Government Counter Fraud Profession

The Public Sector Counter Fraud Journal

ISSUE 7, FEBRUARY 2021

Using social norms to prevent fraud and corruption

Editorial Board

Toni Sless
Chair and Founder
Fraud Women's Network

Jackie Raja
GCFP Development Lead
Department for Work and Pensions

Professor Mark Button
Director of the Centre for Counter Fraud Studies

Mark Cheeseman
Director
Counter Fraud Centre of Expertise, Cabinet Office

David Kirk
Consultant Barrister
RS Legal Strategy Ltd

Maria Kenworthy
Investigator
Ministry of Justice
Counter Fraud and Investigations

Mick Hayes
National Operations Manager
NHS Counter Fraud Authority

Cover image: Evening over Millennium Bridge, photographed by James Padolsey on Unsplash







CONTENTS

Editor's letter

This issue's letter is provided by Toni Sless, a member of the Journal's Editorial Board. Toni is a Fraud Risk Management Consultant and Chair and Founder of the Fraud Women's Network.

We've left 2020 well and truly behind, but not without its battle scars, many of which are still healing in 2021. However, let us not be negative here, lets instead reflect on the good of 2020 and stand proud of what we have achieved together through collaboration, hard work and the dedication of and by you, the Counter Fraud practitioners. Stand proud and tall, you have shown great strength and determination through the toughest of challenges we will no doubt face in our respective lifetimes.

The Journal, which has an audience of over 20,000 counter fraud practitioners nationally and internationally, published outstanding contributions in 2020, showcasing what we do best - sharing best practices, learnings and advice. The Public Sector has come together during a time of great upheaval, rapid change, unsettling times and let's not forget, managing and juggling the new norm of working remotely and home schooling, all at the same time.

The 2020 Tacking Economic Crime Awards bestowed worthy awards and accolades to some of our colleagues in the Public Sector – well done to all the winners and nominees. In case you missed the awards, full details of all the worthy winners can be found on page 22. And we too, the Editorial Board, were a finalist in the Outstanding Partnership category of which we are very proud.

So let's look forward to 2021 and the continuation of our great collaborations, not only within the Public Sector but also with our colleagues in the Private Sector. The Annual Public Sector Counter Fraud Event and Annual Awards Ceremony in February 2021 will be a great opportunity to hear our colleagues speak and celebrate success.

In this edition of the Public Sector Counter Fraud Journal, you'll be able to read about the insider threat, what it is, the threat it poses to businesses and customers alike along with some extremely good advice and educational tools from the Centre for the Protection of National Infrastructure (CPNI).

We also hear from the Federation Against Copyright Theft (FACT) about piracy which is constantly evolving but always fraud.

Our colleagues in the Insolvency Service tell us about their team working and HMRC gives us an insight into how they handled their rapid response to the Coronavirus Job Retention Scheme.

As we look to new horizons, the Public Sector Counter Fraud Journal will be reaching out to you, our colleagues, seeking contributions. If you think you have got something that would be of interest to our readership, do get in touch by emailing us at: gcfp@cabinetoffice.gov.uk. Equally, if there is anything you'd like to read about, then also get in touch.

Toni Sless

What we tell ourselves: how stories can encourage bribery - and prevent it?

Authors:
Fiona Horlick QC and Jeremy Scott-Joynt,
Outer Temple Chambers

Everyone has a reason to take a payoff. As with other kinds of fraud, the vast majority of those who end up involved in bribery do not do so with malign intent: out of some confirmed decision or determination to break the law.

Instead, they convince themselves that they're doing so for defensible, even laudable reasons.

Business is hard. Covid has struck. People need jobs. Everyone does it. Why not me? Why not us? Why not them?

And in any case - so the thought process may run - it isn't actually a bribe. It's a sweetener. A marketing expense. An overhead. A reasonable accommodation. A favour.

Or perhaps just what friends do for one another.

The same old song

In other words: it's a rationalisation, of the kind that all counter-fraud professionals will have heard time and time again. One distinction and difficulty with rationalisations for bribery as opposed to fraud is that it is perhaps easier to find excuses which seem to apply to the common good, not just to one's own circumstances.

Particularly in hard times, there can be a strong temptation to view oneself as the hero - or at least the anti-hero - of the tale: the one prepared to take the tough decisions that others are too cowardly, too strait-laced, or too unimaginative to take. The contract needs to be concluded. The supplies need to be sourced. So, it's not accepting a bribe, it's understanding that sometimes ends justify means, and that you're the only one brave enough to see it. This is a wearingly familiar tale. But seen properly, the nature of the stories people tell themselves is not a problem for those of us who, in the public sector just as in the private, are trying to prevent or detect the taking of bribes. It's an opportunity.

The narrative side of bribery offences

As barristers, our job is to tell stories: to create a narrative out of the facts which shows the world to be as our clients wish it to be, and to show that the law, properly understood, supports that narrative.

Whichever side of a case we are on, we're used to stories like this one. Stories which seem to show that the mental element - in this case of bribery, but it applies to fraud as well - is lacking.

As far as passive bribery (seeking or receiving a bribe, contrary to Section 2 of the Bribery Act 2010 - and indeed active bribery, contrary to Section 1) is concerned, the key mental element concerns the improper performance of a duty. In some cases, there has to be an intent to undertake improper performance of a duty in return for (or in anticipation of) an advantage. In others, the offence is complete so long as accepting (or asking for) the advantage amounts to improper performance in itself.

Either way, the test of what's improper or not appears to be a fundamentally objective one, thanks to Sections 4 and 5 of the Bribery Act. What matters is whether the conduct under examination breaches a "relevant expectation" about how the duty in question should be performed; and that, in turn, is defined by "what a reasonable person in the UK would expect in relation to the performance of the type of function or activity concerned".

So, if the person in the street would find objectionable the idea of someone in (in this case) the public service asking for or accepting a personal advantage (for themselves, a relative or someone else) as a by-product of doing their job, we have the improper performance required.

In many cases there is still a subjective element, however, and in this, bribery differs from the modern test for dishonesty, as established in Ivey v Genting and confirmed in its application to criminal cases in R v Barton. As readers will probably know, the dishonesty test post-Genting is now substantially objective: once we know what a defendant knew and believed, the question to be asked is whether a reasonable person would find their behaviour dishonest

when set against the backdrop of that knowledge and belief.

The Genting test (so to speak) applies to passive bribery where accepting the advantage is itself improper, or where the advantage follows the improper performance: by Section 2(6) of the Bribery Act, the recipient doesn't need to actually know or believe their actions are improper. But where the corrupt "deal" is done in advance of the improper action, belief still counts. There needs to be an intention to act improperly.

And that is where the story-telling can come in. In principle, the Bribery Act 2010 was meant to rule out so-called "cultural arguments": the (frankly discriminatory) excuse that a briber believed a particular kind of misconduct was common practice in an industry, culture or country. In practice, juries have still sometimes seemed to find that persuasive; it was certainly an element, at least, in the acquittals of senior managers of Güralp Systems Ltd in December 2019. And more generally, the need to prove intent to undertake improper performance leaves space for creative story-telling about whether a reasonable person would really find conduct to be improper performance.

Against the particular backdrop of Covid, that could swing both ways. On the one hand, the pressure and stress of trying to keep the show on the road and services uninterrupted could render conduct more reasonable. On the other, the public anger about anyone exploiting the pandemic for personal gain might make such an argument counter-productive - even destructive.

Photo by Paul Chard on Unsplash

How can this help?

Keeping one's mind open to the power of stories can be a valuable additional tool to stop bribery, or spot it where it exists. Workplaces generate narratives like any social grouping, and these narratives have a symbiotic relationship with the workplace: they come both to describe the workplace's culture - and in turn to generate it, reinforce it or change it.

This is not, of course, to the exclusion of more traditional fraud-type controls. A successful bribery relationship will usually require opportunity: not just with the payer, but with the recipient as well needing to subvert systems to cover their tracks.

Necessity too plays a part - although here the necessity may well be a perceived systemic or organisational one, rather than something strictly personal.

In either case, existing procedures and controls can help. As always with counter-fraud processes, a close examination of systems to identify bottle-necks, points at which controls can be most effectively applied (and where possible piggy-backed on other functions such as HR, audit or accounting), will help spot bribery opportunities or highlight areas of the business where poor performance against targets may give rise to temptation.

But being alive to the stories that are told can amplify, even multiply, the effectiveness of these controls. Any good counter-fraud professional will sustain networks of communication both formal and informal across their organisation. Whether you think of this as in-house intelligence or simply an ear to the ground, it's an essential part of knowing where the risks are, and targeting resources and attention effectively. As you do this, be alive to the stories that are told, as well as taking the temperature of the mood surrounding what people say - or avoid saying. It may help you spot a growing problem; perhaps even to choke it off before it can really take hold.

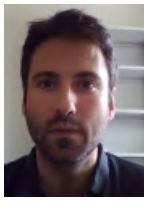
At worst, it may help identify the problem, and undercut the power of the narrative that the culprit may use to justify their behaviour - to their colleagues, or possibly ultimately to a jury.

At best, though, you might be able to exploit the fact that narrative not only describes, but defines. Build story-telling into your control programme. Make sure that proper (and therefore improper) performance is clearly defined, in narrative terms: what doing things properly looks and feels like, rather than simply what the technical policy definition says, and how an everyday person would know - just know - what's right and what's wrong. Imagine the effects of doing it wrong, on people as well as the organisation itself - and then find ways of painting that picture for colleagues to see and understand, at gut level. Where pockets of potentially destructive narrative seem to be growing, look for the root causes, and see if you can start telling a different story. Publicise people who do the right thing. Reward them.

And maybe - just maybe - you can change the story, before it changes you.

Using social norms to prevent fraud and corruption

Author:
Giannis Lois
Assistant Professor, Department of Economics, Maastricht University



John and Paul have recently been hired in the public sector of a developing country. In this country, public officials are usually underpaid, and this has led to a debate over whether minor bribes are not only expected but also morally justified. While John has taken a clear positive stance on this topic, Paul is rather skeptical about the moral repercussions of accepting bribes. Given that petty corruption is an established norm in this country, the government has launched a campaign explaining the harmful effects of minor bribes and condemning them as unethical. Would the government's campaign or the corrupting behavior of John's and Paul's colleagues influence their behaviour? What size of bribes (if any) would John and Paul consider appropriate?

Everyday life is full of examples that resemble this situation where empirical expectations of how others actually behave (descriptive norms) are in conflict with prescriptive expectations of how one should behave (injunctive norms). From a policy-making perspective, the crucial question is how to best utilise social norms to reduce a public officer's willingness to act dishonestly, even in a relatively minor way.

Prevalence of minor dishonest acts

Although huge corporate and government scandals in which few powerful individuals cheat a lot draw public attention, small transgressions of large numbers of people have just as large an impact on our daily lives [1]. Examples of consumer and occupational frauds such as overstating insurance claims, 'wardrobing' (where an item is purchased, used, and then returned for a refund from the retailer), tax

Photo by Elio Santos on Unsplash

deception, and petty institutional corruption are responsible for trillions of pounds of annual losses each year. Apart from the real-life evidence of high prevalence of minor dishonest actions, experiments in laboratory settings have also shown that people are more inclined to misbehave to a small extent rather than take full advantage of their cheating opportunities. For example, in one of these experiments, people misreported their performance to earn more money, but only to a certain degree (about 10-20%) above their actual performance and far below the maximum payoff possible [2]. These findings suggest that most of the cheating was not the result of a few "bad apples" that were totally rotten. Rather, it is a case of many apples in the barrel turned just a little bit bad.

Why do people cheat only a little bit?

When given the opportunity to cheat, many individuals do cross ethical boundaries, but only to a limited extent [3]. The standard economic perspective considers people as rational selfish beings who are interested only in maximizing their own payoffs by estimating the expected external benefits (e.g. getting more money or a better position) and expected external costs (e.g. paying a fine or losing a job) [4]. Within this framework, the decision to cheat only a little bit represents a puzzle: why do they not cheat to the full extent of what they believe they can get away with? In contrast to this classic economic perspective that focuses on external incentives, there exists ample evidence suggesting that people are also internally motivated to care about others and to value honesty [5].

Combining these two seemingly contradicting perspectives, researchers have provided explanations as to why honest people engage in dishonest actions only to a limited extent. One prominent explanation for this phenomenon is that people want to profit from minor acts of dishonesty while at the same time maintain a positive self-image of an honest and moral individual. To achieve this, they actively search for flexible self-serving justifications for their misbehaving [2] or they remain unaware (i.e. ethically blind) of the moral repercussions of their actions [6].

Dishonesty flourishes in ambiguous settings

These processes of self-serving justifications and ethical blindness are more pronounced when there is no well-defined boundary between honesty and dishonesty. In a recent experimental study [7], we examined the role of this ambiguity on dishonest behaviour by allowing rule violations to be the result of honest mistakes or of various dishonest processes. Participants first performed a demanding task in which they had to identify the gender of faces that were overlaid on images depicting houses.

Afterwards, they were given the opportunity to ask and receive extra money, but were instructed to ask for more only when the presented faces were presented inverted (i.e. upside down, making the accurate identification of gender more difficult), as opposed to upright. The more inverted faces they saw, the more money they were entitled to ask for. This cognitively demanding task can result in honest mistakes if participants mistakenly encode in memory or mistakenly retrieve from memory that the presented faces were inverted when they actually were upright. In this ambiguous setting in which the distance between honesty and dishonesty is very small, minor rule violations (asking for the smallest possible amount of money in easy rounds) can go under the radar or can be easily justified as honest mistakes. Consistent with this assumption, our findings showed that most individuals who violated the rule did so only to a small extent far below the maximum possible profit.

Norms influence the magnitude of dishonesty

Given that real-life dishonesty does not take place in a social vacuum, one interesting question is how injunctive norms (how people should behave) and negative descriptive norms (other people actually cheating) interact with each other to influence the tendency of honest people to engage in minor acts of dishonesty in this ambiguous setting. A large body of empirical evidence has shown that misbehaving does not depend solely on the simple calculations of cost-benefit analysis or the internal motivation for honesty, but also on the social norms implied by the dishonesty of others or by beliefs about what constitutes honest behaviour [8].

Coming back to our study, the absence of clear descriptive or injunctive norms led many individuals to commit minor rule violations (i.e. asking for the smallest possible amount of money in easy rounds). In a second phase, participants were informed that other participants had cheated a lot. The behavioural pattern changed dramatically. The exposure to others' misbehaving increased the frequency of major rule violations (i.e. asking for large amounts of money in easy rounds) but had no sizeable impact on the frequency of minor rule violations. A plausible explanation for this result is that in an ambiguous and novel situation, like our experimental setting, people pay attention to the social norm that is relevant to the situation and available at the decision phase, i.e. at the point where they can choose to act dishonestly. At the beginning, people are uncertain about what is the proper course of action due to the absence of both injunctive and descriptive norms. This uncertainty is eliminated once participants are informed that others cheated heavily, resulting in a selective increase in major rule violations.

To avoid these harmful effects of negative descriptive norms, one solution may be to remind people of what is the appropriate behaviour in this context (i.e. injunctive norms). But what happens when information about others' misbehaving is presented alongside a rule reminder? Our findings showed that rule reminders (e.g. "You should ask for extra points only in difficult rounds") are not sufficient to mitigate the increase in major rule violations driven by others' misbehaving. In other words, negative descriptive norms seem to be more powerful than injunctive norms. However, there is a glimmer of hope: rule reminders led to a reduction of the frequency of minor rule violations suggesting that injunctive norms can be effective at minimizing the minor dishonesty of honest people.

Practical implications

These results highlight the powerful impact of negative descriptive norms over injunctive norms on the magnitude of dishonest behaviour but also provide valuable novel insights into how to optimally take advantage of social norms to promote honest behaviour. Reminding people of how they should behave can potentially promote honesty (thereby preventing fraud) in ambiguous settings that are characterised by people engaging in minor acts of dishonesty. For example, "wardrobing", is, to a large extent, the result of many otherwise honest individuals returning just one shirt or sweater, but cumulatively this may cost retailers £1.5bn

each year [9]. Raising ethical awareness by reminding honest people of the consequences of this behaviour can have a crucial impact on this phenomenon.

However, these reminders are less likely to be efficient in preventing larger-scale dishonesty. The limited potential of injunctive norms (in the form of moral reminders) is further undermined by the presence of negative descriptive norms (i.e. other individuals cheating a lot) that shatter any hope for shared honesty. Returning to the "wardrobing" example, studies have shown that this behaviour is not only very popular but also many individuals perceive it as a common practice [10] which strengthens the salience of the negative descriptive norm while weakening the effect of moral reminders.

Taken together, our findings highlight the importance of taking into account people's empirical as well as normative expectations regarding the prevalence of dishonest behaviour [11]. In this respect, any effort to implement effective policies that counteract dishonest behaviour should both emphasise how an honest person should behave in a certain situation (i.e. ethical salience) as well as create the impression that dishonest behaviour in this situation is very rare. The ultimate aim should be to raise moral awareness whilst at the same time instill a feeling of shared honesty. Coming back to the public officials' corruption example, policy makers should address two independent issues. On the one hand, they should raise awareness about the deleterious consequences of taking minor bribes, targeting honest individuals like Paul who are already considering the moral repercussions of their actions. On the other hand, they should ensure that only positive information about others' behaviour is disclosed, thus discouraging major acts of dishonesty from individuals like John who pay less attention to the ethical dimension of their actions.

References

1. Mazar, N. and D. Ariely, Dishonesty in everyday life and its policy implications. Journal of Public Policy & Marketing, 2006. 25(1): p. 117-126.

2. Mazar, N., O. Amir, and D. Ariely, The Dishonesty of Honest People: A Theory of Self-Concept Maintenance. Journal of Marketing Research, 2008. 45(6): p. 633-644.

3. Ayal, S., et al., Three Principles to REVISE People's Unethical Behavior. Perspectives on Psychological Science, 2015. 10(6): p. 738-741.

4. Tittle, C.R. and A.R. Rowe, Moral Appeal, Sanction Threat, and Deviance - Experimental Test. Social Problems, 1973. 20(4): p. 488-498.

5. Fehr, E. and U. Fischbacher, The nature of human altruism. Nature, 2003. 425(6960): p. 785-791.

6. Banaji, M.R., M.H. Bazerman, and D. Chugh, How (un)ethical are you? Harvard Business Review, 2003. 81(12): p. 56-+.

7. Lois, G. and M. Wessa, Honest mistake or perhaps not: The role of descriptive and injunctive norms on the magnitude of dishonesty. Journal of Behavioral Decision Making, 2020.

8. Gino, F., S. Ayal, and D. Ariely, Contagion and Differentiation in Unethical Behavior: The Effect of One Bad Apple on the Barrel. Psychol Sci, 2009. 20(3): p. 393-398.

9. Preventing Wardrobing. Professional Security Magazine Online, 2019: https://www.professionalsecurity.co.uk/products/physical-security/preventing-wardrobing/

10. Ayal, Shahar, and Francesca Gino. "Honest rationales for dishonest behavior." The social psychology of morality: Exploring the causes of good and evil (2011): 149-166.

11. Bicchieri, C. and E. Xiao, Do the Right Thing: But Only if Others Do So. Journal of Behavioral Decision Making, 2009. 22(2): p. 191-208.

'It's okay to say' - a security education programme

Author:
Centre for the Protection of National Infrastructure

The Centre for the Protection of National Infrastructure (CPNI) is the UK government's lead technical authority for physical and personnel security. Our role is to protect national security by helping to reduce the vulnerability of the UK's national infrastructure to terrorism, hostile state actors and other serious threats. We are accountable to the Director General of MI5, the UK's domestic Intelligence Service.

CPNI's People and Personnel Security R&D Team consists of a blend of occupational psychologists, behavioural scientists and security specialists. This team aims to understand the factors that drive human behaviour and then apply good security measures to shape that behaviour to reduce vulnerability from threats to national security. We look at both the harm caused by people within an organisation, commonly known as 'insider activity', and hostile acts conducted by people external to the organisation. The current global pandemic has not reduced the threat, in fact it has created an opportunity for those wishing to act whilst organisations are distracted by other serious concerns.

In this article we will mainly be discussing the threat from insiders: people who have been given legitimate access to an organisation's assets, such as finance, information, buildings, technology and people, and who then use that access for an illegitimate purpose. As a counter-fraud community you will, of course, be very familiar with employees stealing funds and the methods they use to do so.

In CPNI we have conducted a large data study looking closely at over 100 insider cases. These cases have come from both public and private sector organisations. The aim of the study was to understand more about these insiders, both before they acted, during their activity and afterwards. We wanted to identify the kind of malicious acts they conducted, their motivations and their behaviours. We also wanted to understand what factors existed within the organisation at the time of the activity that may have contributed to the insider's ability to conduct their activity. Analysis of this data has provided CPNI with a very rich understanding of insider activity across the UK's Critical National Infrastructure and in turn, this has shaped the development of advice, guidance and tools to help mitigate insider risk.

One factor very quickly came to our attention during analysis of the data collected in this study: the issue of under-reporting or a lack of intervention when counterproductive or unusual workplace behaviours are observed by other employees. For each insider case in our study we often interviewed two or three people about the individual case and it became clear that people close to the insider observed a change in behaviour yet,

for a variety of reasons, did not report it. Our study also showed that anomalous workplace behaviours have often been seen to be precursors of welfare issues or possibly to more serious security concerns. Therefore, we recognised a need to provide an ongoing programme to support organisations with educating staff on identifying anomalous workplace behaviours and setting up mechanisms to promote the appropriate intervention and reporting of such behaviours. This would provide a double benefit: staff with welfare issues would get support and help more quickly and security concerns would be investigated and resolved sooner.

The 'It's Okay to Say' Education Programme promotes the twin positive outcomes of improved security and staff welfare that can result from identifying and reporting anomalous workplace behaviours in an ethical way. The programme has been designed to help staff identify behaviours that strike them as unusual or concerning and to encourage them to take appropriate action, to trust their instincts rather than just 'shrugging' them off. These behaviours will display as acts that are suspicious, unauthorised or suggest an individual's vulnerability and typically deviate from the 'norm'. Education on these behaviours will help build resilience to threats and a stronger security culture for the organisation and its people.

CPNI have worked with world-leading academics with expertise in behaviour change to create a framework for embedding good security behaviour change. This framework is known as the 5Es and underpins all of the CPNI security behaviour change campaigns, including the It's Okay To Say programme. The 5Es framework recognises that to embed change you must:

- Educate why – Education is crucial to encourage staff reporting. Unless staff understand the insider threat – that it can happen and have serious consequences to both staff and the organisation – unusual or unexpected workplace behaviours continue to go unchecked.
- Enable how – Explain the vital part staff can play in mitigating the insider threat by their actions and behaviour. The organisation should communicate what unusual and suspicious behaviour looks like, and develop the right skills to enable staff to identify and report these.
- Shape the Environment – Create a physical environment that makes staff intervention and reporting easy. Establish the social environment by making any good security behaviour the 'norm'. Give people permission to trust their instincts and intervene where they feel something is not quite right.
- Encourage the action – Behaviour change can only occur if the organisation is seen to reward good behaviour. This does not mean necessarily in material terms. It is about recognising and reinforcing the behaviour and culture you want to encourage. Equally, the converse applies; where staff have failed to act when they've seen something wrong there need to be measures in place to follow up as to why this happened. You may like to publicise internally examples of real-life insider threat scenarios where reporting concerns produced a positive outcome (for all involved), and those where a failure may have led to a negative outcome.
- Evaluation – When running a programme it is important to know if it is working to effect behaviour change. This way, you can improve any shortcomings and build on successes. Processes should be put in place to enable a consistent, fair and thorough investigative process which will allow for good metrics as to the effectiveness of the programme. The programme should be evaluated to help measure this by comparing a baseline before and after the programme is implemented.

Underpinning the Es is Endorsement – This is about ensuring the support of key stakeholders and credible experts in the organisation, ensuring that they are aware of, and back, the programme. Such endorsement is critical for the success of the programme; unless management have a positive attitude to the programme – and are prepared to find time to play a role in it – the good education effort will be wasted. Equally, you should consider who is best placed to deliver the required key messages. Credible experts, in tandem with management, that are seen to be enacting the types of behaviour change they are endorsing will be crucial. As one example, it may be that some areas respond better to the 'It's OK to say' programme when it has a welfare rather than a security-focused message.

The It's Okay To Say programme has been developed on the basis of in-depth end-user research with large organisations across the critical national infrastructure. We asked workforces across the critical national infrastructure what prevented them from reporting concerns and what would encourage them. Working with creative and communications' experts, we then developed a suite of materials designed to help organisations implement the 'It's OK to Say' Education Programme.

These materials are all free to download on the CPNI website (www.cpni.gov.uk/security-campaigns/it's-ok-say) and include:

- Detailed guidance outlining how to run the programme, including a pre-requisite check-list;
- Training slides, including audio scenarios designed to encourage discussion of the topic;
- 'It's Okay to Say' animated film presenting the behaviours in a light-hearted fashion and encouraging 'action';
- A selection of posters, stickers and pocket-sized cards using the 'It's Okay to Say' tagline and a template for organisations to provide escalation options; and
- Advice and guidance on how to evaluate the outcome of running the programme.

The materials can be branded with an individual organisation's logo to make them more relevant to a specific workplace.

The philosophy underpinning this work is that it is beneficial to establish a work environment in which people take personal responsibility for contributing to security through their everyday activities and interactions in the workplace. As a result of the pandemic many organisations are adopting remote working, or at least working in a more socially distanced way, so the drive to educate staff and line managers about the continuing need to report concerns has never been more important both from a welfare and security perspective.

Coronavirus Job Retention Scheme: Error and Fraud

The Coronavirus Job Retention Scheme (CJRS) was a unique response to an unprecedented global crisis. When national lockdown forced a dramatic change to working life as we knew it across the UK, it was clear that many individuals would be at risk of losing their livelihoods unless the government acted to protect them. The nature of this threat to the UK economy was unlike anything we had ever encountered before.

The CJRS was only one element of the government and HMRC's response to the pandemic. Schemes like these would normally take a year or more to design, build and test, but these had to be delivered in just a few weeks – delays could have caused irreversible economic damage. With a clear vision of what was required and a committed and dedicated team working from new surroundings as we, like many, were forced home through the lockdown, HMRC was

Photo by iMattSmart on Unsplash

able to deliver vital support to the nation at a time of great need and safeguard millions of jobs in the process.

Our priority from the very beginning was to get money to those in need quickly. While potential fraud had to be managed and minimised, excessive focus on this would make achieving that primary objective difficult. HMRC's Chief Executive Jim Harra told MPs at select committee hearings in April and June that, while we knew that the schemes would prove attractive to criminal and opportunistic fraud, we could not allow this knowledge to hamper our delivery at a time when many workers were at risk of severe financial hardship.

Several months on, with our immediate objective met, HMRC's focus has rightly turned to levels of error and fraud in the CJRS and Self Employment Income Support schemes and how best to tackle this.

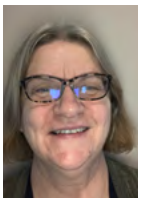
Of course, we did not ignore the threat of fraudulent claims, and we incorporated protective measures from the earliest stages of designing and launching CJRS. More than 32,000 CJRS applications were rejected automatically by safeguards we built into our online system, meaning the claim was never accepted for progression and didn't require caseworker checks. Examples of this included claims where our data showed no employees on previous payroll returns, or where the employer had told us previously that they had stopped trading. A further line of defence came through the active involvement of our experienced data and risking experts, spotting and blocking suspicious applications before any payments were made.

In cases where we suspected financial anomalies had slipped through, we acted promptly. We made around 5,000 targeted calls to employers whose claim looked higher than we expected, or where we had information that suggested fraudulent activity. These calls reduced the chance of error through genuine mistakes and made it clear that we would be taking action and investigating excessive claims.

Once the Finance Bill was granted Royal Assent, HMRC gained full legal authority to act on CJRS fraud and we started our post-payment investigations in depth. Our activities are based on data which we have on payments under the schemes, comparisons with existing information, and reports made to our fraud hotline – at the time of writing we have received more than 14,000 calls about potential CJRS fraud.

We have sent letters to around 3,000 employers a week since August, asking them to check their claims for errors, and have sent a smaller number of letters to those employers where data suggests an anomaly in the amount claimed, giving them the opportunity to voluntarily correct these mistakes.

Author:
Janet Alexander,
Director responsible for COVID-19 compliance, HMRC



There is a real need and a desire to bring those who have intentionally abused the CJRS to account. However, we must also distinguish between intentional abuse of the scheme and innocent error. Many were acting under extreme pressure when they applied for CJRS and inaccuracies may have arisen in the process. We accept that this may be the case with some overpayments, and we will help those individuals to remedy their mistakes without penalty.

At the opposite end of the scale, action against the most egregious cases of deliberate fraud could include penalties and criminal investigation and HMRC will apply legal powers to recover any money that has been wilfully overclaimed. In one of the first of these cases, we made an arrest in July 2020 in relation to suspected criminal activity and made two further arrests in September 2020, with several other criminal investigations now in progress.

It is difficult to provide an accurate estimate of the scale of the problem due to the novel nature of the COVID-19 support schemes. We would normally rely on past evidence as a basis for any estimate of future fraud and error, but in this situation, we have no such figures. Instead, we have utilised analysis of other grant and benefit schemes, such as Tax Credits. The limitations of using such evidence is clear, as the demographics applying for such schemes are very different to those applying for CJRS (mainly employers). These figures have guided our current expectation that error and fraud in CJRS will be around 5-10%.

Our ongoing investigation work will provide us with a more accurate picture of these levels. In addition, as errors are addressed, accounts of concern identified and activity to recover funds progresses, the amount in question will be reduced. We are planning to supply updates on these figures in Spring 2021 and to produce accurate figures for error and fraud in the coronavirus support schemes in 2022.

The tax-paying public will rightly expect us to tackle fraudulent activity and bring to account those who have wilfully abused these schemes at a time of national crisis. As we apply ourselves to this challenge, we must not lose sight of the value of our achievement in creating and launching the CJRS and, through this and the other COVID-19 support schemes, protecting and preserving millions of livelihoods.

Allegations of fraud and wrongdoing relating to the taxes and schemes that HMRC operate can be submitted through the Fraud Hotline service. Access this service by searching 'report tax fraud' on gov.uk or, for urgent and time critical matters, telephone 0800 788 887 Monday-Friday 9am-5pm.

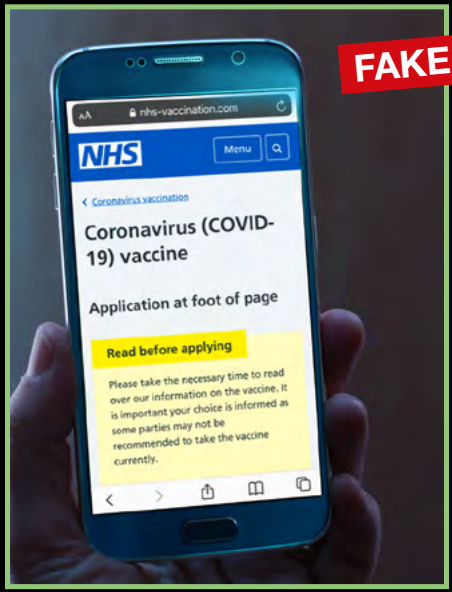
Government Counter Fraud Function

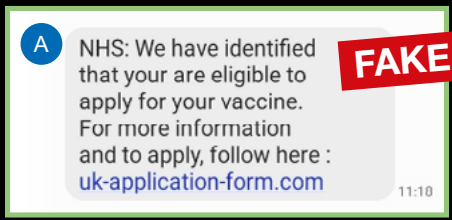
GOV.UK/coronavirus

NHS Counter Fraud Authority

BE ALERT TO VACCINE FRAUD

Criminals are using the COVID-19 vaccine as a way to target the public by tricking them to hand over cash or financial details. They are sending convincing-looking text messages letting people know they are eligible for the vaccine or phoning people directly pretending to be from the NHS, or local pharmacy.





PEOPLE ARE WARNED TO BE ALERT TO THESE SCAMS

The NHS will:

- ⊗ **NEVER ask for payment - the vaccine is free**
- ⊗ **NEVER ask for your bank details**
- ⊗ **NEVER arrive unannounced at your home to administer the vaccine**
- ⊗ **NEVER ask you to prove your identity by sending copies of personal documents such as your passport**

FURTHER GUIDANCE AND SUPPORT

National Cyber Security Centre

If you receive a call you believe to be fraudulent, hang up. If you are suspicious about an email you have received, forward it to **report@phishing.gov.uk.** Suspicious text messages should be forwarded to the number **7726** which is free of charge.

ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk

If you believe you have been the victim of fraud or identity theft, you should report this directly to Action Fraud either online; **actionfraud.police.uk** or via phone **0300 123 2040.**

CrimeStoppers.

If you have any information relating to vaccine fraud you can stay 100% anonymous by contacting Crimestoppers COVID Fraud Hotline online; **covidfraudhotline.org** or phone **0800 587 5030.**

COVID-19: Innovating amid a crisis

In 2020 Craig Martin was called upon to lead the Risk and Countermeasures Team as part of the Government's COVID-19 Fraud Response Team.

He has deep sector knowledge of fraud risk management, with experience in both the banking and public sector.

He previously led on the implementation of the Counter Fraud Functional Standard across government; has twice published the cross-government fraud landscape annual report, and has worked across the public sector to improve the way in which public bodies manage fraud risk.

In this article he reflects on his own experiences during this challenging time.

Author:
Craig Martin,
Head of Fraud MI & Insight, Centre of Expertise for Counter Fraud (CoEx), Counter Fraud Function

We continue to live in unprecedented times, where the government has prioritised the health and economic response to COVID-19; emergency stimulus measures have been introduced to save jobs and to protect the economy. With policy comes difficult choices and the Government's Counter Fraud Function has been working to integrate control measures into the design of the stimulus schemes, whilst also scaling up efforts to detect and prevent fraud with data-driven solutions. All of this has happened, whilst the normal functioning of government was not possible, and our people have risen to the challenge.

There have been many 'don't drop the ball moments' and I recall countless situations, where we have had to think fast, and respond to new challenges in a collaborative and constructive way. The stakes couldn't have been higher and we have been working across the public sector, and with different industries to shape the government's fraud response to COVID-19. Add to that the additional challenges and pressures that the pandemic brought to us all;

Photo by AbsolutVision on Unsplash

Photo by Matt Ridley on Unsplash

a sudden shift to working remotely, family circumstances and uncertainty - then our skills as individuals and leaders have been thoroughly tested.

During the pandemic it was necessary to reshape the Centre of the Function to meet the emerging needs of the response. This required flexibility and adaptability of those already within the Centre of Expertise for Counter Fraud, with large amounts of 'business as usual' taking a back seat. People's jobs changed, sometimes several times in the space of a few months. However, this allowed people to utilise their knowledge and skills in different ways. My own background in the private sector complements those who have experience working in public sector fraud, including those from the frontline.

The collaborative values of the Counter Fraud Function also allowed us to bring in people from other departments to aid with particular projects where there was a gap.

The term 'resilience' is used a lot, but often in the context of the ability to return, after an issue or crisis, to the previous state. This pandemic, however, has resulted in new opportunities to transform and disrupt. This is not only to aid in the immediate counter fraud response, but to put in place the structures and tools to ensure government is better placed to effectively fight fraud and error encountered in more normal times and be better equipped to prevent and detect more fraud in a future emergency.

In March 2020, the Counter Fraud Function immediately sought to address two gaps with two scalable solutions to help expedite the flow of emergency payments to individuals and businesses impacted by COVID-19.

All of the government's COVID-19 financial support schemes have eligibility requirements, and have been designed to help genuine individuals and businesses through the pandemic. But these schemes are not without fraud risk.

To help mitigate the risk of fraud we developed a new solution to help distinguish between genuine and fraudulent applications by validating applications using bank account information. This helped to ensure that public bodies paid emergency grants to the correct businesses.

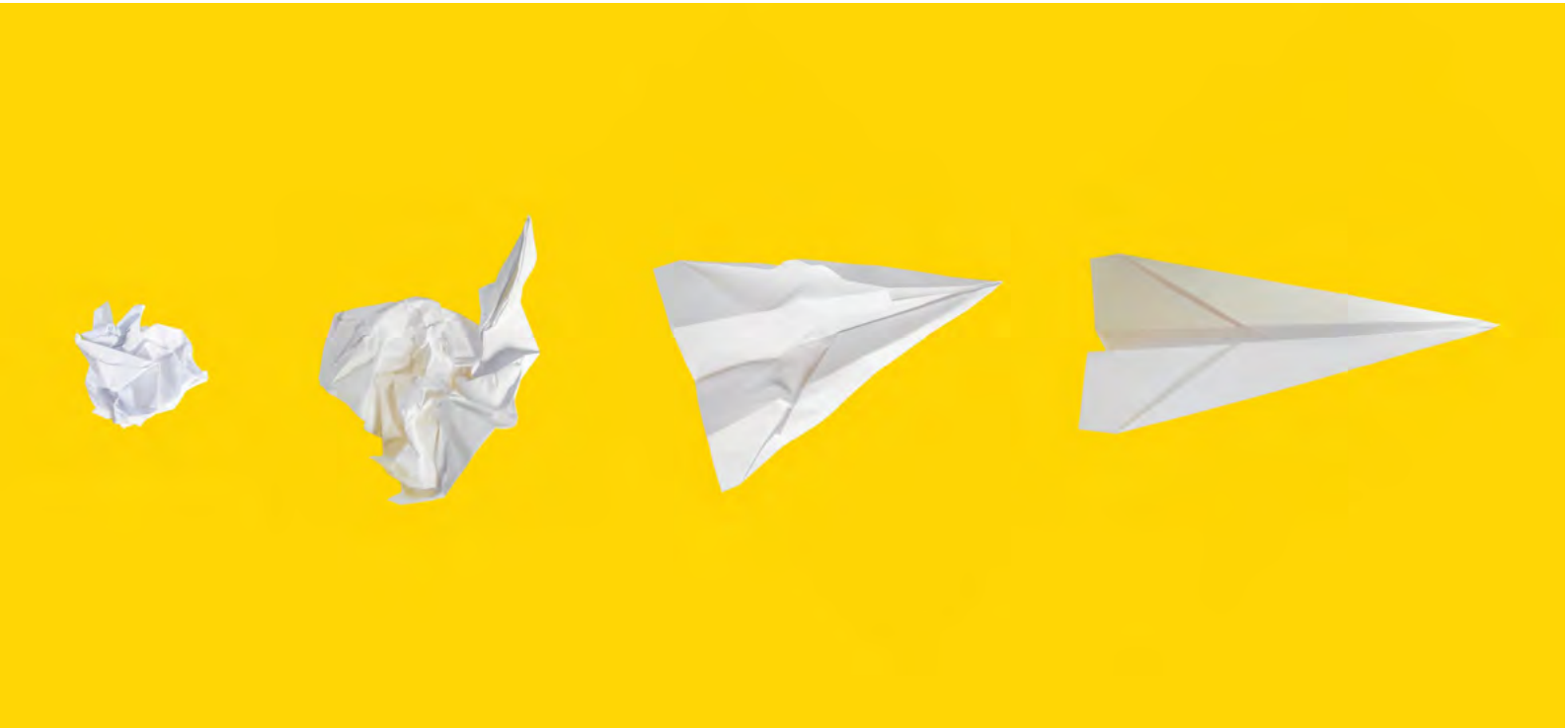
This solution was made possible by amending the Commercial Credit Data Sharing (CCDS) scheme, enabling commercial banking data to be used in the public sector for the first time. We then built a second tool to help validate the trading status of a company using commercial credit data. This has proved immensely valuable across many schemes including Small Business Grants, the Future Fund, and within the Bounce Back Loan Scheme (BBLS).

Data-driven tools, like the Active Company Check and Bank Account Verification Tool have proven their worth many times over. They were developed and rolled out in 23 days as part of a public-private sector partnership and have since become an embedded part of our response. These tools have helped to mitigate the risk of impersonation and first party fraud.

In other areas of the COVID-19 fraud response, we have been working in close collaboration with Her Majesty's Treasury, the Department for Business, Energy and Industrial Strategy and the British Business Bank to develop and run a Fraud Data Analytics Programme for the Bounce Back Loan Scheme. This programme focuses on the detection of fraud linked to organised crime and delivers 'scheme level' analytics using government data. It's an example of what can be achieved through close collaboration and partnerships with organisations including Companies House, HMRC and the National Crime Agency.

But we didn't stop there. Innovation is about exploring what is possible and leveraging technology and data in new ways to achieve better outcomes. When the global demand for personal protective equipment (PPE) surged, so did the number of fraudulent suppliers entering the market. We explored new ways in which global payments data and other due diligence tools could be used to prevent fraud. It's another example of why fraud experts have to keep pace with industry developments: as the threat changes, so must our response.

We have achieved so much as a Counter Fraud Function in such a short period of time because of collaboration and innovation, and I am confident that we will continue on this footing.



Piracy: constantly evolving but always fraud

Author:
Eddy Leviten,
Chief Operating Officer, Federation Against Copyright Theft

The term 'intellectual property' ('IP') refers to creations and ideas such as designs, business names and images, branding, artistic and literary work and inventions. Intellectual property is protected by copyright laws, patents and trademarks, which means that if someone's IP is replicated or counterfeited without the agreement of the rights holder, a crime may well have been committed. According to the Organisation for Economic Co-operation and Development (OECD) 3.3% of global trade is made up of counterfeit and pirated goods, putting a value of a staggering $509bn on imported fake goods worldwide, roughly equivalent to the whole of the UK's exports in 2019.

In 1982 the film industry was seeing a new wave of IP crime as E.T. was not only calling home on the big screen but was finding his way into many homes in the form of pirated VHS videos. This led to the formation of FACT in 1983 to protect the content, product and interests of the film and television industries. By remaining at the forefront of technological advances and as a result of our successes over the years, we are regarded as the leaders in IP protection. We work with rights holders and law enforcement and participate in multi-agency groups working to develop initiatives and share intelligence on the protection of IP including the Government Agency Intelligence Network (GAIN), IP Online Protection Group (IPOP) and the IP Crime Group, chaired by ACC Pete O'Doherty, National Police Chiefs' Council lead on IP, and David Holdsworth, Deputy Chief Executive at the UK IP Office.

IP crime: the impact

The act of committing IP crime is often not seen as particularly serious, but this kind of crime is fraud. Many of FACT's successes as private criminal prosecutions with the CPS and rights holders have achieved convictions on charges of fraud or conspiracy to defraud. Put simply, those stealing another's IP are depriving businesses of revenues that generate jobs and pay taxes. According to DCMS data, in 2018 the Creative Industries employed more than 2 million people in the UK and generated £112bn in Gross Added Value for the UK economy. This revenue and the jobs created are directly at risk as a result of pirated content. IP crime is often seen as victimless but the impact extends beyond the major broadcasters down to the local economy. With increasing pressure on UK employment due to the pandemic there has never been a more important time to act on IP crime.

The piracy evolution

According to the UK IPO's Online Copyright Infringement Tracker a quarter of adults in the UK are using an illegal source to access content, showing there is still much work to be done to tackle piracy, despite the best efforts to date. Since FACT's

formation in 1983 piracy has evolved significantly; from grainy VHS copies to DVD ripping to the vast majority of piracy now existing completely online. Even within the online space we have seen a shift in recent years from filesharing and downloads to streaming now being the preferred method of content consumption. The evolution to streaming presents a number of barriers to prevention. Whereas filesharing depends on some technical knowledge and understanding, streaming is simple for most users. Illegal streaming services are not limited to the dark web or underground corners of the internet but are readily advertised on social media, making them accessible to even basic users. This presents further challenges to prevention by encrypting messages and providing a space for closed and secret groups which would not appear on a search but can have thousands of members. FACT recently investigated a streaming service provider that operated through a private Facebook group, WhatsApp and Telegram. The private Facebook group alone had over 9,000 members and defrauded a major broadcaster of more than £60,000 in a relatively short space of time. The individual running the service pleaded guilty to one Fraud offence and two Copyright Designs and Patent Act offences.

Piracy and Organised Crime Groups

Despite publicised prosecutions of those engaged with piracy, IP crime continues to be perceived as low risk and high profit by Organised Crime Groups (OCGs) and often a method of funding dangerous crime. An OCG trading as Credit Lucky Finance Ltd produced and sold counterfeit DVDs and laundered vast amounts of cash generated from the sales. The discs were produced in factories situated throughout the UK which were then sold in public houses and industrial estates across the country by illegal Chinese immigrants who were being exploited by the OCG and forced to sell the discs. It is believed that the turnover from accounts identified by investigations was £160m across 2006 and 2007. This OCG was additionally involved in the sale and distribution of counterfeit cigarettes and the running of major cannabis factories, with intelligence suggesting that the funds accrued were used to fund prostitution, drug cultivations and other criminal activity across the UK, with funds being transferred to China. With the ability for piracy operations to be truly global – from running servers in different countries to laundering money across international bank accounts – investigations into piracy must be increasingly sophisticated in adapting to behavioural and technological advances.

Making vast sums of money from piracy is not limited to major operations by OCGs. Individual operators also see the provision of pirated content as an opportunity to generate significant revenue. Following the successful prosecution of illegal content providers, a confiscation order will be pursued to reclaim the generated revenue. This is a vital part of prosecution in piracy cases as there is huge potential for significant criminal financial gain. The Law Commission is currently examining the £2bn of unpaid orders with the publication of the Law Commission Consultation Paper on Part 2 of POCA (confiscation). The Paper sets out a review of the current law with a suggestion to appoint a single, central organisation to provide national oversight and regulation of confiscation enforcement, regardless of which body brings the prosecution. This change would relieve the prosecutor of the obligation to be involved in the process of enforcement.

Confiscation: a case study

In 2018 John Dodds was sentenced to four-and-a-half years in prison after pleading guilty to a conspiracy to defraud following a private prosecution brought by the Premier League. He was arrested following an investigation led by the Premier League working in partnership with FACT. Dodds sold illicit streaming devices (ISDs) to hundreds of pubs and clubs, allowing customers to view pay-TV without the permission of and without making any appropriate payment to the relevant broadcasters. Subscriptions to this unlawful service were sold at a rate designed to under-cut the legitimate broadcasters. The fraud caused losses to the broadcasting industry of millions of pounds. In February 2020 Dodds was ordered to pay back £521,000 within three months or face his prison sentence being extended by five years.

Educate to prevent

At FACT we take a holistic approach to piracy prevention. By employing a range of techniques in disrupting, enforcing, prosecuting, educating and raising consumer awareness we target piracy at all levels. The recent shift towards streaming services has allowed law enforcement to seize subscriber databases and identify consumers in addition to taking action against the provider. In September 2020 Norfolk and Suffolk Constabulary issued individual warning notices to thousands of subscribers to a service called GE Hosting. The Police obtained the list of subscribers after arresting a man in connection with GE Hosting and shutting down the service in 2020. The individuals were notified that subscribing to these services is a crime which carries a maximum sentence of up to five years' imprisonment, the potential for a fine and consequently resulting in a criminal record.

FACT communications and media outreach focuses on education and information with the persistent message that providing and consuming illegal content is a crime. We work with clients and law enforcement to publicise reminders to consumers ahead of major sporting events such as the Premier League season start and pay-per-view boxing. Organisations such as the Industry Trust promote the value of legitimate sources and undertake extensive research into risks such as malware and hacking. Resources such as GetItRightFromAGenuineSite and FindAnyFilm allow consumers to find legitimate sources for any content they like and bodies such as the IPO publish extensive resources on IP and IP crime.

In addition to delivering the message to consumers we also engage with and inform law enforcement and groups working to tackle crime. We already work with a wide range of public and private sector organisations and we may be able to help you with investigations that you are currently undertaking. FACT's capabilities include overt and covert investigations into fraud, money laundering and other areas of criminality, as well as carrying out due diligence and business intelligence. You can find more information, including how to get in touch, at: www.fact-uk.org.uk.

Energy theft is more than just a financial threat: Stay Energy Safe

Rodger Holden, Development Director at Crimestoppers, explains that whilst energy theft risks life and property, the sector is working with the charity to fight back.

Energy theft is not a victimless crime. Whilst the consequential losses are mostly financial – to energy companies and their customers – tampering with the meter or energy supply is a dangerous and criminal activity.

The financial costs are estimated at around £400-£500 million each year – a staggering figure that gives an indication of the true scale of the problem across the UK. All of us pay the price

for these criminal actions, with the consumer cost estimated at around £20 per household. It's a key focus for the energy industry.

Author:
Rodger Holden,
Development Director, Crimestoppers

What is energy theft?

Stealing electricity or gas happens in cities, towns and villages and can affect people's homes, shops and restaurants, pubs and bars, and also workplaces such as factories and even farms.

Last year, there were around 100,000 investigations into energy theft. When reports of tampering with the meter or energy supply is suspected, the energy supplier assesses the risk to safety and responds appropriately. Where indications of tampering with the meter or energy supply are credible, the energy supplier or network operator is legally obligated to investigate, and must gain access to the meter to ensure it is safe.

If theft is confirmed, the supplier or network operator must estimate how much energy has been stolen. Even for domestic premises this can present challenges due to the wide variety of technologies, heating systems and household goods now in use. Commercial premises can be especially difficult, but investigators have access to a wide range of approaches and tools to assist them. The value of the lost energy is calculated, investigation costs added and recovery sought from the responsible party. Finally, these confirmed thefts are recorded and reported within the energy industry, as analysing this information can help to design better ways of finding and preventing energy theft.

The human cost of energy theft

The drive to stamp out energy theft is predominantly fuelled by a need to prevent dangerous situations. This isn't only to protect those who have themselves tampered with supplies. Other people may be innocent and unsuspecting victims, unwittingly encountering supplies interfered with by a rogue landlord or business owner.

The Stay Energy Safe service - delivered through Crimestoppers - is a dedicated energy theft reporting line funded by the energy industry. It encourages people to report any suspicions or evidence of energy theft. We guarantee anonymity at Stay Energy Safe, just as we do with our core crime reporting line. This limits what we can say about information received, as we must protect those who have trusted our service. However, in the public domain, there have been shocking and heartbreaking examples of the human cost of energy theft.

Innocent lives

Harvey Tyrrell was just 7-years-old when he was electrocuted in a pub garden after climbing over a wall to collect his football at the King Harold pub in Romford. It was initially believed he had suffered a head injury after falling. However, a post-mortem confirmed that Harvey died as a result of a fatal electric shock. 72-year-old David Bearman admitted gross negligence manslaughter and abstracting electricity worth over £22,000.

This is one case of many where innocent lives are put at risk by people trying to illegally cut corners or avoid costs by messing with the supply of electricity or gas. Every year over 280 people are injured or killed as a result of meter tampering. And whilst injury and death are the most worrying aspects, we shouldn't forget the great potential for fire or explosion to wreak terrible damage to properties.

We know from the intelligence we receive every day that large numbers of people and properties are being exposed to the dangers of energy theft. It may be the occupier copying a post they've seen online; it could be a 'well-meaning' neighbour or family member misguidedly seeking to help mitigate household expenses; or it might be that rogue landlord or business proprietor. All are placing themselves, their friends, family, tenants, staff or customers in potentially serious danger.

Crimestoppers has also seen a notable trend where those under investigation may have been stealing electricity or gas at multiple properties or businesses over a long period of time. For these people, it is very much a business-as-usual activity.

Penalties and punishment

When investigators identify energy theft, the responsible party can either receive a bill on the spot, or an invoice follows subsequently. Charges will be levied for the call-out and any further rectification works that may be needed, in addition to the electricity taken. In some circumstances, for example where the property can't readily be made safe, the supply will have to be disconnected. An energy supplier may also disconnect for theft, and this is particularly likely if there are repeated instances. Suppliers don't enjoy taking such action and it will generally be a 'last-resort' – especially for domestic properties – but they may be left with little choice.

The implications of being caught committing energy theft can be serious - every year, around 300 people are convicted of a criminal offence to do with energy theft. It can involve a criminal sentence, such as in the case of Mr. Bearman above, resulting in a criminal record and no longer being able to run or own a business, or being unable to find insurance for a property. Typically, fines may be a few thousand pounds, although in one recent case a man who had damaged the power supply to 15,000 homes was fined £50,000. The most serious cases, where large amounts have been stolen or people placed in danger, can attract a prison term.

Beyond individual responsibility, actions and harm, there's a deeper concern. Energy theft can often be linked to serious organised crime. This can range from cannabis cultivation in homes and industrial units to situations involving modern slavery and even prostitution.

Spot the signs - electricity theft

There's a possibility of shocks from switches or appliances and the potential for a fire or even an explosion.

However, some of the key things to look out for are:

- Damaged meter casing: the casing may be smashed, broken or removed completely;
- Re-routed cables: cables may be extracted from the meter and connected directly to the service termination;
- Extra wires: unexpected wires sticking out, often much thinner and sometimes with connector clips attaching them to the meter;
- Melted meter: parts of the plastic casing melted or

displaying scorch/burn marks;
- Working but no credit: meter shows credit has run out but electricity is still available;
- Meter dials/display not advancing: the dials aren't going around or the display isn't changing even when electricity is being used; or
- Burning smell: an acrid smell of something burning or even smoke or sparks.

Signs to spot - gas theft

It may not be surprising but messing with any gas supply is seriously unwise given the highly explosive nature of natural gas. It may be possible to smell gas leaking, but not always. Experts warn to look out for the flame on gas fires or on the hob changing size or burning more yellow than blue. The gas pilot may also be more likely to go out. Other key things to look out for are:

- Back to front: the meter has been turned around the wrong way so you can't see the normal dials;
- Smell of gas: a smell of gas near the meter box.
- Rubber piping: pipes replaced by bits of rubber tubing;
- Dial has disappeared: there is no visible dial or counter on the meter any more;
- Working but no credit: meter shows credit has run out but gas is still available; or
- Meter dials not moving: dials on the meter aren't going around even when gas is being used.

Stats correct as of October 2019

How to report

Stay Energy Safe is run by Crimestoppers, working with the energy regulator OFGEM and the UK's energy companies, to track down and stop meter cheats who put lives at risk in a misguided attempt to save money. It was launched in September 2016 and as the reporting line for energy theft, it guarantees 100% anonymity to everyone who calls 0800 023 2777 or fills in an online form at stayenergysafe.co.uk.

In 2020, Stay Energy Safe received nearly 10,000 calls and contacts from the public. This resulted in almost 6,000 actionable reports being sent on to investigators. Comparing 2019 to 2020 showed a year-on-year rise of nearly 34% in actionable reports. Interestingly, a majority of incoming contacts from the public are now received online (68%). The increase in information suggests the public are becoming more aware of the threat of meter tampering and are prepared to speak up anonymously.

Please encourage anyone with information or suspicions to contact Stay Energy Safe on 0800 023 2777 or to visit stayenergysafe.co.uk. It's an issue which is often ignored, but by improving understanding and highlighting the penalties, it's hoped we can go some way to help tackle this persistent and dangerous problem.

Recognising the best at tackling economic crime

Author:
Professor Martin Gill,
Founder, Tackling Economic Crime Awards

The Tackling Economic Crime Awards (TECAs) were launched to recognise companies, teams, individuals and initiatives that performed to an outstanding level in responding to any area of economic crime. The TECAs are not typical awards. For a start the organisers don't appoint the judges, the leading anti-fraud associations/organisations and interest groups do (e.g. Cifas, CIPFA, Cabinet Office, City of London Police, Fraud Advisory Panel, National Economic Crime Centre, Serious Fraud Office); the nominees, all people of high standing, agree to mark to an ethics policy; all judges mark independently; all judges have to declare any conflict of interest on every mark sheet; and so on. There is also an ethical sponsorship strategy designed to attract only credible supporters, and Altia-ABM, Cifas, LexisNexis Risk Solutions, stepped up to be counted and did an excellent job too. There are eleven categories (and more will be added this year), and entries are open to the public, private and third sectors. In short, if you win a TECA it is because you are very good, outstanding in fact; the competition is intense.

2020 was the second year of the awards; the winners were announced on Wednesday 9th December 2020 at a virtual awards show, one with a difference. Alan Dedicoat, who many will know as the "Voice of the Balls" on the National Lottery programmes and the announcer on Strictly Come Dancing was involved in reading out winners' details. Each award was presented by a different individual, often judges, including Professor Mark Button, Centre for Counter Fraud Studies, University of Portsmouth; Stephen Dalton, Insurance Fraud Bureau; David Clarke, Fraud Advisory Panel; Robert Brooker, London Fraud Forum; Mark Astley, NAFN; and Commissioner Ian Dyson QPM, City of London Police.

The audience was diverse, including representatives from across the economic crime sector. They tuned in live to celebrate the outstanding achievements of all the finalists and the winners.

Further details of the awards – including an opportunity to

watch the ceremony - can be found here: www.thetecas.com. However, let's draw attention to those who triumphed and were awarded a TECA. Perhaps what is most interesting is they represent very diverse parts of the tackling economic crime community, evidence itself of so much good work that goes on, all too often though under the radar. The TECAs are throwing a gaze on what outstanding looks like, that is important. Anyone who witnessed the show would have to conclude that the tackling economic crime community is thriving, and provided many examples of performance that merit being widely replicated.

After the virtual awards show there was an online awards networking party. Katy Worobec spoke first, and was clearly delighted and surprised by the honour she received. Many of the other winners spoke about their joy (and usually surprise) at winning. Many judges attended, and spoke about the high standards, the intensity of the competition, and the importance of recognising those who are outstanding. The awards have attracted attention globally, and will continue to do so.

Work has already started on the 2021 awards, as stated new categories are being formed, to broaden the scope for recognising those dedicated to tackling economic crime.

To read more about the finalists and the winners in 2020 visit: https://thetecas.com/winners-2020

TECAS winners for 2020:

Outstanding Team
Zurich Insurance Intelligence Team

Outstanding Investigator
Dave Perry – HMRC

Outstanding Customer Service
Hertfordshire Constabulary & Catch 22 – Beacon Victim Care Initiative

Outstanding New Product
Carpe Data Counter Fraud Solution for Zurich Insurance

Outstanding Training Initiative
Lloyds Banking Group – Fraud & Financial Crime Training Initiative

Outstanding Partnership
BAE Systems & Zurich Partnership

Outstanding Female Professional
Claire Jenkins FCCA – Companies House (see below)

Outstanding Male Professional
Philip Juhasz – Hertfordshire Shared Anti Fraud Service

Outstanding Prevention Initiative
Scam Marshals – National Trading Standards Scams Team (see next article in this issue)

Outstanding Young Professional
Zac Barrett – HMRC FIS Cybercrime

Lifetime Achievement Award
Katy Worobec – UK Finance

Claire Jenkins, winner of the Outstanding Female Professional award reflects on her win:

"To win the Outstanding Female Professional award for the second year running was really amazing.

It is such an honour to be recognised for my work and the passion that I have for counter-fraud from judges who are themselves from the counter-fraud community. It makes me feel valued, encourages me in what I do and raises my profile. We all work in an area which is somewhat in the shadows, so to get recognition and be put into the spotlight is fabulous.

I'd urge people to look at the categories next year and think if you or a colleague should be nominated to be recognised in these awards."

Scam Marshals

In December 2020, the National Trading Standards (NTS) Scams Team won the prestigious Tackling Economic Crime Awards (TECAs) in the Outstanding Prevention Initiative category for their Scam Marshal scheme. This award recognises the hard work of both the team and the Scam Marshals that have joined the initiative.

Author:
Adam Carter,
Senior Project Officer, National Trading Standards Scams Team

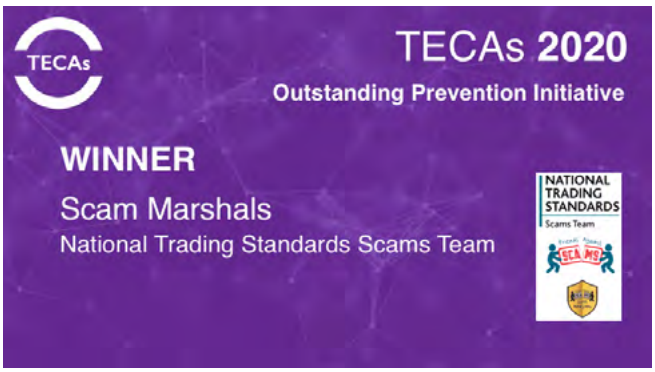
What is a Scam Marshal?

A Scam Marshal is someone who has been a victim of a scam or is being targeted by scams and uses their experiences to help protect others and themselves from future scams. Any individual can join by registering on the scheme and becoming a Scam Marshal. They are asked to talk to family, friends, and neighbours about scams to help increase community awareness which hopefully means communities become more resilient to scams. Scam Marshals are asked to send in any scam mail they receive to the team for investigation, as well as documenting details of scam phone calls they may receive on a log. This evidence is used by the NTS Scams Team investigators to aid enforcement (foreign and domestic) to prosecute, arrest and generally disrupt the flow of scams coming into the UK.

Scam Marshals receive a certificate, a Scam Marshal badge, a 'no cold callers' sticker for their front door, and other materials when they sign up. Every month after registering, Scam Marshals receive a newsletter and a freepost envelope that they can use to send any scam mail in the NTS Scams Team. The newsletter contains valuable information on the latest scams, enforcement news, which can often be credited back to the Scam Marshal, intelligence, and information on any new NTS Scams Teams initiatives. This is all designed to give a sense of belonging whilst arming Scam Marshals with the knowledge to be able to talk about scams to their loved ones and friends, thus increasing community resilience.

Up to July 2018, the scheme operated under the name 'Mail Marshals' and had around 150 people registered. The NTS Scams Team wanted to expand the scheme, as early indications showed that the scheme dramatically improved the wellbeing of the Mail Marshals (victims of the scams) and more could be done with

more Marshals. The team applied for a government grant from the Home Office to relaunch the scheme; the grant was approved, and it was decided to relaunch under the name 'Scam Marshals' to incorporate all types of scams.



The objectives of the campaign were to reach over 1,000 Scam Marshals by the end of March 2019; survey the Scam Marshals at registration, then survey again after three months. Albeit this list is not exhaustive, the measures of success, after three months were:

- 90% will report that they have the knowledge to talk about scams;
- 70% will feel safer and happier in their own homes;
- Scam Marshals will have talked to an average of 5 people about scams; and
- Scam Marshals will see a reduction in the scam mail that they receive, as they are now no longer responding and intelligence received helped to disrupt the criminal processes.

Scam Marshal testimonies

Anecdotal evidence was also gathered from Scam Marshals as testimonies for the project. The Scam Marshal scheme provides a way to communicate directly with scam victims, reassuring them that they are not alone and that they should not feel ashamed or embarrassed about falling victim to mail scams – these are common feelings associated with scam victims.

The Scheme

The NTS Scams Team worked with 174 local authorities and over 100 organisations up and down the UK, including many Police and Crime Commissioners (PCCs) and charities who helped to support the campaign using their social media platforms.

The team hit their target by March 2019 and now have over 1,700 registered Scam Marshals. The scam mail received by the NTS Scams Team is diligently logged and investigated. Most of the scam mail is clairvoyant and advance fee fraud, whereby the recipient is told it must pay an administration fee to release a large sum of money. The investigators within the NTS Scams Team use these mailings to work with postal operators, as well as domestic and foreign enforcement agencies, to help disrupt and prosecute the criminals behind the crimes. This intelligence is a key tool in seeing what is coming into the country in real time, as well as how it comes in.

Many Scam Marshals have appeared in the media, TV programs such as Rip Off Britain and newspaper articles in the Daily Mail, The Mirror and the Sun.

Survey results

Scam Marshals are surveyed after three months and asked for their views on the scheme; with some Scam Marshals speaking about their experiences of scams at conferences and local groups or sharing their story and status on social media platforms; on average Scam Marshals connect with 67 people to raise awareness. Peer to peer support is proving to be invaluable, and shared experiences has made it okay for people to talk about scams and has taken away the shame. Scam Marshals also see a huge reduction in the scam mail that they receive as a result of no longer responding to them. They also feel happier and more in control of their life and empowered.

- 86% of Scam Marshals have not responded to scam mail
- 90% have not lost any money to scam mail
- 87% now know how to spot a scam
- 87% now feel safer in their own home
- 93% know where to get help with scams
- 85% now feel happier
- 89% feel they are not susceptible to falling for a scam
- 83% feel they have been prevented from being scammed

Call Blocker Project

In January 2020, all Scam Marshals were offered a free trueCall Secure+ call blocking unit as part of the NTS Scams Team call blocker project. The unit blocks 99% of scam and nuisance calls while allowing trusted callers to get through. Over 300 Scam Marshals requested one and were supplied with a unit.

Scam Marshals provide other victims with the support they need whilst arming them with the knowledge to take a stand against scams. The Scam Marshals' self-worth, wellbeing, the feeling of safety and the ability to spot a scam are all increased as a result of the scheme as they are part of an army of 'scambusters' helping to increase awareness and protecting their communities from scams - they belong! The intelligence received from the Scam Marshals is vital to the NTS team for investigations whilst also helping to raise awareness of new trends that they see.

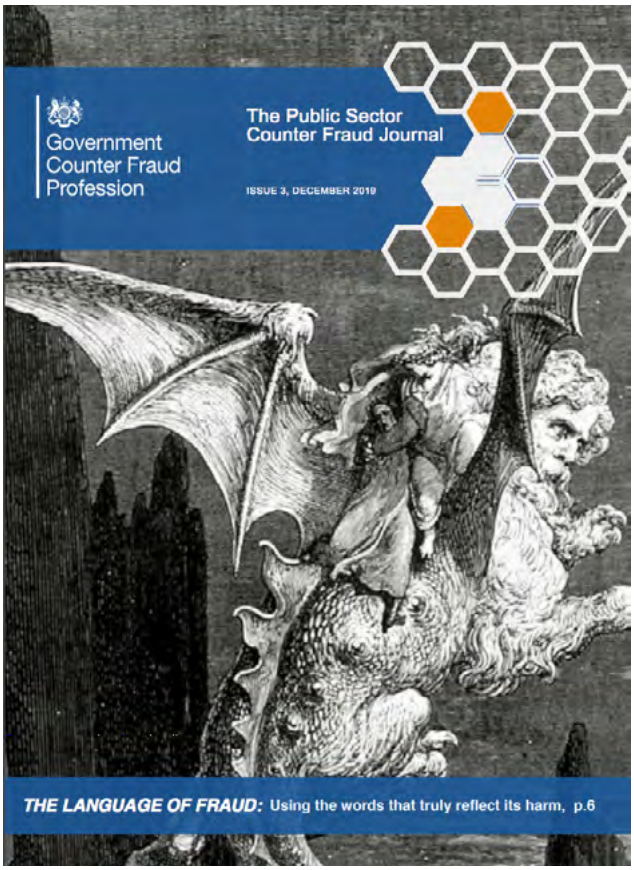
Letter from a victim of scams:

"I look on my phone as a lifeline to the outside world, and when I hear it ringing I feel good. But since I started getting these scam calls, when it rings I now feel worried about what I'm going to have to hear.

It feels like I have been burgled; it is a terrible invasion of privacy.

I do hope you can use your powers to stop these crooks inflicting any more pain on people who are very vulnerable."

Previous issues



Issue 3, December 2019

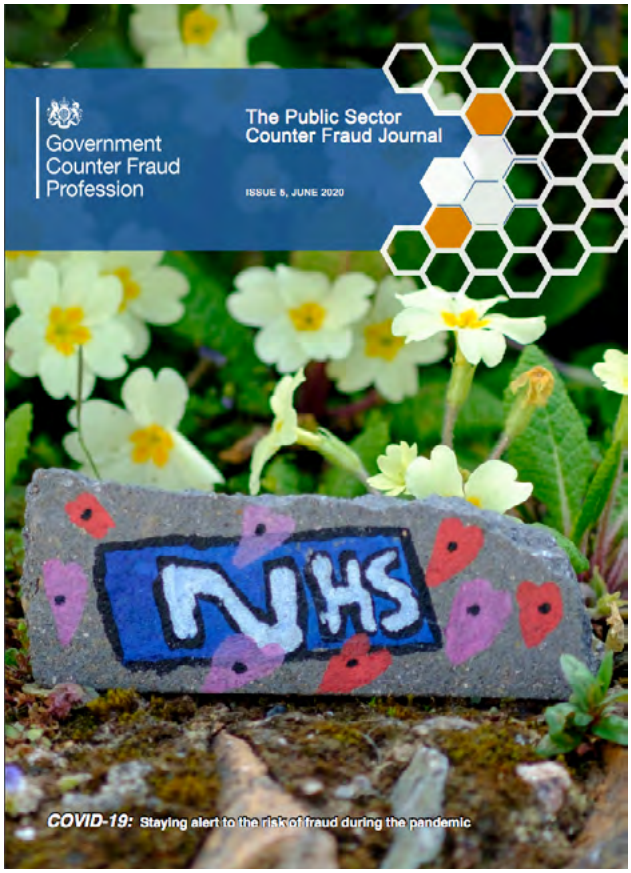
- Is the language of fraud failing its victims?
- Grants fraud
- Claims farming in insurance
- A career in counter fraud
- Scottish counter fraud community

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

Issue 4, March 2020

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

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



Issue 5, June 2020

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

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

Issue 6, October 2020

- Following the money
- Measuring the iceberg: the Fraud Measurement and Assurance Programme
- Positives in difficult times
- Can risk be your friend?
- Fraud fighters unite to defend the UK from COVID-19 crime
- Companies House Intelligence and Enforcement Unit: evolution to revolution
- The journey of a counter fraud distance learning graduate

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

Government
Counter Fraud
Profession

Contact us:

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