Government Counter Fraud Profession

The Public Sector Counter Fraud Journal

ISSUE 10, AUGUST 2023

ISSN 2755-1024

An ounce of prevention: Innovative approaches to stop fraud

Editorial Board

Toni Sless
Chair and Founder
Fraud Women's Network

Shawn Turner
GCFP Development Lead
Department for Work and Pensions

Professor Mark Button
Director of the Centre for Counter Fraud Studies

Laura Eshelby
Deputy Director,
Public Sector Fraud Authority

David Kirk
Consultant Barrister
RS Legal Strategy Ltd

Parveen Akhtar
Deputy Head, Public Sector Fraud Authority

Mick Hayes
National Operations Manager NHS Counter Fraud Authority

CoverImage:JohnCameronon Unsplash

CONTENTS

Editor's letter

Welcome to our first edition of the Journal for 2023! As we move into Quarter 3 of the year we are excited to share a wealth of articles with you, our counter fraud practitioners and stakeholders.

We will get the latest insights from the newly appointed CEO for the Public Sector Fraud Authority (PSFA), who we hope will be a regular contributor!

We also have a contribution from Chris McDermott, from the Commonwealth Fraud Prevention Centre (CFPC) in the Attorney General's Department - Chris has contributed to earlier editions and we are delighted while he is here on secondment with the PSFA that he has shared with us his development of 'Fraud Personas' and how they support understanding, finding and preventing fraud.

Colleagues from the NHS share their approach and efforts to tackle procurement fraud, including an article from Lorraine Harris where she shares the progress made and the impact this is having, leading to considerable savings for the taxpayer as a result.

Since we last published, there have been some exciting progress in the development and future aims of the Government Counter Fraud Profession - you can read more about this on page 17. The Profession offers a structure to bring together expertise and best practice for those working in counter fraud in government and beyond.

At the heart of the Profession are plans to promote inclusion and build future career paths for those starting their journeys in counter fraud. This edition includes a focus on the investigation apprenticeship and we meet two of the most recent individuals to successfully complete it, Charlotte Robson and Kylie McCarthy. I hope their reflections inspire others to consider an apprenticeship for themselves and their staff. I'm really excited to have an article from the newly formed Risk Threat and Prevention team of the PSFA, where Jac Davies shares highlights of the services they will be soon rolling out across the public sector.

Moving onwards to learn from other sectors, its great to have the spotlight on scams and emerging threats being identified by Mark Tierney, CEO of Stop Scams UK.

Keeping on this theme, other industry leaders sharing threat insights are CIFAS and in this edition we gain understanding of how specifically COVID-19 fraud is linked to a potential increase in risk of insider fraud, from one of their experts Tracey Carpenter.

We are also delighted to get some first hand insight from those also leading the work to do more to prevent fraud upfront, Shawn Turner and also Mark Bushell, who led for Deprtament for Work and Pensions (DWP) on the development of the prevention standards for professionals.

Finally, I would like to take this opportunity to thank two of our Editorial Board members, Jackie Raja and Maria Kenworthy, for their support with the development and delivery of the Public Sector Counter Fraud Journal. Jackie is retiring after nearly 45 years in the Civil Service - she joined the DWP when she left school and has had a formidable career within the Public Sector. Maria is stepping down as an Editorial Board member allowing her to commit to other priorities in the Ministry of Justice (MOJ). Speaking on behalf of the Editorial Board, I wish to add my enormous thanks to Jackie and Maria who have helped to make this Journal a reality. We will miss your counsel but wish you both the best for the future.

The Journal is published openly and based on our analysis has a readership of c12,000, across sectors.

I hope the range of articles are interesting to you and inspire you as you continue your efforts to protect your organisations and vital public funds from fraud. We are always planning ahead and seeking contributions for future articles.

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.

Laura Eshelby
Deputy Director, Public Sector Fraud Authority

Foreword

Mark Cheeseman OBE

Chief Executive Officer, Public Sector Fraud Authority

'No one who achieves success does so without the help of others'[1]

All those working in fraud and economic crime know that the challenge we face is large. Fraud is 40% of all crime[2] and, in the public sector, our best estimate of the level of fraud and error is £33.2 - £58.8bn.[3]

Individually, this can feel daunting, and the impact that we have can feel marginal. However, there are over 13,000 people within central government, and many more in other sectors, putting considerable effort into better understanding, and taking action on fraud and economic crime.

Collectively we can have, and have had, a huge impact. When we come together and collaborate, that impact can be even greater. Whether it is sharing practices and experiences, analysing what has worked, and what has not, the time we spend reaching out from our own roles to understand and collaborate with those facing the same challenge is often well spent.

That is one of the reasons that I am delighted that the Journal of the Government Counter Fraud Profession is being relaunched and reinvigorated. The time we take to share and learn from cutting edge approaches, practices and experiences through the Journal will help us as Counter Fraud Professionals to have a bigger impact - to go further in finding and fighting fraud.

1 Alfred North Whitehead

2 Crime in England and Wales - Office for National Statistics Appendix Table 2 - https://www.ons.gov.uk peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingdecember2021#fraud

3 Page 23 Cross - Government Fraud Landscape Report Annual report 2022 - https://www.gov.uk/government/publications/cross-government-fraud-landscape-annual-report-2022

And we need to challenge ourselves to go further. While we should be proud of the individual and collective impact we have had in the past, we know that our adversaries - those who commit fraud - are capable and their methods are evolving quickly. In government, we have been asked to increase our ambition in finding and dealing with fraud. We now need to rise to that, and challenge ourselves to continually improve in understanding and fighting fraud.

Public Sector Fraud Authority

In August 2022, the government launched a new Authority to work with departments and public bodies to better understand and reduce the impact of fraud against the public sector. The new Public Sector Fraud Authority (PSFA) is being built scrutinise performance across the public sector, to support public bodies through expert services and by continuing the public sector's journey in the professionalisation of fraud expertise.

The PSFA is recruiting experts to help build and deliver these services and functions. However, to be successful, it will have to build strong relationships with experts across the public sector and more widely (in other sectors and administrations). It is in bringing this expertise together, and creating an environment where their experiences and learned capability can be drawn into leading practice and standards, that we will be able to better collaborate and increase our ambition and impact on the challenge of fraud.

Increasing our Ambition - Four Focuses

The Covid-19 Pandemic was a huge collective experience. To deal with the impact of a global health crisis, the government supported individuals and businesses with a range of schemes. As with all crisis situations, the focus was, for good reason, on the pace and accessibility of this support and a higher level of fraud risk than in usual circumstances was acknowledged and accepted.

Since the pandemic, the UK government has invested over £1bn in action to reduce fraud (and error) loss. The creation of the PSFA was part of this investment. The PSFA is working with departments and public bodies to modernise how we deal with fraud. We know the nature of fraud has evolved quickly over the past decade. How we fight fraud is changing to meet this and the PSFA will work with public bodies to cement a modern approach, rooted in an understanding of risk and the deployment of data and technology to reduce risk and detect residual fraud levels, alongside the more traditional approach of awareness and investigative action.

This modernisation is rooted in our most recent experience - the pandemic. From this there are four focuses which underpin how we will be working to better understand and reduce the impact of fraud.

1. Working to get more fraud expertise in up front and making a step change in prevention.

The more we can develop our expertise in understanding fraud, and the tools and techniques we can use to prevent it, the better we can reduce fraud by making it hard to commit.

This means developing, and respecting, expertise in fraud. It has become an increasingly specialised area - where most have some experience but the difference in capability between the interested and the expert is becoming more and more marked.

It also means that fraud experts should challenge themselves to get better at understanding business processes, exploring new tools for preventing fraud, and measuring their impact when they do so.

2. Taking more and better action where fraud occurs.

As the volume of fraud and misclaiming increased in the pandemic, it became harder to take action. Those who were more able to take action were those with access to powers and capability as a result of facing and taking action on fraud and misclaiming in the past. We know that crises can affect any part of the public sector and our experience in the pandemic gave us a basis on which to increase both the powers available to our organisations and the increasingly diverse capabilities that we need to draw on to effectively take action on fraud.

This means proactively getting ready to deal with fraud, making sure our organisations have access to powers and experts, and are using them not just to take action, but also to be ready to take action.

3. Increasing the use of data, analytics and intelligence to find fraud.

The advent of the digital revolution has brought increased accessibility to services, information and entertainment for all of us. Sadly, the tools that we use to improve our lives have also been used by fraudsters to attack both us and public services. We are all familiar with mass scam messages and phishing attempts, and should be under no illusion that some of those who commit fraud are also looking at how to use data and tools, like AI, to make their attacks more effective.

Whilst these tools are frustratingly powerful in the hands of fraudsters, they are also transformational tools for those who fight fraud. Counter fraud specialists and organisations should challenge themselves to understand how these tools and techniques can be used to mitigate their fraud risks and look for the residual fraud and misspending in their systems. Any organisation that is not considering this is leaving itself vulnerable - it is really a case of when and how, rather than if.

4. Resolutely focusing on performance and outcomes.

During the pandemic, we saw that those parts of the system who measured their investment, and the financial outcomes of taking action on fraud and misclaiming, were much more able to react quickly to the changing threat level.

Historically, much counter fraud investment has been on a

'value' base, an investment because one should, or it is the right thing to do. These investments have not necessarily had measurable outcomes. Sometimes the focus has been on producing the right paperwork, and talking about fraud to build awareness, rather than using these as the foundation to take measurable action to find fraud and misspending and reduce the risks.

It is a more difficult path to focus on performance and outcomes, but also the right one. Fundamentally, an investment in counter fraud is a business choice - meaning investment is not going elsewhere. Expertly done fraud work is a benefit for the business, because it both suppresses cost and can make financial savings through reducing loss. An investment into fraud and compliance can be a win/win, giving the organisation more confidence in the integrity of its payments and receipts while also saving money.

If we want to increase our ambition and have a bigger impact, this is the route to take. It will enable us to demonstrate our value, and to make cases for further investment to take on the often unseen and underestimated problem of fraud and misspending.

PSFA Plan - From Understanding to Action

The Public Sector Fraud Authority has used the experiences in the pandemic to underpin its approach. This can be seen in its published plan[4], which we will continue to publish each year.

Inherent to the delivery of this plan, and in the modernisation of fraud management in the public sector, and more widely, will be continued collaboration and cross system working to test new ways of working - from prevention methodologies to data and analytics techniques - and to share learnings and practices. The UK government is doing this in a systematic way - to build structures that will help those working to fight fraud now have a bigger impact, and help those who pick up the mantle in the future.

Building for the Next Generation of Counter Fraud Professionals.

In 2018, the UK created the first professional structure for those working in counter fraud roles - the Government Counter Fraud Profession. This set out the skills, knowledge and experience that was expected of those undertaking fraud roles - from investigators, to intelligence officers, to risk assessors and beyond. Since 2018, the government has continued to build the Profession, launching an investigator apprenticeship, from which we had the first graduates this year, and new professional and practice standards.

Fighting fraud has become an increasingly complex - and expert - activity. Tools and techniques from all disciplines have become more sophisticated and deep expertise and experience is needed to be effective.

Recognising this, the Counter Fraud Profession has become an integral part of the Public Sector Fraud Authority - within the new Practice, Standards and Capability Function of the organisation.

Our collective drive to increase our capability will be essential to us making good progress on the four focuses - and it will need to be a collective endeavour. Across the public sector and private sector and administrations, those fighting fraud are having experiences, be they successful or otherwise, as they try and find increasingly effective ways to understand and take action on fraud.

By having a recognised structure (the Profession) that we are investing in, we intend to bring together many of these learnings to help make sure that we collectively improve and can have increasing impact.

That way we can make sure that both us, and future fraud fighters, can be more confident and more capable, able to face the daunting task with more certainty and well rooted determination, knowing that we are calling on leading tools and techniques.

That way, together, we have more impact on the problem - pushing back against those who attack our public services and ensuring more public money goes to where it is needed most.

This Journal is part of that journey - making the thoughts and experiences of leading thinkers and doers available to those who are taking action. I hope you enjoy it.

4 Public Sector Fraud Authority 2023/24 Delivery - It contains the key activities and outcomes the PSFA expects to deliver by March 2024.https://www.gov.uk/government/publications/public-sector-fraud-authority-202324-delivery

Introducing a powerful and versatile tool to underpin your counter fraud capability: the humble Fraudster Persona

In February this year, the Australian and UK Governments announced a new strategic partnership between the Commonwealth Fraud Prevention Centre and the Public Sector Fraud Authority. Sharing expertise and capability across our two countries will better equip, enable and empower our respective public sectors to find, prevent and deal with the increasing problem of fraud.

Author:
Chris McDermott
Director of Capability and Development in the Commonwealth Fraud Prevention Centre. Between April and June 2023, Chris was seconded to the UK as a Deputy Director in the Public Sector Fraud Authority.

I've also had the pleasure of being seconded to the UK for three months between April and June to further solidify this partnership and share some of our experience working with Australian public bodies to strengthen their counter fraud capability.

Fraudsters are a committed adversary, consistently finding ways to evade the controls we put in place to counter them. Yet while fraud schemes vary in their complexity and creativity, fraud intelligence and investigations reveal that those who commit fraud tend to also use common tried and tested methods to mislead or exploit the system.

This may seem like a contradiction – how can a fraudster be both creative and re-use the same methods?

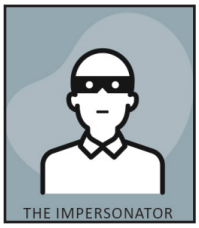
It is similar to an artist – they may always use oil paints and a brush, but no two artworks are the same.
Controlling fraud risk is an equally creative yet methodical process, and it helps to think like a fraudster to identify threats to your public body's schemes and functions, or when looking for vulnerabilities in controls. But how can we anticipate how a fraudster might target our schemes and functions so we can put the right controls in place to counter them?

Some studies have analysed the characteristics of the people who commit fraud to build a profile of a typical fraudster and identify risk profiles for individuals. For example, they compare demographics to identify common characteristics of fraudsters, such as age, gender, level of education, position and tenure. While there is some value in this research, these profiles can be seriously misleading. Cases of fraud consistently demonstrate that all individuals, not just those that fit a typical profile, are capable of committing fraud.

The Fraudster Personas developed by the Commonwealth Fraud Prevention Centre are different to the typical profiles – they are based on how fraudsters commit fraud. Intelligence and fraud investigations across all different types of schemes and business functions reveal that fraudsters:

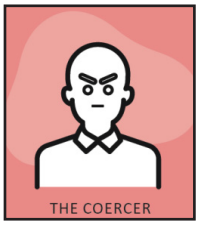
Are often Reckless – acting without care, responsibility or regard to the consequences of their actions (including the harm caused to others).

Deceive – making others believe something that is not true.



Impersonate – pretending they are another person or entity.

Fabricate – inventing or producing something that is false.



Coerce – influencing, manipulating or bribing another person to act in a desired way.

Exploit – using something for a wrongful purpose.

Conceal – preventing actions from being seen or known about.

Sometimes Organise - using a combination of methods in a planned, coordinated and sophisticated way.

Here are 8 examples of how these 8 Fraudster Personas can practically support a public body's fraud prevention efforts:

1. Raising awareness about fraud

A key objective of fraud awareness messaging is to raise sustained awareness of fraud, particularly among the first line of defense. Fraudster Personas are an engaging and practical tool that can help employees quickly and easily grasp what fraud looks like, the typical actions they need to be looking for, and what to report.

A growing number of public bodies in Australia and New Zealand use the Fraudster Personas in their fraud awareness campaigns, including use on posters, flyers, factsheets and screensavers.

2. Educating people about fraud

Fraudster Personas can help you educate employees about how people commit fraud – particularly when combining them with relevant case studies.

Multiple public bodies in Australia use Fraudster Personas to educate staff through face-to-face training. For example, the Australian Taxation Office (ATO) has applied the Personas to their own context using ATO case studies.

3. Identifying fraud risks

A good fraud risk assessment helps you identify how fraudsters could target your public body's schemes and functions. The processes should be both evidence-based and creative. Those completing the assessment need to consider who might defraud their scheme or function and how they would do it.

An innovative approach used by Australian public bodies is to combine Fraudster Personas with business process mapping. By identifying different risks across the business process, you can better understand where and how a scheme or function might be susceptible to fraud. This will also help you communicate these risks to stakeholders and decision makers, and co-design proportionate and effective controls at the right point in the process.

4. Identifying control vulnerabilities

In my previous GCFP Journal article in 2019, I highlighted the research which consistently shows that gaps or weaknesses in controls lead to more fraud than any other factor. When asked to identify threats and vulnerabilities within a scheme or function, it is often suggested that officials should 'think like a fraudster'. Fraudster Personas give these officials more practical direction on how to adopt a fraudster's mindset.

If you can anticipate the actions of fraudsters and discover precisely where and how your public body's schemes and functions are vulnerable, you are then better equipped and informed to prevent, detect and deal with fraud. Moreover, as they represent the different actions fraudsters use, they are an effective tool to test, probe and find creative ways to bypass controls – just like fraudsters do. Australian public bodies regularly use the Fraudster Personas in this way to identify control vulnerabilities. Building off the success of this approach, the Fraudster Personas will be an important component of a new Fraud Control Testing Framework that I'm developing for the UK public sector.

5. Identifying data requirements to counter fraud

Having a clearly defined purpose for sharing data can help you plan and establish the right type of arrangement to meet your specific needs. A clear purpose can also help others understand why you are requesting data and what you are going to do with it.

Fraudster Personas can help you identify and articulate your purpose in a really clear way – helping to increase trust and buy-in from executives and stakeholders. Fraudster Personas can also help you articulate your requirements for fraud data analytics. These requirements should be informed by specific fraud risks at particular points in a scheme or function.

6. Designing more fraud resilient schemes and functions

Fraudster Personas can help policy teams, business teams and counter fraud teams co-design more fraud resilient programs and functions. Using Fraudster Personas alongside other policy design tools, such as business process mapping and customer journeys, can help you proactively identify how participants, providers or third parties might undermine the policy or program outcomes through fraudulent means.
Adding Personas to your public body's policy and program design toolkit will help build integrity into the design of schemes and functions from the outset, rather than retrofitting controls later.

7. Deterring fraud through messaging

Fraud messaging can be an effective and low-cost method for reducing potential loss from fraud by influencing people's behaviours and decisions. For example, the messages we communicate can change a person's beliefs and perceptions about the risks and possible benefits of committing fraud. Reducing a person's ability to rationalise their actions can be the determining factor in stopping them from attempting to defraud the government or continuing to commit fraud.

Furthermore, behavioural research has found that a person's fear they might get caught offending is a much greater deterrent than their fear of the consequences that would follow. Therefore, an effective message to communicate when looking to deter fraud is that your public body has structured processes in place to find fraud, discrepancies will be discovered, and offenders will be caught.

Fraudster Personas can help you clearly communicate this message by highlighting to would-be offenders that you are aware of how people commit fraud and you have ways to detect them.

8. Reporting about fraud

Countering fraud can be complex, technical and sometimes counter intuitive. Fraudster Personas can help you report types of fraud and counter fraud activities in a clear, simple and compelling way. How the audience understands these activities is largely dependent on how the results are presented.

Using Fraudster Personas as a visualisation tool or as reporting categories can help management, stakeholders and risk committees understand the types of fraud impacting your public body's schemes and functions. This approach can help you highlight the methods fraudsters are using against different schemes and functions or the types of fraud that are causing the greatest material impact.

This can sharpen their focus on ways to prevent, detect and respond to these actions. For example, a higher prevalence of The Impersonator could help them direct resources into strengthening identity controls, while a higher prevalence of The Exploiter could help them prioritise efforts to improve internal controls and awareness campaigns.

As you can see, Fraudster Personas are a powerful and versatile tool that can be immediately adopted and used in different practical ways.

What are some ways you could use Fraudster Personas to underpin your public body's capability to counter fraud?

Learn more about the work of the Commonwealth Fraud Prevention Centre, including Fraudster Personas, at **www.counterfraud.gov.au.**

Fraud prevention in procurement

Author:
Lorraine Harris
Fraud Prevention Manager with the NHS Counter Fraud Authority

Since its inception, fraud prevention has been an essential strategy for the NHS Counter Fraud Authority (NHSCFA). This has been particularly important in the area of NHS procurement fraud due to it being a huge area of spend and activity but with a relatively low level of fraud reporting. At the NHSCFA we understand all too clearly about the negative impact that fraud can have on people's lives.

The National Health Service is an emotive subject for many of us living in England, as it touches all our lives, whether at birth, maintaining our health or treating illnesses. The impact of fraud simply delays patient care whether through the diversion, delay or availability of funds which can go on to affect the provision of staff, services and medical equipment.

This article will explore how NHSCFA has successfully undertaken a range of proactive fraud prevention activity resulting in the reduction of financial vulnerability to fraud in the area of NHS purchase order (PO) spend.

What is the purchase order fraud risk?

The risk of fraud in the procurement process is significantly heightened when purchasing activity does not follow the organisation's pre-established procurement protocols and policies. Risk of fraud is mitigated when organisations use established control mechanisms such as their purchase-to-pay (P2P) / PO system.

Where non-PO spend occurs, an organisation is exposed to a far greater risk of fraud in the procurement process. Spend via the organisation's pre-established procurement route (i.e., the P2P / PO system) acts as a deterrent and mechanism to prevent fraud.

Ideally all purchases made within NHS organisations should be raised by PO using an electronic P2P accounts payable system with key controls around separation of duties. This provides budget holders with a means of oversight ensuring non-pay expenditure is controlled. Non-PO spend is not fraud, but it exposes organisations to a far greater risk within finance and procurement systems.

The national exercise

In 2019/20, NHSCFA estimated the financial loss to fraud, wastage and error from procurement and commissioning budgets to be approximately £300.4 million[1]. In the same year, a national proactive exercise was undertaken, directed at building a more accurate understanding of financial vulnerability exposure in procurement and commissioning, and tackling fraud risk vulnerabilities within NHS procurement systems. By asking NHS organisations to undertake local proactive activity, NHSCFA was able to establish an understanding of procurement fraud risk and identified financial vulnerabilities within NHS P2P / PO systems.

The national exercise comprised three phases:

1. Collecting baseline data in 2019;
2. Influencing behavioural change through a national fraud prevention campaign; and
3. Collecting comparable data in 2021 to understand the impact of the national fraud prevention campaign.

What data did NHSCFA collect?

Each NHS organisation was asked to identify, by quarter, the following information sets, broken down by different spend types (the NHS-eClass system[2] was used to classify spend):

- All spend by spend type; and
- Spend that did not link to a purchase order, by spend type.

The 2019 data collection (for the 2018-19 financial year) acted as the baseline dataset, and the 2021 data collection (for 2019-20 financial year) acted as the comparable dataset. These two datasets were collected to analyse the level of non-PO spend present in each NHS organisation and the impact of NHSCFA-led fraud prevention activity. We requested data to be broken down by the NHS-eClass system so that comparisons could be drawn between different spend types.

1 NHS Counter Fraud Authority (2021) Strategic Intelligence Assessment 2021

2 NHS-eClass is a bespoke classification system for products and services, owned by the English NHS. The purpose of NHS-eClass is to facilitate the accurate analysis of expenditure.

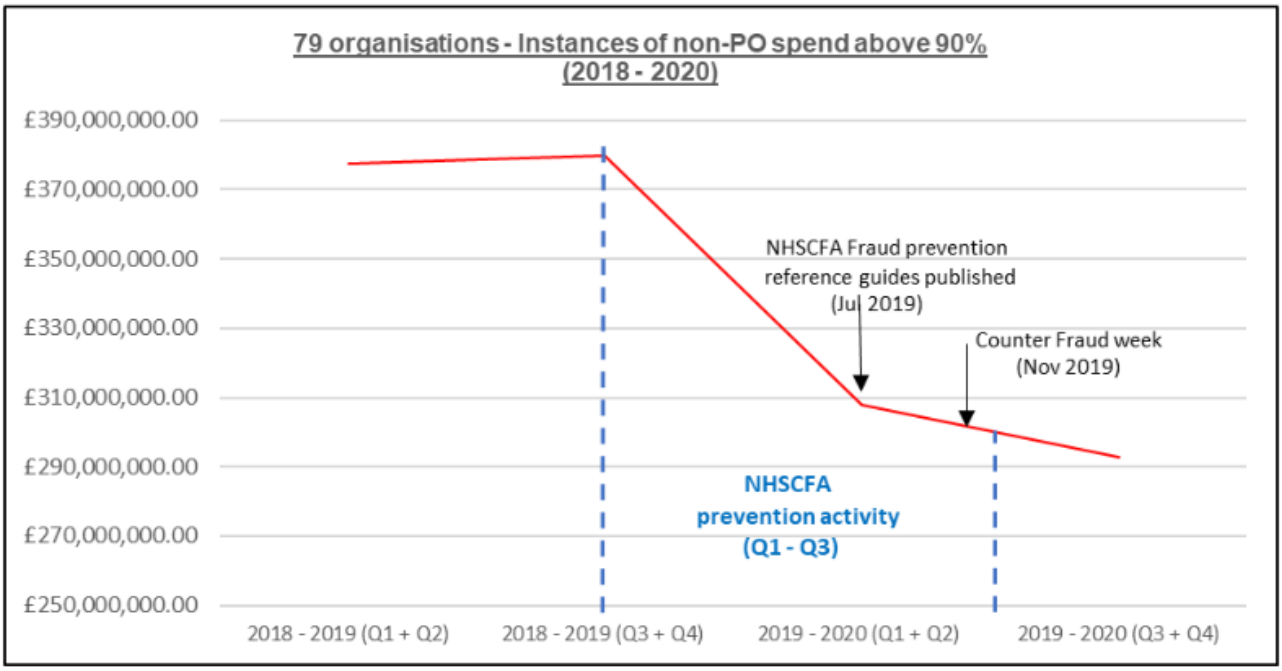


Figure 1: Instances of non-PO spend above 90% in categories above 30% 2018-2020 (79 organisations)

Phase 1 of the National Proactive Exercise (NPE) demonstrated positive participation, achieving an 81% return rate from NHS organisations[3] which in turn provided a substantial basis for analysis work undertaken to establish the baseline indicator.

The success of phase 1 and positive engagement encouraged a 10% increase in response rate (91%) of participating NHS organisations in the comparison dataset exercise (2019 – 2020) for phase 3 of the project.

Influencing behavioural change

NHSCFA led a fraud prevention campaign of prevention activity to influence behavioural change across the NHS procurement landscape, thereby effecting change in staff and organisational behaviours. The campaign purposely targeted NHS staff in procurement and finance teams to educate and increase awareness of fraud risk vulnerability within finance and procurement processes. The range of activities and products NHSCFA provided to support behavioural change included: targeted workshops and focus groups, webinars and a range of procurement focused fraud prevention guidance documents. A toolkit was also developed to assist the local counter fraud community with implementation and engagement activities on procurement fraud prevention.

A series of eight fraud prevention quick guides were created focusing on specific areas of fraud risk vulnerability in NHS finance and procurement:

- Contract splitting (disaggregate spend)
- Contract reviews
- Buying goods and services
- Due diligence
- Suppliers' code of practice: preventing fraud, bribery and corruption
- Mandate fraud
- Petty cash
- Credit card.

The purpose of the guides was to reduce the NHS's vulnerability to procurement fraud by helping organisations to embed control measures and implement preventative action.

NHSCFA also undertook site visits at 25 NHS organisations of varying sizes and types, meeting with Directors of Finance, Heads of Procurement, and Local Counter Fraud Specialists to identify the impact of the campaign, promote good practice and further promote implementation of NHSCFA's fraud prevention materials.

Feedback obtained from the site visits undertaken by NHSCFA staff established that the campaign had supported internal policy and procedural change in many NHS organisations. Several key themes emerged from these engagement meetings, particularly around the difficulties associated with managing contracts and contract oversight within NHS organisations. The visits also revealed NHS organisations were undertaking reviews of local policies, procedures, and Standard Operating Procedures against the fraud prevention guidance and developing action plans to raise awareness.

3 231 NHS organisations in England and 9 NHS (Welsh Health Board) organisations in Wales were invited to participate in the NPE, of which an 81% response rate was obtained covering all three areas of fraud risk vulnerability; Disaggregated spend, Contract management and PO vs non - PO spend.

Financial vulnerability exposure

Financial vulnerability exposure (FVE) is designed to give an indication of the exposure of the NHS to potential fraud. It should not be used as a financial instrument or to categorically define losses to fraud. FVE has been introduced to NHSCFA's Strategic Intelligence Assessments [4]and more accurately reflects the nature of intelligence and the confidence the NHSCFA can attribute. For example, we may not be able to say that something is exposed to fraud exclusively, but we can have more confidence in stating that something is exposed to fraud, wastage, or error. This provides more clarity and context around fraud risks.

To understand whether fraud prevention activity had influenced a reduction in FVE, NHSCFA assessed the value of the most vulnerable instances of non-PO spend to identify if spending behaviour was positively or negatively impacted. This could only be achieved by looking at the 79 organisations that participated in both data collection exercises (2019 and 2021).

NHSCFA led fraud prevention activity nationally that was implemented locally in NHS organisations with the outcome of influencing a reduction of £156.8 million (from £757.4m to £600.6m) in financial vulnerability exposure across 79 NHS organisations that participated and provided data across both data collection exercises (baseline and comparable), see Figure 1.

This is fraud prevention in its truest sense in that the aim was to stop fraud before it occurred by influencing behavioural change. NHSCFA achieved its aim to have a positive impact by influencing behavioural change and thereby reducing the most vulnerable instances of non - PO spend across the NHS provider sector.

Conclusion

The exercise had a positive outcome with approximately half the sample data demonstrating a significant improvement in the reduction of non-PO spend, however the other half presented a significant increase in non-PO spend. This demonstrates there are still lessons to be learnt, and ongoing prevention interventions are required. We have demonstrated that behavioural change does result in a positive impact in reducing risk and vulnerability to fraud, however it requires constant vigilance.

NHS organisations must disrupt these practices by reinforcing existing organisational Standing Financial Instructions, policies and procedures through embedding a culture of PO spend. This should be supported by the implementation of regular audits on departments' performances with staff being held to account if procedures are not followed.

NHSCFA continues to work on preventing NHS procurement fraud and will be focusing next on how it supports the sector to improve due diligence and contract management.

If you have any suspicions or concerns about fraud, bribery and corruption affecting the NHS, report them to the NHSCFA. You can report online or call **0800 028 4060**. All reports are treated in confidence and you have the option to report anonymously.

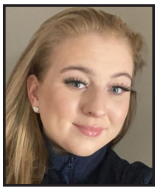
4 The Strategic Intelligence Assessment provides an annual assessment of the threats faced from fraud and an overarching estimate on the losses from fraud to the NHS. It is neither a risk assessment nor an audit document. The losses presented are an estimate based on available information at the time of writing.

Fireside chat

Last month at the inaugural Counter Fraud Investigators Apprenticeship Conference we caught up with Kylie McCarthy and Charlotte Robson….

The Counter Fraud Investigator standard was the 500th new apprenticeship approved for use for employers and learners. The Level 4 Counter Fraud Investigator Apprenticeship launched in October 2019, to train the next generation of fraud investigators. This two-year programme provides structured learning (combined with on the job experience) and on completion it enables individuals to run both civil and/or criminal investigations.

Authors:
Kylie McCarthy is an investigator with the Education and Skills Funding Agency, an executive agency of the Department of Education; Charlotte Robson is an investigator in the Durham County Council Counter Fraud Team.



Q: How did you find the Counter Fraud Investigators Apprenticeship programme?

Kylie: I really enjoyed the course. Being new to investigations I don't feel I could've done the role without doing the apprenticeship. For me the two come hand in hand.

Charlotte: From someone coming from an apprenticeship that I found difficult to link with the job I was doing, the Counter Fraud Investigators Apprenticeship (CFIA) was much more fitting to my job role and I am grateful to have been the first to complete the pathway. The CFIA was well organised, help was always on hand. I had a very positive experience. There was a manageable amount of work to be done using off the job hours and the tasks set for each module I felt were fair.

Q: What were the challenges you faced and overcame?

Kylie: My main challenge was achieving my functional skills in maths. I had math anxiety which I have had since I was a child. I knew my next career move was going to incorporate an apprenticeship of some sort and I had to make sure I was ready to take on the maths challenge. My tutor was extremely supportive and she fostered the right environment which meant I was able to learn. My tutor, line managers and colleagues were all very supportive and understanding it was because of this support I was able to move through my anxieties. I am sure there are plenty of people who are put off from completing an apprenticeship because of anxieties surrounding maths and English. I want to let these people know that this was the one of my biggest personal challenges I had to overcome with the biggest reward of self-accomplishment. If I can do it, anyone can.

Charlotte: A challenge I faced was having trouble comparing some of the examples used in the programme, to a Local Authority (LA). A scenario to make it more relatable to me and my role. I overcame this by talking with my peers and other people working for LA on the cohort.

Q: What were the highlights of the CFIA?

Kylie: My highlight was applying what I had been taught about interviewing (practical and theory) and putting it into practice. My first interview was with the Director of an educational provider. My line manager asked if I wanted to lead the interview and my default position was to sit back and allow others to lead however, I decided to go for it. I used my notes from the course and made sure I prepared as best as I could. The interview went well. There was a good flow of questioning and because I had lived and breathed the case, I felt confident challenging the Director. I asked my line manager for feedback, and he agreed I had prepared well and the questions flowed, he gave me feedback on areas of improvement which I welcomed. As investigators we need to keep learning and developing ourselves. It was because of this interview I started to see myself as an investigator not a trainee.

Charlotte: My highlight was making friends, gaining confidence and exposure to things I had not yet faced in my role. The main highlight was becoming qualified and being able to apply for a promotion.

Q: How did you balance your work and home commitments with studying for the apprenticeship?

Kylie: My manager and senior managers from the outset saw the importance of the apprenticeship and ensured I had enough time to complete on the job training[1], assignments etc during working hours, in order to be compliant with the funding rules.

1 'On-the-job' training is delivered by the employer, such as skills and knowledge that fall outside of the apprenticeship, but are required for the job role.

Managers did their best to provide suitable work experience to ensure I could achieve my on the job training and End Point Assessment (EPA). I am a mother of two small children and I work full-time which means I have very little time outside of work.

Charlotte: My line manager was great in providing the off the job hours[2] expected and wouldn't hesitate to give me more time if needed to complete a task, I also tried to forecast any priorities in the coming months to plan when I would have time to focus solely on the apprenticeship. I ensured to keep up my hobbies outside of work as an outlet, netball and looking after my horses.

Q: How did you manage your time?

Kylie: Off the job hours were worked out at the beginning of the course, and I shared this with my line manager and I allocated this time in my diary. I was very protective of this time as was my line manager, we made sure I used the time for coursework only[3]. By doing this I never fell behind with my off the job hours or assignments.

Charlotte: I made the best use of my time by utilising diary organisation, ensuring I made the most of the off the job hours that were given. During busy periods, my line manager allocated me less cases so my normal workload did quieten down to make up for the increased workload specifically when preparing for EPA.

Q: What advice would you give to others who are undertaking the apprenticeship or are thinking about undertaking the apprenticeship?

Kylie: My advice would be scheduling breaks and taking them - this helps to prevent burnout. Halfway through the course I realised I was doing too much. I spoke with my line manager and we both realised I needed to take a break. We are not superhumans and it's important to find your voice and say when enough is enough, stop, recharge and then go again. Also, if fear is holding you back, in my experience sharing your thinking with someone you trust i.e. line manager, colleague or loved one etc, helps to see the truth from the false and break down barriers which we have created in our heads.

Charlotte: Do it! An apprenticeship is a great way to widen your knowledge and qualifications, a different route to university, and still the same outcome. I would only just be finishing university if I had done the course I intended, but instead I have a level 3 and a level 4 apprenticeship under my belt, I am fully qualified and in no debt that university would have given me.

Q: Some of our apprentices, in the room today, will be planning for their EPA – can you give them any advice?

Kylie: Look at your off the job hours and gauge for yourself where you are and schedule time each week to complete them. If you need more time allocated to complete these hours then speak with your line manager. Most managers are reasonable and want you to succeed, it's important you complete your apprenticeship because you have worked so hard until this point, it's time to see it through. Look at your EPA guidelines and ensure your example for your assessment is in line with the EPA. Your mock EPA is important as this is when you can make mistakes in a safe environment. Ask for feedback and listen and use that feedback to improve. If you have timings for presentations etc make sure you time yourself and you have a clock, as timings are important in passing your assessments.

Charlotte: Try building up your portfolio of evidence as early as possible so you are not leaving things till the last minute. Another piece of advice would be to plan the case you are going to use as part of your EPA and familiarise yourself with it as much as possible. Don't let it be daunting for you, remember you are talking about what you do every day and you know your job.

Q: What support were you provided with in your organisation and did this help?

Kylie: An apprenticeship is a three way relationship between learner, employer and training provider. To have a successful apprenticeship all three parties must work together and come together regularly at the progress reviews, the aim of these is to improve the learner's knowledge. In my experience the three-way relationship worked extremely well. I had full support from my line manager, who offered a level of praise and challenge. My training provider recognised the amount of effort I was putting in and also gave me nudges in the right direction. The learner must take full responsibility for their learning. You are in the driver's seat. Be open and honest and if you need help ask, most people want to help. As a learner you are supposed to feel stretched and challenged; anything less or more has to be addressed and monitored.

Charlotte: My line manager went above and beyond to make sure I had enough time to carry out what was expected of me from the course, I was given all off the job hours.
We also made a group chat for those in our cohort and were able to use this to talk about any queries and help support each other along the way.

Q: Looking back at your apprenticeship journey would you change anything?

Kylie: No, it happened at the right time. I started my apprenticeship at the start of lockdown. This gave me something positive to focus on. If someone had asked before lockdown, how do you prefer to learn virtually or face to face, I would have said face to face. Now, I would

2 Off-the-job' training is delivered during the apprentice's normal working hours. This must deliver new skills directly relevant to the apprenticeship standard.

3 Apprentices are required to spend at least 20% of their working hours completing 'off-the-job' training. This time is protected as it is a legal requirement for apprenticeship delivery.

say a mixture. I enjoyed learning in a virtual classroom. I found it less stressful regarding logistics etc. Also, systems are very interactive now and we worked in small groups etc. It was a positive experience. It was great mixing with the cohort in person as not only were we doing the course together we were also from the same team based in different locations, so getting together was lots of fun. Mixing with different cohorts in different organisations was interesting and helps to embed learning as different organisations do things differently and you can all learn from each other.

Charlotte: The thing I would change would be to start planning my EPA earlier.

Q: What made you decide to choose counter fraud as a profession to take?

Kylie: I had been working in the Post-16 education sector for a few years and I knew I wanted a change, however, I wanted to keep my knowledge of the sector. Working in the Department for Education (DfE) they promote apprenticeships and I had a few discussions with my then line manager on what to do next. During a team away day the investigations team did a session and I saw from their organisation chart they were looking for an Apprentice Post-16 investigator. I discussed this with my line manager. Within a month I stepped into the team as an apprentice.

Charlotte: I was always interested in pursuing a career in law, I went to sixth form and after a year realised that it wasn't for me. I then started looking at what apprenticeships were available and knew this would be something I would be interested in, and linked to the subjects I was studying at sixth form. I have a passion for counter fraud and have developed my skills and knowledge to become a well-rounded investigator for the five years I have worked in the Local Authority Counter Fraud Team.

Q: What's next? Has this inspired further study?

Kylie: During my apprenticeship I discovered a love for learning. I achieved my apprenticeship at the end of February this year and then started my Institute for Leadership and Management (ILM) coaching and mentoring level five at the end of March 2023.

I want to help others release their full potential.

Charlotte: For me, I have been in education since I was 4 years old. I have a vast amount of qualifications now and plan to focus on my new promotion and progression within my role, carrying out things such as more interviews and looking at more criminal cases to progress.

Q: Are you now using the skills developed in your work-place?

Kylie: I could not have been an investigator without completing the Level 4 CFIA. Most of the things I learnt during the apprenticeship I have put into action in my role. The knowledge I have gained means I am able to influence and develop procedures, in particular interviewing. Managers were so impressed with the apprentices interviewing skills they have been working with the training providers to offer refresher sessions with colleagues to help develop their skills. As an organisation we don't complete IIMARCH [briefing model][4]. I am going to use this tool for my current case as we need to cease learner files from multiple sites. This ensures we follow the correct policies and procedures and to ensure we secure the best evidence.

Charlotte: The skills I developed on the apprenticeship are embedded every day in the work I carry out from the beginning of an investigation, to understanding the legislation all the way through to the final closure report.

Q: What are the next steps for you in counter fraud and within the Government Counter Fraud Profession (GCFP)?

Kylie: Next steps for me is to complete my ILM coaching and mentoring level five and also, apply for promotion in counter fraud/enforcement/investigations when the opportunity arises. This is the most confident I have felt when thinking of applying for promotion and I believe this is because I successfully achieved level 4 CFIA and functional skills math.

Charlotte: To continue with my CPD and the GCFP, I have been given responsibility for some of our tenancy fraud work with a large client that will eventually look at training on the financial investigation pathway.

Editor's note:
If this article has sparked your interest please do get in touch to see how you can get involved in the Level 4 Counter Fraud Investigators Apprenticeship to help build capability across government and public bodies.

Email us to find out more: **gcfp@cabinetoffice.gov.uk**

Further details of the Level four Counter Fraud Investigators Apprenticeship and the assessment criteria can be found at: https://www.instituteforapprenticeships.org/apprenticeship-standards/counter-fraud-investigator-v1-0

Institute for Apprenticeships and Technical Education

4 Information, Intent, Method, Administration, Risk Assessment, Communications and Humanitarian Issues is the briefing model used by investigators.

The Government Counter Fraud Profession

Author:
Laura Eshelby
Deputy Director, Practice, Standards and Capability, Public Sector Fraud Authority.

In March 2023 we published the three year strategy for the Government Counter Fraud Profession (GCFP), setting out the aims and ambitions for the next three years. This helped us to focus the direction and areas for growth following the pause in development during the pandemic, which led to resources in the central team in the Cabinet Office being diverted to other vital counter fraud work.

The strategy was the result of engagement and discussion with experts across the public sector and beyond including industry leaders. The strategy is focussed on five key areas.

Taking these in turn I will update on the progress to date and plans for growth in these areas over the next few years. This is to be transparent with members of the Profession, and interested stakeholders, to encourage wider engagement and involvement of those of you in the public sector and industry not already engaged in helping us accelerate the professionalisation of counter fraud. Maybe you are on your own journey as a lead in an organisation or seeking support to develop and grow your counter fraud talent. If so, do reach out and get involved in the many forums we bring together to do this.

Investment in leadership skills now and future

We have started the work to develop a bespoke leadership programme for those in senior leadership in the civil service. This has been piloted and lessons learnt are now being evaluated to build into the business as usual delivery, with applications for public sector leaders opening this Autumn. We want to turn our attention next to how we support emerging and future leaders, and build a pipeline of talent for the public sector and how we can support interoperability across sectors to benefit us all.

Building deep counter fraud capability

We have started to build towards recognition of those working in counter fraud disciplines, beyond investigation, intelligence and data and analytics - to recognise the skills of fraud risk assessment (FRA), measurement and prevention, underpinned by culture.

This financial year to date we have trained 46 people in FRA, (against a total year target of 100), who are now completing their assessments to consolidate their knowledge. We have commenced work to uplift the existing training provision on FRA to incorporate initial fraud impact assessments, allowing early consideration of fraud risks for all major schemes across the public sector. We will start work now to develop new training offers, including for fraud loss measurement, scope the potential for a new apprenticeship in counter fraud and training provision for prevention. Bringing this all together to ensure there is a variety of mechanisms and routes to market over the next few years, providing both value for money and quality learning options for members. We want to bolster this focus with practical tools to help organisations and senior leads plan with their fraud staff their unique pathways into the profession. We will be introducing a new membership pathway diagnostic tool to achieve this.

Continual development of members

To move to a profession where we have a focus on continuous development we need to shift from a once and done approach to learning. We have started this by introducing annual reviews of our standards and producing curriculum to be more readily available and updated for users, starting with investigation. We aim with all of our production of standards guidance and continuous professional development (CPD) events to take into account the range of members we have, from central and local government, and policing units, working in civil, criminal and regulatory environments. To achieve this we are targeting our CPD events and products. We are working in collaboration with other sectors, industry and police, using their expert insight to inform the topics. This currently includes; disclosure, cyber and investigative best practice. These events are recorded so they are available at any time for members. This shows the commitment to recognising the different working patterns and hybrid approaches organisations operate within.

Increase diversity and inclusion (D&I)

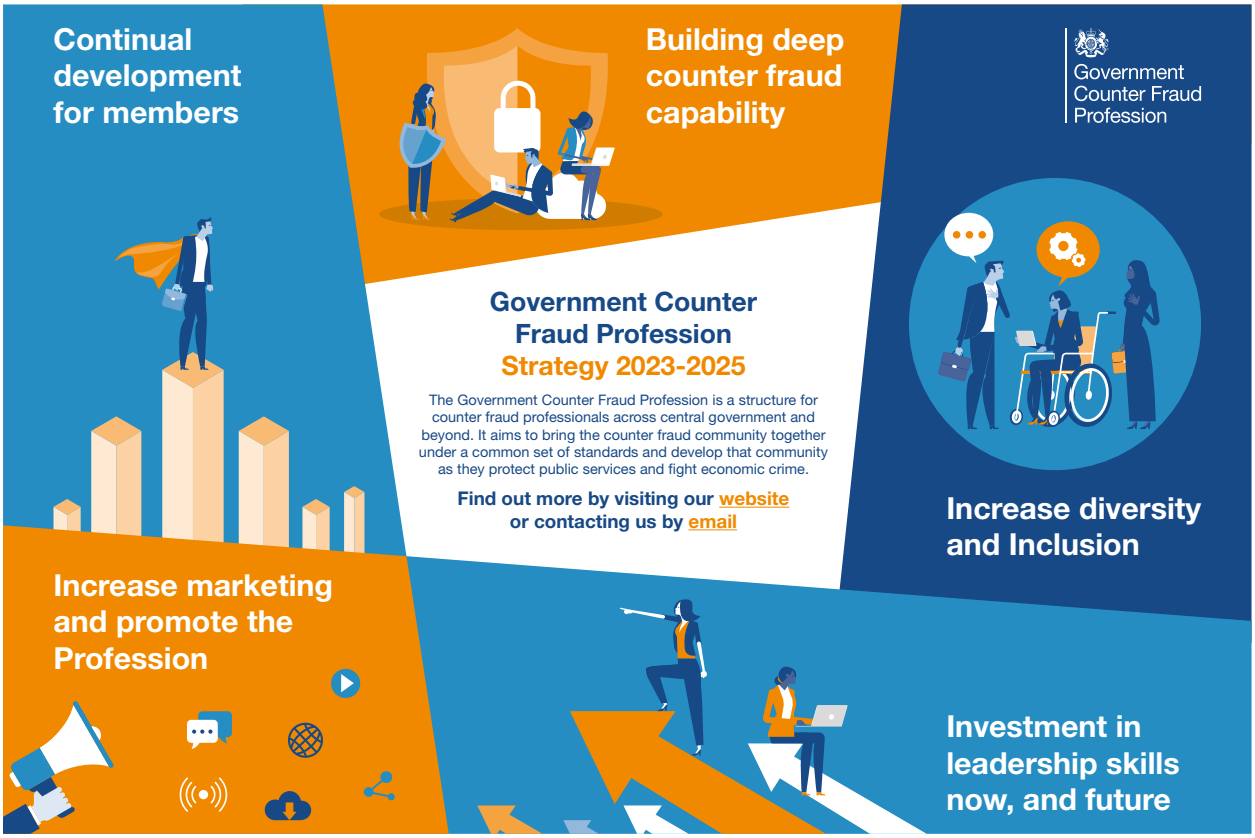
The most recent survey showed the profession is currently under-represented in multiple attributes, including gender, ethnicity and those with long term conditions/disabilities. We also identified a gap in our data, with little information on the representation of those in socio economic deprived groups. We want to build our diversity of representation for all groups and understand the barriers to entry, including any causal link to socio economic deprivation. The core aim is to build a future profession that is more accessible to all, that is representative of the people we ultimately serve in our role as guardians and protectors of vital public services. The work that has commenced on the development of more routes including to those in other professions such as the apprenticeship are a good starting point, but we want to do more and will develop a stand- alone strategy to give D&I the due focus it deserves, and share with members by Q3 2023.

Increase marketing and promoting the profession

The final area of focus is to increase the awareness of the profession and to utilise all opportunities available to raise the profile of it. All of us involved across organisations and working to counter fraud can help play a role in doing this. So for all events and publications you have coming up, consider how you can include information on the aims and objectives of the profession and encourage others to join or be part of the groups who are shaping and building the structures needed to help it grow.

That concludes the brief update of the work against the areas of the strategy, I will write again in the next issue of the Journal to update you on the reflection as we mark five years since the formal launch of the profession, and provide more clarity and information on the journey and ambition as we forge ahead to continue to modernise and build our future profession for those working in counter fraud.

If this inspired you and you want to get more involved in shaping the future of the profession contact me via **gcfp@cabinetoffice.gov.uk**



"An ounce of prevention is worth a pound of cure"

Author:
Jac Davies
Deputy Director, Risk, Threat and Prevention, Public Sector Fraud Authority

On the 23rd May 2023, Baroness Neville-Rolfe, Minister of State at the Cabinet Office was invited to formally launch the Risk, Threat and Prevention Services (RTP) of the Public Sector Fraud Authority (PSFA) whilst visiting the Cabinet Office's second headquarters in Glasgow, Scotland. The launch was the public announcement of meeting the commitment in the PSFA mandate[1] to support "... ministerial departments and public bodies in understanding the [fraud] risks and threats they face, and mitigating these risks through controls, prevention and deterrence activity…".

The quote forming the title of this article was included in her speech as it encapsulates the aims of RTP's delivery. It derives from advice given by Benjamin Franklin in 1736 to the population in Philadelphia, USA, who were threatened by fire. However, it is, of course applicable in many other domains: giving up unhealthy habits to avoid chronic disease; safety standards to help avoid accidents; and, of course, the prevention of fraud, which is always preferable to having to deal with its impact and after effects.

Previously, the Centre of Expertise for Counter Fraud in the Government Counter Fraud Function, PSFA's precursor, provided some support to departments prior to the creation of the PSFA. But the organisation's limited resources and scale meant that its reach and impact was understandably limited.

The creation of the PSFA brings a fresh opportunity to create services which are able to meet the needs of departments and government; designing for the future, but with the present in mind. Essential to achieving this has been the input of counter fraud and service design expertise. We have leveraged the input of various stakeholders from across the public sector combined with cross-sector support and internal PSFA capability to devise a target operating model (TOM) for RTP and then built its component parts.

The launch marked the end of the journey to design and build the first parts of RTP, and in this article we will detail what RTP can currently provide, and its future trajectory.

Tactical Support Services: Fraud Risk

The Professional Standards and Guidance for Fraud Risk Assessment (FRA) were developed and published by the Government Counter Fraud Profession in 2020 and some 225 people have completed the FRA training programme now provided by PSFA. But some departments do not have direct access to expertise in assessing their fraud risks, or measuring fraud losses.

PSFA's mandate commits to offering "[...] a service to targeted ministerial departments, public bodies or specific schemes to support them in conducting initial fraud impact assessments and/or fraud risk assessments [...]". RTP's service offer will be to support and augment existing counter fraud resources within departments, taking the lead where necessary, with an aim to provide a high-quality end product and better equip the department to face similar challenges in future.

RTP has recruited a number of specialists to work in this area, with everyone within the team successfully completing the FRA training programme. We are currently consolidating that learning through working closely with, and under the tutelage of, fraud risk experts within PSFA and partner organisations. PSFA's stated mission is to "[be] seen as a beacon of fraud and error expertise and a destination for those wanting to make a difference in fighting public sector fraud", hence the early prioritisation of building counter fraud expertise.

Team members are based in Glasgow, Newcastle, York and London and work in a matrix structure which is flexible to changing needs and priorities.

1 https://www.gov.uk/government/publications/public-sector-fraud-authority-mandate

Strategic View of Risk: Global Fraud Risk Assessment (GFRA) and High Fraud Risk Portfolio (HFRP)

Our mandate required that the PSFA "[...] create and maintain a Global Fraud Risk Assessment, (GFRA) that looks at fraud risk across government." During the COVID-19 pandemic the Government Counter Fraud Function tracked the new support schemes as they were launched and, using publicly available information, anticipated the likely ways that criminals would seek to defraud them, thus creating a 'Global Fraud Risk Assessment' (GFRA). This provided PSFA with a firm worked example, and an opportunity to consider how to take this foundation further.

Departments routinely complete FRAs and Initial Fraud Impact Assessments (IFIA) and submit these to the PSFA for assurance against the Professional Standards and Guidance. These FRAs and IFIAs are now also used to populate our new GFRA, and a 'Fraud Risk Universe' is used to match the identified fraud risks to a common typology. This, combined with other data held by the PSFA, allows us to identify trends and draw other insights from the GFRA which help build the view of fraud risk across government as never before. Naturally, we are in the very early days of populating this and therefore it cannot currently provide a complete view across government spend, but with each and every additional FRA and IFIA we receive, the understanding and depth improves, thus it will become increasingly useful as its coverage extends.

The areas of highest risk in the GFRA, will be considered for inclusion in the new HFRP. This will reflect, for example, where the scale of a scheme or spend area is very high, and/or where the counter fraud capacity capability appears to be out-of-step with the assessed level of risk. A governance board, comprising of the PSFA and HM Treasury, will review the proposed schemes and make the decision on what is ultimately included in the HFRP and reported to Ministers.

Tiger Teams

Occasionally there will be counter fraud problems that require skills that RTP does not have, or, because of an urgent deadline such as a crisis, RTP will need additional resources to meet that counter fraud commitment. During 2022, the rapid creation and roll-out of financial support schemes for citizens and businesses to help meet the rising cost of energy bills meant PSFA was asked to provide expertise to recommend measures to reduce opportunities for fraud. PSFA was already committed to creating a Tiger Team model for just such an eventuality, and so supporting these energy schemes proved an invaluable opportunity to develop this at pace based on lessons learned. If called upon, PSFA is now in the position to stand up another Tiger Team based on urgent government direction.

More still to come…

The launch in May 2023 marked the commencement of some of RTP's services, but design work continues to enable the full suite to come online:

- The measurement of fraud losses is a highly specialised area, and RTP expects to offer services to support departments in conducting fraud measurement exercises.
- A Fraud Risk Advisory Panel will help boost the expertise available to RTP to support departments, with specialists outside the PSFA called upon to help advise departments on how to better assess and manage fraud risks.
- As it matures, RTP will offer support to departments in developing and implementing preventative and detective fraud controls, strategies and aligned action plans.

And finally…

General Stanley McChrystal, a retired United States Army General, likened the ideal organisational response to risk as being akin to an immune system, which identifies, assesses and combats the threats it faces. Our new team, informed by our innovative strategic view of fraud risk across government, and with our investment in developing a new cadre of fraud risk experts, will help support departments to better respond to fraud, strengthening their risk immune system and creating a more robust resistance to fraud.

If you would like to learn more about the services we offer or discuss your Risk, Threat and Prevention requirements then please contact the team at: **psfa-rtp-services@cabinetoffice.gov.uk**

Helping consumers back from the brink of danger

Author:
Mark Tierney
Chief Executive, Stop Scams UK

Let me introduce you to Cathy. Aged 52 she lives in Carnforth, Lancashire, with her husband Peter and works in insurance. She has been with the same bank for most of her life, a relationship built on familiarity and trust.

One tea-time in March, Cathy picked up a call at home. A recorded voice asked her to confirm if she recognised two payments. At the end it said: "Press 1 to Confirm, 2 to be put through to the fraud department." Hmm. Cathy goes for 2. A reasonable choice to make, but it takes her somewhere she does not want to be.

Something makes Cathy suspicious. She never uses her phone for banking. In fact, when she does use her landline, it's only to call her daughter. Because Bea lives in New Zealand those conversations happen late at night. Something clicks. She remembers hearing advice on TV a week or so earlier about what to do if you get an unexpected call about your finances. They say your bank will never call you. Before anyone answers, Cathy puts down the phone. She follows the advice; stops, hangs up and dials 159.

159 connects her directly with her bank. To her relief, staff there confirm that they don't see any large payments on her statement from last week.

The call had been a scam.

Cathy was lucky. 159 helped prevent a scam and kept Cathy and her money safe. Hers is one of more than 350,000 calls that have been made to this important consumer phone service.

I should say now: I have made Cathy up. But a High Street bank that is a member of Stop Scams UK told us that this was exactly what happened to one of its customers who used 159 to report a scam and kept themselves safe.

The point is that Cathy could be any one of us – young or old, born digital or technologically hesitant. We are all vulnerable to being scammed.

Cathy's experience is a moment in a much bigger story. By some estimates fraud now costs the UK as much as an eye-watering £219 billion a year.[1] 41 per cent of all crime is estimated to be fraud and the City of London Police predicts things are only going to get worse.[2]

Fraud has grown so explosively that entire industries are dedicated to tackling it. In the public sector alone, thousands work to uncover wrong-doing and ensure criminals are brought to book.

Stop Scams UK is part of the same world of fraud fighters, but our lens is different. We focus on prevention: we seek solutions that can be put in place before a scam happens.

Stop Scams UK is a collaboration of responsible businesses coming together from across the UK's banking, technology and telecoms industries. At the time of writing, our membership comprises 21 businesses[3] collaborating across commercial, cultural and sector boundaries to find ways to stop scams for the common good. Products and services that give consumers like Cathy tools to help themselves are a core part of our work.

Why scams and not fraud?

You may well ask why we say scams, and not fraud?

Our work started some three years ago in response to an unchecked rise in Authorised Push Payment (APP) fraud. It embroils millions in unwanted emails, texts and phone calls.

1 CROWE Consulting, "Financial Cost of Fraud 2022" 14/06/2023

2 Office of National Statistics "Crime Survey for England and Wales year ending December 2022" 27/04/2023, and Fraud Act 2006 and Digital Fraud Committee "Fighting Fraud: Breaking the Chain" 12/11/2022

3 Stop Scams UK's members as at June 2023: AnyDesk, Barclays, BT, the Co-operative Bank, Gamma, Google, HSBC, Lloyds Banking Group, Meta, Metro Bank, Monzo, Nationwide Building Society, NatWest, Santander, Starling, TalkTalk, TeamViewer, Three, Tide, TSB and VISA.

Huge sums have been lost, sometimes at great speed, to criminals behind these schemes, who find it easy to move between platforms and services.

We define scams as a type of fraud in which the target authorises a payment and often unwittingly plays an active part in their own deception. Using scams in our name reflected the urgency of this sudden digital crime bonanza and its impact on ordinary people. A popular term, "scams" resonates. Our name raises a sense of hope that something is being done.

We believe the initiatives our members are progressing can be applied well beyond scams and APP fraud. In time, ideas incubated at the Stop Scams UK table will help close down opportunities for many other types of fraud too.

Our mission is to stop the scams at source. We facilitate collaboration between the industry sectors most affected by what has become a Scams Emergency. Stop Scams UK's members shape and lead work which addresses their needs. From small beginnings, our pilot projects and proofs of concept are conceived with scale and replication in mind. They are driven by an awareness that no one organisation or sector would be able to accomplish this alone.

Helping customers keep themselves safe

159, our first public-facing initiative, launched in late 2021.[4] It's a short number that's easy to remember; it offers a route back to safety for those times when a call comes in unexpectedly about a financial matter and you risk being scammed. Unlike long-form numbers, 159 cannot be spoofed or impersonated.

The service has so far had only limited PR and TV coverage and still achieved impressive call volumes. Banks that participate are highlighting 159 in their customer scam awareness campaigns. In July 2023 a YouTube and online ad campaign launched with a simple message, "If you think you might have fallen for a scam, stop, hang up and call your bank on 159."

Sixteen banks can be reached via 159, with others eager to join. 159 now covers more than 97 per cent of UK current accounts. We are developing the service to add more bank brands and offer an even better customer experience. As 159 grows we aim to collect more information about the calls that come in, so we can report fresh insight as fresh scams emerge, and on the patterns of scam attempts, which we will share with regulators and others like the National Cyber Security Centre.

Stopping scams at source: sharing data across sectors

While 159 helps the public keep themselves safe, perhaps our most exciting work is in cross-sector data sharing, which is the most powerful mechanism to stop scams at source.

Last year we asked the Royal United Services Institute to research with our members how cross-sector data sharing might work in practice. The report we published together in October 2022 recommended starting small, with immediate, real-world issues, rather than aiming at the outset for a single, system-wide solution. Speedy progress, building trust and demonstrating value are key to the success of this work.[5]

However, we know that large-scale, real-time intelligence sharing is essential to enabling businesses to identify scam risks. System-wide approaches can break scammers' business models. Our projects identify and overcome obstacles to this nirvana – whether they are commercial, technical, legal or regulatory, delivering powerful insights, which will help transform the data landscape.

Initiatives in progress include:

Reporting: When a scam is reported, the intelligence often doesn't reach all the relevant companies in a timely fashion, making it difficult to identify some forms of harmful activity. What firms do receive often comes too late, in part or in an unusable form. Much of this intelligence is gathered by the banks. We are helping them report timely, reliable and actionable scam data to tech and telecom companies.

Scam intelligence pilot: We are engaging directly with scammers by email and phone, to understand what they do, and what platforms and tactics they use. We share the resulting intelligence with those businesses who provide the services the scammers abuse. This work will help identify and close bad actors' accounts, and even refund fraudulent payments.

Voice matching: Recordings of phone calls made by scammers to banks and telecoms firms, either to gather intelligence or attempt an account takeover, are analysed and matched using audio technology. The project aims to map, disrupt, and ultimately break criminal business models which perpetrate phishing by phone.

Stop Scams UK is showing that collaboration led by industry across key sectors can lead the way in defeating scams and fraud. Our pilots are starting to demonstrate that scammers' business models can be broken, and that the incidence of scams can be cut.

With the cost of fraud to the UK economy estimated to be as much as £55,000 each hour[6], it's hard to imagine how devastating the consequences might have been for Cathy if the call she answered on her rarely used landline had moved on to its conclusion. If in doubt, call your bank on **159.**

4 https://stopscamsuk.org.uk/159

5 https://rusi.org/explore-our-research/publications/conference-reports/enabling-cross-sector-data-sharing-better-prevent-and-detect-scams

6 https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/annual-fraud-report-2023

‘How the cost of living crisis can leave organisations vulnerable to internal fraud’

Author:
Tracey Carpenter
Insider Threat Manager, CIFAS

If you asked someone how they were before the pandemic, you would have expected a favourable response. But in a post-pandemic society we've learned that it's okay not to be okay. This includes in the workplace, where businesses are more concerned with employee wellbeing than ever before. Over the last six months or so, I've been particularly focused on ensuring that Cifas members see wellbeing as a preventative approach to safeguard their organisation against the insider threat, rather than merely a "nice to have."

We all have a point where if we are pushed enough, we would be dishonest. You may have started reading this article believing that you would never commit fraud against your organisation, but what if your family was hungry and you couldn't put food on the table? Or you were struggling to keep a roof over your head or your house warm because you couldn't afford to pay your rent, mortgage, or utility bills? Is that the point at which you would decide that dishonesty is your only option?

Employers are suffering the effects of the economy as well as individuals, and so I am not going to suggest that employers should automatically support employees financially – which many have already done and can no longer afford to. However, there are many other ways that employers can support employees when they are struggling such as allowing someone to change their working hours to allow off-peak travel, condensing their working hours into four days instead of five to reduce the cost of childcare, or initiating a carshare scheme for employees travelling to their workplace. Employees can also support their co-workers by donating unwanted items such as food, toiletries, outgrown school uniforms, old winter coats, and so on to office pantries.

The Trussell Trust hit the nail on the head with their TV commercial at the end of 2022, in which families were seen having to sacrifice a product such as food in order to keep hold of female hygiene goods, or having to choose between using a kettle or a toaster.

But what if employees don't have the option of sacrificing one product for another and are just unable to afford the necessities? You may believe that your employees would never be in such a situation because you offer them a living wage. What you may not know is the unique circumstances of employees, such as whether they are a single parent or live in a single occupancy household, whether they have a spouse who has lost their job, or whether they are financially supporting a friend or family member. By directing employees to their local food bank and other resources might mean the difference between someone eating a meal tonight or not. As children we were taught that eating breakfast before school would help us to concentrate, and this applies to adults too. So if an employee is going without a meal to allow their children or a partner who may have a more physically demanding job to eat, then it is likely they could make errors in work which could result in a data breach.

An individual from an organised crime group may approach an employee via social media and offer them £500 to expose some confidential data. Usually this isn’t something an employee would contemplate as they know it is dishonest, but what if that employee's car broke down on the way to work and they didn't have the money to have it fixed? Then they got a call from their partner saying the washing machine had leaked all over the kitchen floor? Would the employee react differently if they saw the identical request now, and would they consider that £500 to be a method to cover those unforeseen bills?

We all have our 'go to' thing when it feels like it’s been a long day at work or life is just getting on top of us. For most of us, this is something affordable and under our control such as a takeaway, chocolate, or a glass of wine. However, some people have acquired an addiction that makes them feel good such as alcohol, drugs, gambling or shopping.

Addictions are thought to have increased as a result of the pandemic, and logical reasoning is likely to go out the window when it comes to addictions. I know from talking to people who have had gambling addictions that they didn't care where the money came from; all they knew was that they needed to place the next bet. Organisations should ensure that their employees understand how they can seek help. For example, does your company offer an Employee Assistance Programme, and if so, do employees know how to use it? Are employees reminded of any available support on a frequent basis? Are there Mental Health First Aiders available to guide employees through the initial steps of obtaining treatment and support? Is the employer's culture one in which employees can discuss personal difficulties such as addictions and financial wellbeing with a manager or HR Team? Some employers may believe that as long as an employee's personal life does not interfere with their work, it is not their responsibility. But they do have a responsibility to care for their employees' well-being, and by failing to do so, they risk becoming a victim of insider threat. Even something as simple as directing employees to resources and granting time away from work to attend counselling or support sessions might be the difference between an employee overcoming an addiction and committing a fraudulent act to fund it.

Sometimes it feels good just to be able to chat to someone. A problem shared is a problem halved, as the old saying goes. Allowing employees to sit down and talk to someone who is removed from a certain scenario can be beneficial. When I check my bank statement, I may believe that my outgoings are all essential and that the amounts I pay for utilities are all reasonable. Someone else may look at that same statement and see that I can save money on my outgoings meaning I can afford the basics and am not tempted to act dishonestly - so financial health checks can be a great way for employees to learn more about where they can save money.

If you offer emergency loans to employees to pay for unforeseen expenditures, are they aware of the service and how to request this?

Employees are more likely to be dishonest if they have an opportunity to commit fraud, the motive to do so, or the ability to justify their behaviour. I'm not implying that every employee who is struggling because of the cost-of-living crisis will commit fraud, but if organisations don't have the proper controls and processes in place to prevent them from being targeted, as well as ensure they are aware of the support available before it gets to that point, they are more likely to be a target. Employees may feel driven to be dishonest if, for example, there are no bonuses for the majority of employees but the press constantly mentions how their CEO received a significant bonus or a high number of shares in addition to their large annual salary. This, along with increased workloads and reduced staffing, can make an employee disgruntled. Faced with an opportunity to steal money or commit fraud against their employer, they may see it as a justifiable act of revenge.

Of course, the incentives I discussed at the beginning of the article about people being dishonest in order to pay the necessities can mean that employees can both motivate and rationalise dishonest activity. We can all easily justify our behaviour. For example, you may start the week intending to eat healthy and lose a few pounds, but by Wednesday, it has been a really long week, meeting after meeting, it is raining and miserable outside, but you did get a large piece of work finished today as well, so you're going to have a bar of chocolate or a chip shop supper just because of the type of week it has been. That is how easily we can justify our actions.

Employees are critical to keeping businesses safe against the external threats they face, and employers must play a role in keeping their workers safe and supported before they feel compelled to being the ones committing fraud.

Image: Geralt on Pixabay

Fraud in DWP: Prevention is better than cure…

Author:
Shawn Turner
Government Counter Fraud Profession Lead, Department for Work and Pensions

Being in the Civil Service for some 20 years now I have seen a full range of ways we tackle criminality, from my time at the Inland Revenue (HMRC for our newer colleagues) processing tax returns and some frankly ridiculous claims for expenses, through to spending 10 years as a front-line Border Force Officer seizing class-A drugs, cigarettes, and the occasionally unpleasant bags of rotting meat (yes that happens!). But working for Counter Fraud Compliance and Debt (CFCD) in the Department for Work and Pensions (DWP) really opened my eyes up to the complex nature of fraud, the myriad of different benefit types that we deal with as an organisation and the teams of people set up to respond to fraud.

During my short 4 years in DWP now however I have seen a shift in the way we try and tackle these attacks on what is theft of taxpayer money. The focus continues to shift to stopping fraud at source, whether that's enhancements to the way people claim benefits through Universal Credit (UC) or how we deploy our fraud professionals to stop suspicious payments from ever walking out of the door. I also continue to be proud of the colleagues I work with as on top of protecting the public purse, they also deal with the most vulnerable in society and do so with the upmost empathy and professionalism. I think that balance drives real passion in our people throughout CFCD.

DWP has played a huge role in our cross-department vision of professionalising our fraud colleagues through the Government Counter Fraud Profession (GCFP) and changed its approach to tackling fraud and error by creating standards to gain that consistency and professionalism across the Counter-Fraud community.

The creation of a standard

Author:
Mark Bushell,
Government Counter Fraud Profession Team, Department for Work and Pensions

Developing the Fraud Prevention standard for the Government Counter Fraud Profession (GCFP); easy……. right?

In mid-2021, the DWP loaned a small team to the GCFP team within the Cabinet Office. Its mandate was to develop the Fraud Prevention Standard to provide guidance and a set of standards to people working in fraud prevention across Government.

With a combined experience of almost 40 years in counter fraud investigations within DWP, Mandy Kipling and I needed to change the way we thought. We needed to really understand how fraudulent activity was affecting the wider public sector and what could be done to prevent it. This was definitely outside of our comfort zone.

The first struggle was to adapt to the challenges of moving departments. Understanding the culture and new Information Technology (IT) Systems within the Cabinet Office which we moved to, took some getting used to, although we have since returned to the DWP, it is just as challenging to move back.

The months of research and stakeholder engagement introduced us to many different counter fraud teams. Each team is very different from the previous one, all facing very different fraud problems and all with different resources. Coming from a department with extensive resources to counter fraud, it was easy to forget that many other departments and their arm's length bodies were not in the same fortunate position. This brought a new consideration to the project. The standard must be cross-cutting and prevention methods need to be transferable. Working parties became a vital part of building the standard, ensuring input, concerns and solutions were gathered from across the public sector.

A slight distraction

In the spring of 2022, life in the Cabinet Office changed. All of a sudden, colleagues were being taken offline to develop something new. Our already small team started to reduce further. The Public Sector Fraud Authority (PSFA)

had been announced and all available resources were being utilised to develop and launch this new authority. Mandy and I were now working in relative isolation while the world around us changed. The GCFP would still fit as a key area within the new PSFA, so we ploughed on.

Armed with copious documents and notes of prevention processes across both public and private sectors, we then needed to decide the key areas for inclusion. We currently had enough information to write three standards. I soon found out that writing a standard requires a dedicated mindset. We are not telling people how to do fraud prevention, only what should be done to prevent fraud. This particular skill took me some time to put into practice. Many of my early sections were quickly returned covered with notes reminding me we are not producing a training guide (yet).

Let's go international

As a key partner in the International Public Sector Fraud Forum, the Australian Government's Commonwealth Fraud Prevention Centre (CFPC) is seen as an expert in the field of fraud prevention. It seemed a logical step to collaborate with them in the standard production. It quickly became evident that the appetite to join this project was immense and the wealth of information that could be shared around the world became invaluable. Both countries agreed, this GCFP Prevention Standard needed to be the world's first international standard in fraud prevention and a new stakeholder was engaged.

Finalising the standard

With a framework in place, and a rough draft of the Prevention Standard drawn up, it needed to be refined for submission to the GCFP Board. As a member of the Cross Sector Advisory Group and the (now) PSFA's expert talent pool, we engaged the services of Dr Mike Gilbert. Using all his skills and experience, and, as part of Chartered Institute of Public Finance and Accountancy (CIPFA) where he delivers the prevention course, Mike reviewed the draft and provided expertise in developing the competency framework finding the right balance to stretch practitioners in the skills matrix, but still being obtainable was key.

Mike's praise and encouragement on the content of the draft standard was a re-affirming moment for Mandy and me. We had actually created something that could work and benefit the public sector. With a full skills matrix in place, we needed to present to Mark Cheeseman, the Chief Executive Officer (CEO) of the PSFA, and then the GCFP Board.

Sign off

After a nervous meeting with Mark Cheeseman, CEO of the PSFA, Mandy and I left Whitehall with a pleasingly low number of suggested alterations. All proposed to stretch the practitioner and enhance the capability within the Standard.

The final presentation to the GCFP Board was completed in March 2023 where the newly developed "Fraud Prevention Professional Standard" was signed off and agreed for publication.

My journey

I was on loan to the Cabinet Office and later the PSFA between November 2021 – March 2023. During this time, I was privileged enough to work with some amazing professionals in Counter Fraud. There are far too many to name individually, but the Standard would not be where it is without guidance and input from Mandy Kipling, Mike Betts, Laura Eshelby, David Whitehouse-Hayes and Mark Cheeseman from the PSFA. The working parties, especially NHSCFA, NHS Scotland, GIAA, CIPFA, Mike Gilbert and Chris McDermott from CFPC.

I'm not saying my time there was easy, but if something is not challenging, what's the point in doing it?

Mandy and Mark have since returned to the DWP where they continue their work promoting the GCFP as part of DWP's GCFP development team. During their time at the PSFA, the research conducted during the Prevention Standards project, also aided in the development of an internal fraud prevention interactive guide, available from the PSFA.

Government
Counter Fraud
Profession

Contact us:

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