# Tackling Economic Crime Awards

The winners of the first-ever Tackling Economic Crime Awards (TECAs) were announced on 9th December 2019 at the Sheraton Grand London Park Lane. Some 250 representatives from the financial crime sector were in attendance. Guests were welcomed with drinks, dinner and entertainment to celebrate their achievements with their colleagues, clients, peers and the judges at an unforgettable gala dinner.

Recognising who is good at tackling economic crime is not an exercise that is done for the sake of it. Those who tackle economic crime play an important role in protecting people and companies and in supporting economies. As such so much work is undertaken under the radar it is largely unheralded and its importance diminished. Worse still it is not always easy to show that you are doing a good job. Recognising those people, teams, initiatives and companies who excel then is important, very important, just as it is vital that the process for achieving that is credible. This is why the TECAs have attracted so much attention and will continue to do so. To be judged by a fair, transparent process, by the leading peers in the sector is the ultimate accolade.

### Why are the TECAs different?

These awards are different. The judges are nominated by the leading associations and groups involved in tackling economic crime, representing the elite of the sector.

Author:  
**Professor Martin Gill**, founder of the TECAs

All the judges agree to follow an ethics policy and mark independently, using criteria which are published. On every marking sheet they have to declare any conflict of interest.

There is an ethical sponsorship policy too. The overall sponsor Alti-ABM supported this initiative knowing none of its staff could enter. In fact Ian Watson and Rob



Sinclair from Alti-ABM said they supported it because they supported the principle of an awards committed to independence and transparency. Similarly, Cifas sponsored the menu and International Security Expo sponsored the drinks reception showing their support.

If you win a TECA it is because you are very good.

### The awards presentation

All the winners are announced for the first time on the night. No-one knows in advance, not even the judges, which generates a lot of excitement.

There are different categories reflecting the broad range of areas those involved in economic crime work in. It was extremely competitive as the awards are open to anyone working in the UK, public, private or third sectors and, of course, who excels.

### The 2019 awards

All the categories are competitive, the judges made that point. In fact only those who scored above a threshold were finalists; you have to be good just to be shortlisted. The winners were:

*Outstanding Manager or Director:* Simon York – Fraud Investigation Service, HMRC

*Outstanding Team:* The DCPCU (Dedicated Card & Payment Crime Unit)

*Outstanding Consultant:* Graydon Business Intelligence Unit – Graydon UK

*Outstanding Customer Service Initiative:* Cyber and Economic Crime Awareness Service – Greater Manchester Police

*Outstanding Training Initiative:* James Jenkin – Serious Fraud Office

*Outstanding New Product:* The Paybase Risk Suite – Paybase

*Outstanding Partnership:* Hertfordshire Shared Anti-Fraud Service

*Outstanding Investigator:* DC Adele Shallcross – Avon & Somerset Constabulary

*Outstanding Young Professional:* Dave Laramy – Capital One UK

*Outstanding Female Professional:* Claire Jenkins FCCA, Integrity & Enforcement Unit – Companies House

*Outstanding Male Professional:* Russell Chinn – Metropolitan Police, DCPCU

*Outstanding Prevention Initiative:* Santander UK – APP Scam Prevention

Our judges were: Dr. Stephen Hill, Association of Certified Fraud Examiners (ACFE); Mark Cheeseman, Cabinet Office; Mike Betts, Cifas, Mark McAuley, CIPFA; Commissioner Ian Dyson QPM, City of London Police; David Clarke, Fraud Advisory Panel; Stephen Dalton, Insurance Fraud Bureau; Robert Brooker, London Fraud Forum; Tom Keatinge, RUSI; Katy Worobec, UK Finance and; Professor Mark Button, University of Portsmouth.

The North East Fraud Forum also supported the TECAs.



Professor Michael Levi, winner of the Lifetime Achievement Award


### Lifetime Achievement Award: Professor Michael Levi

There is always an interest across the sector as to who wins the Lifetime Achievement award. There is no doubt the winner proved a popular choice. It was Professor Michael Levi. Many will know of Mike's achievements; they are considerable. He has been not just the UK's but arguably the world's leading scholar on the study of economic crime; his book *The Phantom Capitalist* has been a 'must read' for scholars and professionals alike. Since the 1970s he has played an important role in the development of economic crime policy. During his career, Michael has contributed to the Prime Minister's Strategy Unit, the Council of Europe and the European Commission – to name just a few.

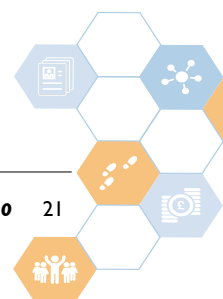
### The awards in 2020

The 2020 awards are already being planned. Entries will open on 1st May 2020 but you can register your interest now. We encourage you to take the time to nominate those you think are deserving for a TECA.

Hopefully you too will consider it a great honour to be able to play a part in recognising the achievements of outstanding players in this sector.

[www.thetecas.com](http://www.thetecas.com); [enquiries@thetecas.com](mailto:enquiries@thetecas.com). 

**To be judged by a fair, transparent process, by the leading peers in the sector, is the ultimate accolade.**





---

# Award-winning collaboration

## How the Hertfordshire Shared Anti Fraud Service used a £300,000 funding bid to detect and prevent more than £18m in fraud and error.

In December 2019 the Hertfordshire Shared Anti-Fraud Service (SAFS) won the award for 'Outstanding Partnership' at the Tackling Economic Crime Awards. Sitting with the team in a room full of counter fraud professionals, knowing that we had won this award, was possibly the proudest moment of my career. The other finalists in our category were:

- Bank Signature Forgery Campaign and All-Party Parliamentary Group on Fair Business Banking;
- Charity Commission for England and Wales and Fraud Advisory Panel;
- Insurance Fraud Prevention Partnership – Hastings Direct and BAE Systems;
- National Fraud Initiative (Cabinet Office) – Synectics Solutions and QBE;
- Nationwide Branch and Support Team; and
- Statutory Accounting and Corporate Structure Fraud Project Team – Companies House, Cabinet Office, HMRC and Insolvency Service.

And they were just the finalists. To say I was chuffed would be a considerable understatement.

### Foundation and first steps

SAFS was established in 2015 following a year of project planning and implementation, led by an enlightened group of Chief Financial Officers. It is a true partnership. The aims of the service were agreed early on and have remained largely unchanged; they just make sense and help us focus our efforts to:

- Ensure ongoing effectiveness and resilience of partner anti-fraud arrangements;
- Deliver financial benefits in terms of cost savings and/or increased revenue;
- Develop a FraudHub working in partnership with the Cabinet Office and others;
- Improve the reach into new areas of fraud risks across all partner services;
- Develop services which can be shared for mutual benefit; and
- Continue to develop SAFS as a recognised centre of excellence.

Thinking back to March 2015, when the SAFS Team was set up, I remember arriving at what would become our main

office in Stevenage on a cold, dark morning; it isn't always cold and dark in Stevenage! At that time we didn't have an office, just some floor space in the County Council offices. There were no staff (except me), no systems, policies or equipment, let alone desks, laptops, notebooks or printers. The first few weeks were spent recruiting, procuring systems, desks, secure storage and working out where the canteen was. We then had to train new staff, develop processes and work through numerous data access and sharing agreements. Being a partnership between six councils meant we also had to deal with IT, data protection and security, human resources and legal teams for each authority.

It may have taken 12 months to build our first data-hub, my hair may have gone grey and fallen out in the process but, the end result wasn't really the data-hub itself, it was the amazing relationships we developed with officers across all six councils. By working with these teams and staff we had built up a level of trust and understanding that would not have been achieved otherwise: it's still as strong to this day.

### Expansion

SAFS has grown considerably, with Luton Borough Council and a number of social housing providers joining the original partners: Hertfordshire County Council; Hertsmere Borough Council; Borough of Broxbourne Council; East Herts District Council; North Hertfordshire District Council and Stevenage Borough District Council.

The team has also increased, from 9 to 18, with additional posts created for data analysts and financial investigators added, all hosted and employed as one team by Hertfordshire County Council. As our staff are not just fraud investigators, managers or analysts, all job titles within SAFS use the term 'counter fraud'. The role of all staff is to provide services that include training, awareness, 'fraud-proofing' of policies and processes, and publicising anti-fraud initiatives. All of these things help to foster an anti-fraud culture in every organisation we work with.

Suspected fraud is reported directly into the service by public and staff alike using our on-line reporting system or using our hotline. All partner websites are linked to our own. This provides a simple and effective way for people to find out what the Partners are doing to prevent fraud and how fraud can be reported.

We make extensive use of social media to deliver anti-fraud campaigns including the International Fraud Prevention Week held last year in November 2019 which saw hits on our website quadruple that month.



*Teamwork: The Hertfordshire Shared Anti-Fraud Service celebrate their Tackling Economic Crime Awards win in December 2019*

## Using data

SAFS has the ability to bring together data, knowledge and intelligence from a wide variety of sources and to share this to enhance investigation opportunities and improve prevention.

One of the key aims for SAFS was to create a fraud hub using data from our partners and third parties to prevent fraud, detect fraud early and help recover fraud losses. This has been an ongoing project with the creation of the data hub initially.

Now, we have a much broader approach to the fraud hub concept, not just focused on data or how we analyse it, but a much wider remit considering what data we need, why we need it and how we can share this across the Partnership to prevent fraud occurring. This is what wins awards.

## Challenges and Successes

Oversight of the service is provided by the SAFS Board, comprising Chief Finance Officers from the partners. SAFS Champions are in place in each council, and our regular reports to audit committees ensure that SAFS delivers its own service plan and each partner's anti fraud plans every year, whilst delivering a clear return on investment. SAFS has to meet its Key Performance Indicators and keep the Board and the team focused on the aims of the service. One challenge, with its limited resources, has been to meet

the additional needs of services across local authorities that may not previously have been aware of the risk of fraud. Once explained it's no surprise that new areas of fraud have come to light, creating new and 'interesting' pressures on the service.

At the end of our fourth year SAFS received more than 4,000 reports of suspected fraud. Of those, we have closed over 1,800 investigations, resulting in more than 60 successful prosecutions, 120 other disposals (including staff dismissals, cautions and fines), recovery of more than 80 social homes and identified or prevented more than £18m in fraud against the public purse.

Building SAFS into what it is today has been a great privilege. The team are simply the best, with an excellent mix of skills. They thrive on the variety of work, which includes everything from staff misconduct and blue badge abuse to false insurance claims, housing fraud, council tax and business rates fraud, adult and children's care fraud, and fraud in schools and contracts.

Not bad for what was a two year pilot paid for by a successful bid for £300k as part of the Ministry of Housing, Communities and Local Government Counter Fraud Fund in 2014.

***A list of all Tackling Economic Crime Awards 2019 winners can be found on page 20***

## Collaboration

SAFS isn't just limited to its own partnership. We will work with anyone where there is a lawful gateway to do so and that will assist any one or all of our partners:

- We work closely with the DWP on housing benefit and council tax fraud and SAFS was part of the successful joint working pilot in 2016/17
- We have arrangements in place to work with Hertfordshire Constabulary with the police assisting in arrests, searches of premises and providing use of police interview rooms for our more challenging interviews
- Working with Trading Standards and Consumer Protection teams has often been helpful in creating disruption where normal methods of investigation are ineffective
- Other Councils and third party providers are able to provide specialist skills where these are lacking, such as IT for surveillance, and we are always open to creating partnerships that allow us to access and utilise these
- We have contracts and working arrangements in place with a number of public and private sector providers to access data and intelligence





---

# On the right track

**Adam Deane, Head of Business Integrity at Network Rail and member of the Government Counter Profession Board, talks about his counter fraud journey and the part the Profession is playing**

## **A long, long time ago...**

...I was involved in my first investigation into a suspected case of fraud..This involved successfully stopping a multi-million pound attempt to defraud a large IT project in my company.What a buzz!

I was at Railtrack back then - soon to become Network Rail, the organisation that owns, maintains and operates the rail infrastructure for Britain. I was relatively inexperienced

## **And today...?**

I now lead the counter fraud and investigation team in Network Rail and represent the organisation on the Board of the Government Counter Fraud Profession (GCFP).

Like many large organisations overseeing large resources, we are an attractive target for would be fraudsters.This keeps me on my toes with over 40,000 staff to educate on the counter fraud message; counter fraud risk and measuring programmes to oversee, and of course, allegations of fraud to review.

As the workload of the team has grown, we have continued to expand.Team members have a variety of complementary skills, from data discovery and analytics to investigators, from finance and contract specialists to fraud risk assessors.

Over the years we have investigated many intriguing and challenging allegations of fraud - from such things as mandate frauds; ghost working; and contract issues through to an attempted prepayment fraud involving the purported sale of the nation's entire train track to another country!

Previously, as a limited company, we faced a number of these challenges alone, but we are now an arms-length body to the government. Being part of the GCFP has given us access to a whole community of counter fraud and investigation experts, including the counter fraud champions and access



in the world of fraud but, as the allegations came in, I enthusiastically continued on my counter fraud and investigation journey. I set up a confidential reporting line; developed processes and procedures to educate and investigate; engaged with the police for prosecutions and most importantly got full board support for our activities.

The challenge at the time was finding a trusted source of guidance and expertise that covered all the counter fraud activities relevant to our organisation.

to various government department events and conferences. In particular it has allowed us to significantly expand our counter fraud activities in a direction and way which we can now hold up as best practice. This has helped us create our own quality counter fraud strategy tailored to the very specific needs of our organisation, accompanied by a robust fraud response plan. These are rooted in the good practice set out in the Profession Standards and the Counter Fraud Functional Standards allow us to benchmark against other

organisations within the government.

Put simply, the work done through the GCFP has distilled the expertise many of us take a lifetime to learn, into good-to-go quality principles; standards and disciplines, fit for fighting fraud as it is now and as it continues to change.

This has helped form a pan government community of like-minded counter fraud professionals, learning from each other and supporting each other in a job that previously had no professional recognition. As an organisation we can play our part in offering interesting and varied counter fraud careers to that community.

Recently one of my team successfully completed the foundation fraud risk assessment course. As well as now being able to better service our own organisation, this has opened up the prospect of development opportunities for the team member in assisting other organisations in this area.

### **Moving forward...**

You will know the challenges and risks from fraud are ever growing; we need to meet those challenges. You will have seen articles about all the energy that is going into the Profession. The Board is ambitious to continue to develop it, but it is really about the members utilising the Profession to develop their own capability and careers which will really drive forward the counter fraud campaign and help

Author:  
**Adam Deane**, Head  
of Business Integrity  
at National Rail  
and member of the  
Government Counter  
Fraud Profession  
Board



organisations in the fight against fraud.

As a member of the Board we have to ensure that the development of the Profession remains sustainable; while we are all keen to maintain the pace we must also manage expectations. By building the strong foundations now we can be sure that the Profession will have a large and lasting impact.

In the years to come I'm particularly looking forward to the further roll out of the remaining disciplines that will allow members to develop broader skills across a number of disciplines, in addition to deepening their expertise in their normal area of work. This diversity gives flexibility to organisations in their resourcing requirements and encourages new learning opportunities for members.

### **And finally...**

The counter fraud agenda is constantly moving – here are some things I'm currently considering: How do we predict and mitigate new types of frauds? How do we encourage more people to report suspected fraud? How do we better utilise disparate data to discover and prevent fraud? How do we keep the risk of fraud on the agenda of busy managers in our businesses? How do we better work across departments and industries to mitigate fraud? How do we encourage good behaviours in our customer and supplier chains? And so forth...

If you have answers to any of these please get in touch! [✉](#)



*Bristol Area Signalling Renewals and Enhancements (BASRE) is leading to more seats for passengers, improved reliability, and faster and more frequent services – including nearly twice as many between Bristol and London. The six-year project involved disconnecting and removing old equipment from the 1960s and 1970s and transferring signalling to one of the largest and most advanced signalling centres in the country.*





---

# How an apprenticeship can boost your counter fraud career

***With the new Counter Fraud Investigator Apprenticeship coming online in 2020 we explore, in this article, what apprenticeships are and the benefits they bring.***

## **Government commitment to apprenticeships**

An apprenticeship is a high-quality structured programme of learning directly related to an area of work and is delivered by a registered training provider, college or university. Apprenticeships recently changed following the government's commitment of 30,000 apprenticeship starts by 2020.

Employers, rather than training providers, lead the development of apprenticeship programmes to ensure they have relevance in the workplace. All Civil Service departments have been given a legal target of 2.3% of its workforce starting an apprenticeship and apprenticeship learning will be funded through the Apprenticeship Levy.

Most of the learning is on-the-job and apprentices are supported by a mentor and training assessor supplied by the provider. Any off-the-job training may be delivered in the workplace, through day or block release or away from the working environment depending on the apprenticeship chosen.

An apprenticeship programme is a great way to build and develop skills, knowledge and behaviours in the workplace. They are not just for people who are leaving education; they are available to people of all ages and experience levels to help them build or change career.

Learning over this length of time requires a degree of commitment, however. It enables apprentices to learn, practice and reflect in a live environment which leads to knowledge, skills and behaviours that are embedded. An apprenticeship is work-based learning and generally 20% of a working week is for off-the-job learning.

## **Counter Fraud Investigator Apprenticeship**

In October 2019 John Manzoni, Permanent Secretary for

the Cabinet Office and Chief Executive of the Civil Service, announced the launch of the Counter Fraud Investigator Apprenticeship, the 500th apprenticeship approved for delivery by the Institute for Apprenticeships and Technical Education.

This new level four apprenticeship, which takes two years to complete, was developed by HM Revenue and Customs, the Cabinet Office and other partners in the Government Counter Fraud Profession and is based on the Profession Standards. Following the approval, work commenced to put in place the structures to enable the first apprentices to enrol during 2020.

## **Apprenticeships in the Ministry of Justice**

Thomas Hart, from the Ministry of Justice's (MoJ) Counter Fraud and Investigations, is currently completing a Level 4 Business Apprenticeship, balancing his study with a busy counter fraud role. He shares his experiences below.

Thomas' apprenticeship is not counter fraud-specific, as he started before the new Counter Fraud Investigator Apprenticeship (CFIA) was launched. With the new CFIA learners will complete their investigator training as an integral part of their apprenticeship.

**Q: What is your role Tom?**

I am an MoJ Counter Fraud Intelligence and Risk Officer on a fast track apprenticeship (Level 4 Business).

**Q: How long have you worked there?**

Since February 2019.

**Q: What were you doing before?**

I was a store manager for a well-known coffee chain.

**Q: What are the most common types of fraud you deal with?**

I am responsible for the triage of information and allegations received by the team. The referrals mainly relate to suspected fraud against the Legal Aid Agency (LAA), which includes 'client fraud', namely the recipients of Legal Aid

Author:  
**Maria Kenwothy**  
Investigator  
Ministry of Justice  
Counter Fraud and  
Investigations





Thomas Hart is currently completing an apprenticeship while working in the Ministry of Justice Counter Fraud and Investigations teams

when they shouldn't actually be financially eligible, or 'provider fraud' which comes in many forms, but in essence it is when solicitor firms make a personal gain, or cause a loss to public funds through deception. I may also get discreet referrals relating to internal frauds and referrals from other Government partners – anything that is assessed as potential fraud.

**Q: What do you enjoy most about your job?**

I believe I am in a valuable role and there is support in place to develop myself, and really make a difference. I feel instrumental in shaping the counter fraud response for the LAA and wider MoJ. By preventing loss to public funds or by recouping losses, monies protected by counter fraud has a direct impact on public sector spending, for example public service priorities such as the justice system, schools and hospitals. The biggest personal benefit is the flexibility of the working patterns, especially as I have a young family.

**With the new Counter Fraud Investigator Apprenticeship learners will complete their investigator training as an integral part of their apprenticeship.**

**Q: What is the most challenging part of your job?**

It has been quite a steep learning curve, but the complexity of some fraud cases, and getting to grips with the Legal Aid system, has been the most mentally challenging, although in an enjoyable way. While my brain gets a better workout these days, a reduced physical demand and the change in pace from my previous role challenged me in a way I didn't expect. That and the lack of quality coffee on tap!

**Q: What training or experience has been most useful in your job?**

I am currently on a Skills Development Course run by the LAA Capabilities Team. I didn't have this opportunity before and the different modules offered have given me the chance to look to how others view me, how this could hinder or help me progress, how to lead rather than just manage and how to effectively lead through change.

**Q: How has the counter fraud landscape in your area changed in recent years?**

I have only come into this line of work recently, but it seems communication channels are opening up more and more. Raising awareness, sharing knowledge and experience, and working in partnership is the best way to be: proactive rather than reactive.

**Q: What does the Government Counter Fraud Profession mean to you?**

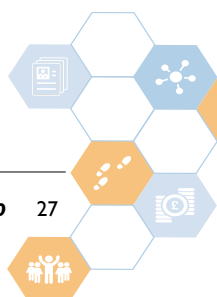
It's a key network channel that aids pro-activity. It also allows me to measure myself against other counter fraud professionals across government. That aside, recognition in any form is always welcomed.

**Q: Where do your energies go outside of work?**

I have two girls, aged 1 and 4. My family are my only focus and I spend all my energy on them. The work-life harmony created by flexible working has facilitated this more than I could ever have expected or asked for.

**Q: What are you most looking forward to over the next year?**

Finishing my apprenticeship and hopefully putting in for an accredited counter fraud specialist course. ð







# Why businesses must be just as alert to fraud as consumers

**T**he threat faced by consumers of becoming a victim of fraud rightly receives considerable attention, not least in the media. But it is not just individual members of the public who are at risk from fraudsters, with businesses just as much at risk of being targeted by them.

I regularly see the impact that a fraud event can have on a business and it can have severe implications, with the money lost preventing that business from investing in growth, whether that is opening new factories or offices or hiring staff. In the most severe cases, the financial impact of the fraud can put the business's entire future in jeopardy and result in redundancies as the business seeks to put itself back onto a financial even keel.

Fraudsters targeting businesses often use similar phishing and vishing tactics to those used on consumers, but there are a few differences to the most common tactics used, which we set out in this article.

Author:  
**Keith Flanagan**  
Commercial Banking  
Business Risk, Lloyds  
Banking Group



The continued threat of fraud to businesses remains very real, with the impact often traumatic to those affected, particularly if it has severe financial implications to them. In my experience businesses that proactively embrace the threat of fraud and take steps to invest in their people, processes and technology to ensure they are not a soft target, are significantly better placed to repel any fraudulent attempts. Fraud should be viewed as a business critical action for any management team. Avoiding being hit by a fraud not only prevents unnecessary trauma, but also means that a business's growth ambitions are neither delayed nor derailed, thereby ensuring a business is best placed to benefit from the UK's long-term economic prosperity.

## **Impersonation fraud – Are they really who they say they are?**

Impersonation fraud techniques are used by criminals attempting to trick businesses and organisations into making payments to fraudulent accounts. Here we look at the

methods of deception used, which can make these scams very convincing.

Impersonation fraud, as the name suggests, is where a fraudster impersonates a genuine person or business and makes a request for their target victim to make a payment to what they do not realise is a fraudulent bank account. Fraudsters will impersonate anyone who they think staff within an organisation will trust to be genuine such as the CEO or a trusted supplier. The aim of the fraudster is to make the payment request seem as genuine as possible, so that funds are sent without a second thought or additional verification checks.

### **Common Types of Impersonation Fraud:**

**Business Email Compromise (BEC)** – is the method by which the vast majority of impersonation frauds occur. Fraudsters will usually prepare for this type of attack by monitoring existing genuine email traffic between an organisation and its suppliers, contractors or employees. They usually do this by hacking into computers using malicious software. This may not be due to a vulnerability in the computer system within the organisation itself, but often fraudsters hack into systems of others they communicate with via email, such as their suppliers or customers, who may not have sophisticated protection in place. It enables the fraudsters to organise a very convincing attack.

The fraudulent email when it is received will be made to look like it has been sent by a genuine supplier, or the organisation's own CEO or MD. It may even come from their email account if they have been hacked and the content of the email will therefore look genuine, containing previous email exchanges and attachments. It will often be timed so that it falls in line with expected payment dates. Everything could look genuine apart from the account number, which will be altered to a fraudulent one.

Of course an email attack could also be supported by advance phone calls by the fraudster trying to gather important information from staff, or they might set the scene for a fraudulent email by impersonating the supplier on the phone, saying to expect an email or otherwise priming staff for the email attack.

This type of attack is often very hard to detect if email is used as a trusted communication method for payment correspondence; after all the fraudulent email has actually come from that trusted person's email address.

**CEO Fraud** – this is a fraud which impersonates a senior person within an organisation. This is a specific type of BEC which has been prevalent in recent times and fraudsters will create the email to look like it's from anyone within an organisation who staff would believe has sent a genuine request.

The request will often state that the payment needs to be made urgently and be labelled as strictly confidential and therefore not to be shared with any other staff due to the sensitivity of the transaction. If the fraudster has done some research on the individual they are impersonating, they will likely send the request when the genuine person is not available due to holiday or meetings. Of course this is all intended to deter the member of staff from questioning the payment or to rush things.

**Invoice Fraud** – in 2019 this was by far the most prevalent scam modus operandi against businesses. It refers to a fraudulent payment which a victim organisation makes in the belief that it is a payment being made to a usual or genuine beneficiary - one which they intended to pay. However, in reality, the fraudsters have tricked a member of staff into making the payment to a fraudulent account number.

A common way in which this happens is where fraudsters impersonate a supplier or contractor and provide fraudulent account details on an invoice or email communication. If the changes to the beneficiary account details are not independently validated before the invoice is paid, the funds will often be lost.

**Payroll Fraud** – is a fraud which combines aspects of both CEO and invoice fraud. A fake request from a senior member of staff to change the account number for their next salary payment. If the person responsible for payroll does not validate the request as genuine with the staff member, then the next salary payment is sent to the fraudulent account.

Other types of impersonation fraud include phishing (email) and vishing (voice phishing) where fraudsters will try to trick victims into taking action such as clicking on a link within a phishing email to invite malicious software onto their device, or in a vishing call to give away confidential information such as payment authentication card and reader codes, or passwords. <sup>1</sup>

### **Top tips to enable businesses and organisations to guard against Impersonation Fraud**

Businesses should develop the Fraud Prevention Strategy within their organisation by considering three categories:

**People** – they can be an organisation's biggest asset when it comes to fraud prevention; or alternatively the weakest link. Businesses should invest in their people with a regular programme of fraud awareness training, including within induction training, so that they are better prepared to spot the warning signs of a potential fraud.

**Process** – businesses should challenge their existing processes to see how resilient they are to fraud e.g. do they utilise dual authorisation for payments? Do their processes ensure that staff independently validate all payment requests sent by email?

**Technology** – as a minimum, businesses should take the basic steps to protect their technology, e.g. running up to date anti-virus software, email filtering, patching or updating software promptly to avoid any compromise.





# Fighting public sector fraud through international collaboration

**The International Public Sector Fraud Forum (IPSFF) consists of senior representatives from organisations in the governments of Australia, Canada, New Zealand, the United Kingdom and the United States. The IPSFF recognises that fraud is a constantly evolving threat that does not stop at national borders and requires international co-operation.**

The Forum Aims to:

- Develop and share international best practise on counter fraud; and
- Identify collaborative opportunities between the Five Eyes countries to fight fraud

The Forum Achieves These Aims by:

- Learning about counter fraud best practise and key challenges through regular forum meetings and bilateral engagement at the operational and strategic level;
- Working collaboratively with counter fraud experts across the Five Eyes to find solutions to deal with common problems; and
- Developing products to support the public sector's understanding and response to fraud.

## A Guide to Managing Fraud for Public Bodies

This guide, the first IPSFF product, established the five principles of fraud and corruption:

### **There is always going to be fraud**

It is a fact that some individuals will look to make gains where there is opportunity, and organisations need robust processes in place to prevent, detect and respond to fraud and corruption.

### **Finding fraud is a good thing**

If you don't find fraud you can't fight it. This requires a change in perspective so the identification of fraud is viewed as a positive and proactive achievement.

### **There is no one solution**

Addressing fraud needs a holistic response incorporating detection, prevention and redress, underpinned by a strong understanding of risk. It also requires cooperation between organisations under a spirit of collaboration.

### **Fraud and corruption are ever changing**

Fraud, and counter fraud practices, evolve very quickly and organisations must be agile and change their approach to deal with these evolutions.

### **Prevention is the most effective way to address fraud and corruption**

Preventing fraud through effective counter fraud practices reduces the loss and reputational damage. It also requires less resources than an approach focused on detection and recovery.

The Principles are underpinned by practises for managing the risk of fraud and corruption.



In February 2020 IPSFF released four further products, which are summarised below. They can be downloaded from the link below, or by using the QR code at the bottom of the page.

[www.gov.uk/government/publications/international-public-sector-fraud-forum-guidance](http://www.gov.uk/government/publications/international-public-sector-fraud-forum-guidance)

International Public Sector Fraud Forum  
Guide to Understanding the  
Total Impact of Fraud



### **Guide to Understanding the Total Impact of Fraud**

Builds a case for investing in counter fraud measures by explaining the comprehensive impact of fraud. Sets out the key extending impacts of fraud, noting that many cases of fraud will have a number of different impacts: human, government outcomes, reputational, government systems, industry, environmental, security, financial and business.

Understanding these impacts enables public bodies to prevent or mitigate these impacts and educate their employees and stakeholders on the importance of counter fraud measures.

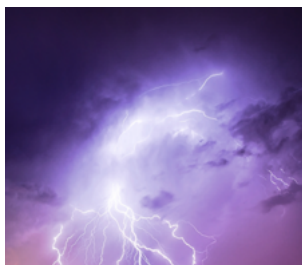
International Public Sector Fraud Forum  
The use of Artificial Intelligence  
to Combat Public Sector Fraud  
Professional Guidance



### **The Use of Artificial Intelligence to Combat Public Sector Fraud: Professional Guidance**

This paper considers the appropriate elements of a framework for the use of Artificial Intelligence (AI) technology by public sector agencies in dealing with fraud and corruption. It also discusses central issues raised in the use of AI. These include; scoping, accuracy, human control, transparency and explainability, fairness, privacy and civil liberties.

International Public Sector Fraud Forum  
Fraud in Emergency Management  
and Recovery  
Principles for Effective Fraud Control



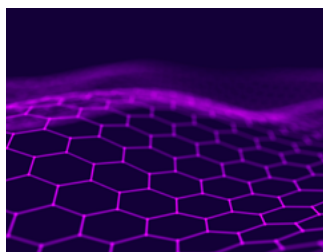
### **Fraud in Emergency Management and Recovery: Principles for Effective Fraud Control**

In times of emergency or disaster recovery situations, it is important that government can get funding to where it is needed as quickly as possible. This includes providing support and services to those in need and rebuilding communities and infrastructure. Fraud can undermine these efforts if it is not controlled.

This guide focuses on the time-critical aspects of emergency management rather than the longer-term efforts to manage potential emergencies and establishes principles for effectively controlling the levels of fraud in emergency management contexts.

International Public Sector Fraud Forum  
Bringing countries together to fight public sector fraud

International Public Sector Fraud Forum  
Guide to Designing Counter Fraud  
and Corruption Awareness Training  
for Public Bodies

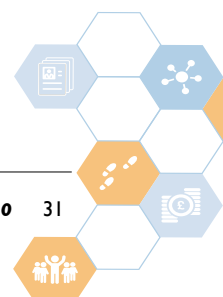


### **Guide to Designing Counter Fraud and Corruption Awareness Training for Public Bodies**

This Guide assists those leading fraud control responses in public sector organisations to take the necessary measures to implement an effective and lasting counter fraud and corruption program.

Part I: Emphasises and focuses on the value and importance of implementing a counter fraud and corruption awareness training program for public bodies. It underscores the importance of delivering sustained fraud awareness at all levels of the organisation and the need to secure senior management and employee buy-in.

Part II: Focuses more specifically on the steps required in planning, designing, developing and evaluating an effective counter fraud and corruption awareness training program. <sup>1</sup>







# Government Counter Fraud Profession

THIS JOURNAL IS FOR INTERNAL DISTRIBUTION ONLY

Crown Copyright Notice

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

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

Contact us:

Email: [gcfp@cabinetoffice.gov.uk](mailto:gcfp@cabinetoffice.gov.uk)

Web: <https://www.gov.uk/government/groups/counter-fraud-standards-and-profession>

