Government Counter Fraud Profession

The Public Sector Counter Fraud Journal

ISSUE 12, February 2024

ISSN 2755-1024

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
In Memoriam

Parveen Akhtar
Deputy Head, Public Sector Fraud Authority

Mick Hayes
National Operations Manager, NHS Counter Fraud Authority

Cover Image: Parveen Akhtar

CONTENTS

Editor's letter

Welcome to the February 2024 edition of the Counter Fraud Journal. Before diving into the variety of articles, I'd like to acknowledge the tribute to David Kirk, a valued member of our Editorial Board. His wisdom and wit will be greatly missed.

This edition features insightful articles covering various fraud related topics. From HM Treasury, Conrad Smewing, discussing strategic collaboration with the PSFA to Tim Townsend providing an international perspective on the New Zealand Counter Fraud Centre, emphasising proactive prevention.

Jordan White shares his experience with the Counter Fraud Investigator Apprenticeship programme, highlighting its benefits.

Additionally, articles by Joe Whitfield and Jack Whitaker explore the intersection of fraud and technology, showcasing both its potential for prevention and its exploitation by fraudsters.

In his article Joe describes the history of the National Fraud Initiative from its humble beginnings in 1996 through to the highly sophisticated use of artificial intelligence and predictive analytics to identify potential occurrences of fraud or error within very large data sets. This work has led to significant savings for the public purse.

The second from Jack Whitaker from the University of Surrey shows us that while technology can be harnessed to reduce fraud, each new technological advance will also offer fraudsters new opportunities. I certainly hadn't appreciated that the invention of the printing press by Johannes Gutenberg in 1440 gave 15th century fraudsters the opportunity to flood the market with counterfeit bibles. Jack's article shows that while in one sense there would seem to be little new in the world of fraud, recent advances in technology have enabled a whole range of new opportunities for fraudsters which may require a more robust response by the technology providers.

The National Audit Office (NAO) discusses the importance of embedding consistent financial reporting to save millions, underscoring the importance of transparency and accountability in combating fraud.

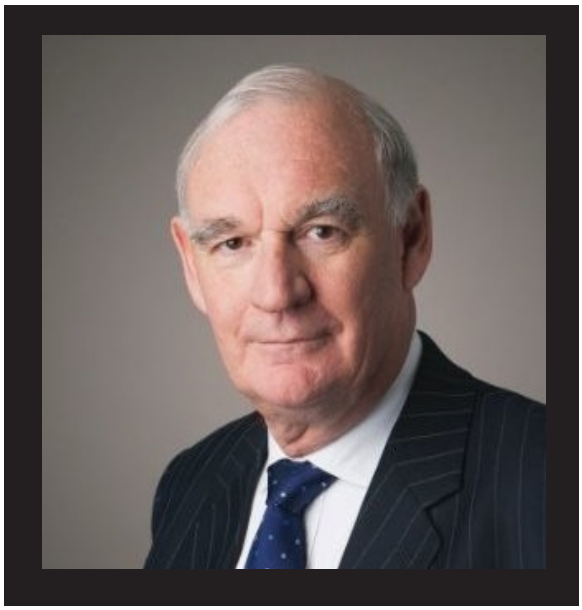
Finally, many of you will be familiar with the Fraud Investigation Model (FIM) which redefined the approach to the investigation of fraud. The FIM emphasises the importance of prevention and early disruption to help reduce the harm caused by fraud. In this article Chris Freeman and Mike Betts of the PFSA introduces the Public Sector Fraud Model, which builds on the earlier work on the FIM and suggests that fraud reduction within the public sector requires a 'holistic whole system approach' where speed of organisational response is key to reducing the harm and loss period. In this model the criminal investigation is only one aspect of a more rounded counter fraud response. I am sure this will promote a lively debate.

I hope you have found the range of articles interesting. We are always seeking contributions for future articles so, if you think you have got something that would be of interest to our readership, or if there is anything you would like to read about in the journal please contact us at GCFP@CabinetOffice.gov.uk

Mick Hayes
National Operations Manager
NHS Counter Fraud Authority

Foreword

In Memoriam: Celebrating the life and legacy of David Kirk



It is with a profound sense of honour and privilege that we commemorate the life and professional journey of David Kirk - a distinguished figure whose impact resonates deeply in the realms of law and counter fraud. As we celebrate the life of a man who consistently embodied respect, professionalism, and inclusivity, we reflect on how he enriched ours with his wisdom and camaraderie.

Personal reflections - Laura Eshelby, Deputy Director, Public Sector Fraud Authority

Over the past ten years, I had the distinct privilege of working with David in various capacities. This started some years ago now, with David providing strategic insights, challenges and experience as we started to plan the Counter Fraud Profession. David was able to bring his real world experience of working in a variety of legal and economic crime roles to bear, as we engaged across government to find common cause. This effort resulted in the development of the first framework of disciplines, laying the foundation of subsequent standards in Investigation, Intelligence, as well as Sanctions, Redress and Punishment that he actively supported. His role as a cross - sector advisor and a member of the Public Sector Counter Fraud Journal Editorial Board allowed me to witness first hand his generosity and his role as a true sounding board. In the developmental phase of our profession, his insights were invaluable, guiding us through the launch of our initiative.

In recent weeks, conversations with David's friends, colleagues, and family have painted a vivid picture of a warm, loyal, and generous individual. Beyond professional motivation, he inspired those around him. The unanimous warmth and respect expressed by those who knew him underscore the magnitude of the void left by his passing. His sharp wit, calm demeanour in crises, as well as his passion for socialising, reading, cooking and music will be dearly missed. David leaves behind his wife Penny and their three sons - Edward, Charlie, and Henry.

Career Highlights and Achievements

- 2019- 2023 Door Tenant, Outer chambers
- 2018-2023 Consultant Barrister, RS Legal Strategy Ltd
- 2014-2018 Partner, Maguire Woods
- 2013 -2014 Chief Criminal Counsel, Financial Conduct Authority
- 2009-2013 Chief Criminal Counsel, Financial Services Authority
- 2006-2009 Director of Fraud, Crown Prosecution Service
- 1994-2006 Managing partner, Simons, Muirhead & Burton
- 1988- 1994 Partner, Head of Fraud and Regulation unit, Stephenson Harwood LLP
- 1985-1988 Senior Legal Advisor, Attorney General's Office
- 1976-1985 Senior Legal Advisor, Director Public Prosecutions

From 1968 -1971, David had studied English Literature and Language at Oxford University. It was only later that his lifelong interest in Law was kindled. David's illustrious career serves as a testament to his versatility and expertise. Spanning both public and private sectors, his journey as a barrister and solicitor focused on economic crime since the early 1980s. His pivotal roles included prosecuting fraud cases for the Director of Public Prosecutions, advising on criminal matters, and contributing to the establishment of key legal entities.

In 1988, recognising the need for expertise in the criminal fraud landscape, David was appointed to lead the fraud and regulation unit at Stephenson Harwood. His tenure included high-profile cases such as Guinness, Blue Arrow, and British Rail investigations. Notably, he was part of the team investigating the Kuwait Investment Office's investments in Spain (the Grupo Torres case).

Transitioning to Simons Muirhead & Burton in 1994, David continued advising and representing clients in corporate fraud cases. His career took a new trajectory in 2006 when he assumed the role of Director of the newly formed Fraud Prosecution Service at the Crown Prosecution Service. Subsequent leadership roles at the Financial Services Authority (FSA) and US law firm McGuireWoods further underscored his influence.

A hallmark of David's legacy is his co-authorship, with Tony Woodcock, of the 'Serious Fraud: Investigation and Trial' books. A seminal work in the field, the latest edition, published this year, stands as a fitting tribute to his enduring contributions.

Insights from Friends and Colleagues

Stephen Parkinson - Crown Prosecution Service Colleague

In his reflections on the life of David Kirk, Stephen was privileged to have known David for almost four decades through various roles and phases of his distinguished career. Much like characters in "A Dance to the Music of Time," their paths intersected as David seamlessly navigated between public and private sectors. Beginning his journey in the Department of the Director of Public Prosecutions, David was remembered by

colleagues as a delightful, engaging, and technically adept lawyer, embodying fairness with a touch of humanity. His journey continued through the Attorney General's Office (AGO) and private practice, culminating in his pivotal role leading the revitalised Fraud Prosecution Service in 2006.

David's warmth and effective leadership, evident in his subsequent roles at the Fraud Conduct Authority (FCA) and McGuireWoods. Even in retirement, David remained connected, his genuine interest in others and his selfless nature standing out. If I were to distil one enduring memory of David, it would be that every encounter left you feeling uplifted - a testament to his thoughtfulness, gentleness, and genuine likeability.

In the words of a colleague, he was the loveliest of men, leaving a legacy of positivity and kindness.

Adrian Berrill-Cox - Financial Conduct Authority Colleague and Friend

Adrian's recollections offer a glimpse into the personal and professional dimensions of David's life. From their initial connection at the FSA to their continued collaboration at the FCA, David's "can do attitude" and willingness to take risks in prosecuting challenging cases left a permanent mark. Adrian highlights David's foresight in navigating transformations, emphasising his calm and unflappable nature. The decade-long friendship between David and Adrian, marked by social events and shared passions, stands as a testament to David's warmth, loyalty, and generosity as a friend and professional.

Tony Woodcock - Colleague at Stephenson Harwood

Tony's tribute, delivered at a memorial in October 2023, paints a vivid picture of David's courageous move to establish the criminal fraud and regulation practice at Stephenson Harwood. Despite the challenges of transitioning from public service, David excelled, securing major instructions in landmark cases. His empathy, commitment, and reputation as a leader in the field are evident in the praise from colleagues and solicitors. Tony's acknowledgment of David's role in laying the foundation for subsequent success at Stephenson Harwood speaks to the enduring impact of his leadership.

Closing Remarks - Mark Cheeseman, CEO, Public Sector Fraud Authority

Though David is no longer with us, he leaves us with a legacy built from a life, much of which was spent so profoundly dedicated to the timeless principles that underpin our work. David's unwavering commitment, courage to challenge the status quo, naturally collaborative approach, and ability to provide objective counsel and direction not only defined his professional journey but also left an indelible mark on those who worked with him.

David had a brilliant ability to seamlessly navigate diverse sectors, contributing significantly to the establishment of key legal entities. This stands as a testament to his brilliance. He was not just a legal luminary, he was a trailblazer who shaped the landscape of counter fraud and legal practice. His legacy extends beyond any accolades and titles, encapsulating a spirit that encouraged and inspired and paved the way for others.

As I pen these closing remarks, I am reminded of the continuing relevance of 'Serious Fraud: Investigation and Trial' - a collaborative effort that echoes David's intellectual prowess and his passion for literature. The continued impact of this work serves as a tribute to his influence, ensuring that his insights endure in the pages of legal scholarship.

But his impact goes well beyond what is written down. His can- do approach and ability to encourage those he worked with on their own journeys, while prodding them in a sensible direction has left its mark on the work that I have had the privilege of being involved in for the past ten years - the creation of structures in the public sector to confront and take action on the often hidden damage that fraudulent activity brings.

In celebrating David Kirk, we celebrate a life that embodied dedication, wisdom, and an unwavering pursuit of justice. I hope, and expect, that his contributions will echo through our Profession, encouraging future generations of future fraud fighters to embrace the path less taken. His legacy is a beacon, a reminder that the right path is not always the easy one, but it is the one that leaves an enduring mark - making the part of the world that we touch a richer place - just as he did.

A collaborative approach to responsible public spending: The role of the Public Sector Fraud Authority.

Author:
Conrad Smewing, Director General of Public Spending, HM Treasury

The creation of the Public Sector Counter Fraud Authority (PSFA) is a great example of government taking an open, cross - cutting and performance - linked approach to tacking a vitally important issue: the battle against fraud in the public sector.

Strategic Imperative: Modernising Response to Fraud and Error:

The PSFA was set up by the Chancellor in the Spring Statement 2022 to implement lessons learned on fraud and error during the COVID - 19 pandemic. Led by Mark Cheeseman, CEO of the PSFA, it has marked a significant shift in the government's approach. It places a much greater emphasis on performance and outcomes, and employs cutting-edge practices, tools and technology to comprehensively modernise the response to fraud and error. It is creating a more extensive and specialised set of services to assist government departments and public bodies in tacking fraud. Lastly, the PSFA, acting as the central co - ordinator of the government's counter fraud function, reinforces public trust by ensuring a more robust protection that taxpayers' money is used as intended.

This article outlines the broad range of steps it has taken to achieve this. But the numbers also speak for themselves the PSFA was launched on 3 August 2022 with £25 million of funding over 3 years. This additional funding is paying dividends: the PSFA has far surpassed its target of achieving £180 million of savings for the taxpayer in its first 12 months by preventing and recovering £311 million. In its plan for 2023/24 the PSFA commits to recognising £185m in audited benefits from its services.

Counter Fraud Leadership Programme: Catalyst for Change:

A pivotal element of its strategic approach is the Counter Fraud Leadership Programme. This innovative initiative is designed to equip functional leaders, particularly those overseeing portfolios which encompass fraud, with the necessary skills to set the 'tone from the top'. The objective is to create a leadership culture that actively tackles fraud within the public sector. This programme helps ensure leaders possess the knowledge and expertise to drive comprehensive counter fraud measures across their respective domains.

Foundations: Initial Fraud Impact Assessments and Fraud Risk Assessments:

The implementation of initial fraud impact assessments (IFIA) and fraud risk assessments (FRA) into the design of schemes and projects serves as a crucial foundation. These assessments not only guide leaders in identifying and addressing areas susceptible to fraudulent activities but also embed a culture of responsibility in the senior leadership across the public sector. The shift brought by IFIAs is

significant; now departments must assess how fraud will impact a new scheme, starting with the assumption that fraud will occur, rather than leaving room for questioning its likelihood. It also compels departments to expand their perspective beyond obvious financial losses, prompting a consideration of the total impact.

It is important to acknowledge that the government's capability in assessing fraud risk varies. The Government Counter Fraud Profession has taken steps to address this disparity. Professional standards, available on GOV.UK[1], supported by practice notes, have been published. The professional standards for fraud assessments encompass a comprehensive learning programme covering both IFIAs and FRAs. Additionally, the PSFA has established a Risk, Threat and Prevention (RTP) service, launched in May 2022, which collaborates with departments to assess their fraud risks. This service helps draft FRAs and provides support in revising and updating existing assessments. Furthermore, it offers specialised advice through the Complex Grants Advisory Panel, operated by the Government Grants Management Function[2], aiming to ensure that fraud risks are properly considered in the design of new grants.

Accountability is crucial. The Performance, Assurance and Evidence (PAE) team works across the central government to agree financial targets. It also gives assurance, through operating the Counter Fraud Prevention Panel with cross government experts, that counter fraud outcomes are reported accurately.

Conclusion: A Collaborative Approach to Financial Integrity:

By identifying fraud, preventing its occurrence, and actively recovering misappropriated funds, the PSFA not only safeguards public resources but also strengthens the public's trust in the responsible use of their money. The creation of the PSFA is a sign of the government's commitment to tackle fraud: since 2022 the government has invested over £1 billion in counter fraud systems, fortifying defences against fraud and error and driving greater efficiency and productivity in government operations. It is a key part of achieving a more secure, accountable, and efficient public sector.

1 https://www.gov.uk/government/groups/counter-fraud-standards-and-profession
2 https://www.gov.uk/government/collections/grants-management-function

Image: Andrew Hester

Tackling public sector fraud in New Zealand- challenges and opportunities

Operating in a small country like New Zealand can present challenges - but also opportunities. This rings true for the country's relatively new Counter Fraud Centre (CFC). Born from the COVID-19 pandemic, the CFC's value was brought to the forefront just a few years on, when the country was hit by severe weather events that caused millions of dollars in damages.

Author:
Tim Townsend
Manager, Counter Fraud Centre
Serious Fraud Office, New Zealand

How it started

It is well documented that times of economic stress and disaster can increase the risk of fraud. Both the Counter Fraud Centre (CFC) and its parent agency, the Serious Fraud Office (SFO), have their roots tied to such events.

The SFO was created as a response to the fallout from the 1987 share market collapse and the ensuing economic recession, which exposed fraud on a scale never seen before in New Zealand. Since its inception in 1990, the SFO has been recognised for its specialist expertise in tackling the most significant fraud and corruption cases for the benefit of New Zealanders.

Historically, the SFO's focus has been on investigating and prosecuting serious and complex fraud. Over time, there has been a parallel increasing demand for prevention guidance as agencies look to protect themselves from fraud and corruption. While investigation and prosecution will always be critical, effective prevention measures are key to reducing harm from fraud and corruption.

As we have heard repeatedly from our colleagues around the world: "You can't prosecute your way out of fraud".

In 2020 the SFO was funded to lead public sector fraud prevention efforts relating to COVID-19 relief packages. Over the next two years the prevention team proved its worth through a number of initiatives and following that, the CFC was funded on a permanent basis in Budget 2022. The CFC works with public sector organisations to build their resilience to fraud and corruption.

Key objectives include:

- Engaging with our international partners;
- Building understanding of fraud and corruption;
- Developing and sharing of fraud prevention information;
- Establishing and supporting an anti-corruption culture; and
- Providing a central point of contact for advice and intelligence gathering.

We are achieving these through:

- Developing educational awareness, guidance and tools

Historically there has been a lack of counter fraud guidance, resources and products for public sector organisations in New Zealand. The CFC regularly engages with Australia's Commonwealth Fraud Prevention Centre (CFPC), UK Public Sector Fraud Authority (PSFA)

and International Public Sector Fraud Forum (IPSFF) to share experiences and leverage counter fraud and corruption material. This has been of huge assistance in developing materials for the CFC, which are publicly available on the SFO website.

Resources produced include guides and fact sheets covering a wide range of topics to help build good counter fraud practices, such as Fraud Risk Assessments, Control Testing and Identifying Insider Threats.

Case studies have been developed which use SFO prosecutions to tell the story of organisations that have been defrauded and give information on countermeasures that could have helped prevent the fraud. They identify fraudster personas, the impact on people and organisations involved and red flags that could have helped detect the fraudulent activity.

- ## Counter Fraud Community of Practice (CoP)

Another challenge has been the shortage of collaboration and information sharing across the public sector. To address this, the CFC established a Community of Practice (CoP).

The CoP brings together a highly engaged group of fraud experts and practitioners from central government agencies and has a wide membership base, with a total of 99 current members representing 37 agencies. Membership continues to increase with further agencies joining the CoP throughout 2023. The community is governed by a Charter and membership is administered by the CFC.

The CoP aims to build the capability of the public sector's response to fraud and corruption by:

- providing a forum for members to share information and intelligence in relation to loss of public funds;
- facilitating opportunities for collaboration between members, by which knowledge transfer can take place;
- promoting counter fraud awareness; and
- identifying gaps/risks present in New Zealand's public sector counter fraud response and discussing appropriate mitigation strategies.

The CoP has become an integral part of the CFC's work. The forum successfully promotes cross-government engagement, sharing of technical knowledge and provides opportunities for collaboration. This has led to further subgroups being formed by members to address specific challenges that they are facing, most notably around disclosures of interest, identity theft and the development of digital identities.
CoP resources have also been shared by the international team of the Office of the Auditor General, with audit offices in the Pacific Islands that they support.

Topics and discussion at the monthly meetings in 2023 included:

- Agencies demonstrating training and e-learning modules they have developed to build internal capability;
- Insider Risk and a presentation around the Insider Threat Capability Framework; and
- Examples of how data analytics can be used to uncover fraudsters and their activities, highlighted by the demonstration of detection programmes within the agency.

- ## Fraud Perceptions Survey

Fraud prevention is a relatively new field in New Zealand and as a result there can be a challenge in gaining insight into what counter fraud and corruption capabilities exist.

A fraud perceptions survey was created following a similar tool that had been developed by the CFPC. The survey seeks to understand public sector employees' perceptions of their agency's fraud risk exposure and fraud management actions. Employees rated their knowledge, exposure, and capability regarding the seven fraudster personas and 24 countermeasures. Employees' perception of an organisation's fraud control activity informs their perception of organisational culture or 'the way things are done around here'.

The assessment provides participating agencies with the two fraudster personas they are perceived to be most exposed to, the perceived strength of countermeasures that mitigate these fraudster personas, and opportunities for improvement of countermeasures and fraud awareness. It also offers a comparison with other public sector agencies.

- ## Local Government Engagement

Given the size of New Zealand, it is rare for one local government body to possess all the necessary fraud prevention skills. Across local governments there are varying levels of capability between and within the different regions. These small organisations also often face challenges around declarations of conflicts of interest owing to the community-based nature of these regions.

The CFC had previously focused on central government agencies and building capability within them. However, there was also a recognised need for building similar levels of capability across local government. In early 2022, the CFC ran three webinars which particularly highlighted the need for further fraud prevention initiatives within this space. Further engagement with councils resulted in the establishment of a local government CoP which will be facilitated by the CFC in a similar way to the successful central government CoP. Skills can now be leveraged and shared across local government bodies.

Responding to natural disaster

New Zealand is vulnerable to severe weather events. In February 2023 the country was struck by a number of these including Cyclone Gabrielle as well as flooding which impacted Auckland, the largest city. The New Zealand Government introduced a number of funding schemes to help assist people who had been impacted.

Previous experience has shown that in emergency funding situations, the need to deliver funding urgently can mean reliance on high trust, quick distribution mechanisms, which are more vulnerable to exploitation. With this in mind, within days of Cyclone Gabrielle the CFC reached out directly to organisations involved in the relief efforts to offer guidance and support.

Because of the relatively small nature of New Zealand and the organisations involved, we were assisted in having already spent a number of years building relationships with the appropriate people. We were able to move quickly to offer guidance and support to public sector agencies administering relief funding.

Since the event we have been able to incorporate learnings back into our work, including having an impacted agency present to the CoP on assurance work that was done around recovery grants. Engagement with local councils around this event also assisted us in our local government engagement work, covered earlier.

What's next?

The CFC continues to provide education, awareness and resources by publishing resources on an ongoing basis, as well as delivering presentations to various organisations and groups. Upcoming work includes:

- Developing a reporting framework for the impact of our prevention work, which is a continuing priority and a challenge for the CFC.
- Providing further resources for local government entities and supporting them to develop their counter fraud frameworks.

SFO

SERIOUS FRAUD OFFICE

TE TARI HARA TĀWARE

Spotlight on Apprentices

This month we catch up with Jordan White, an Internal Audit and Anti Fraud Investigator at the Royal Borough of Greenwich

Author:
Jordan White, an Internal Audit and Anti Fraud Investigator at the Royal Borough of Greenwich

I worked as an Intelligence Analyst at Medway Council for just over 3 years, before transitioning to a Counter Fraud Investigator role. After that, I moved to the Royal Borough of Greenwich to start a new chapter in my career.

My decision to dive into the Counter Fraud Investigator Apprenticeship (CFIA) stemmed from a realisation I had at Medway Council. Despite a recent promotion, I felt a gap in some areas of my fraud investigation knowledge. The CFIA presented itself as the perfect opportunity to bridge that gap, and thanks to the encouragement and support of my managers, I was able to enrol on the course in November 2021.

Fast forward to June 2023, and I proudly achieved a Distinction in the Accredited Counter Fraud Specialist qualification. Receiving the results was a moment of pure elation - a testament to the dedication poured into the apprenticeship. For me, it was not just a grade; it's a statement that I'm serious about achieving excellence in counter fraud investigation.

Now an Accredited Counter Fraud Specialist, I seamlessly apply my newfound skills at Royal Greenwich. My managers trust me with intricate cases, thanks to the confidence I've gained through the apprenticeship and my growing experience in the role. My success during the recruitment process at Greenwich solidified the impact of my accreditation.

In our fraud team, our mission is clear: combating fraud at every level across the council. Recently, we achieved a significant milestone with a high-profile case resulting in the imprisonment of two ex-employees involved in contractor fraud exceeding £1.5 million[1]. It's these impactful cases which drive my passion for unravelling complex schemes and seeking justice. Looking ahead, I aspire to delve deeper into investigations of this calibre. The thrill of untangling intricate webs of deception, coupled with the pursuit of justice, fuels my commitment to making an impact in the world of counter fraud.
I'm also now collaborating on an exciting initiative with Ben Harrison, Counter Fraud Investigator Apprenticeship lead at HM Revenue and Customs (HMRC), to craft valuable resources for apprentices preparing for their End Point Assessment. The tips and advice are born from first-hand experiences from my apprenticeship, and if they can help fellow apprentices navigate the challenges and triumphs of this journey, I'm all for it. My top tips for other apprentices embarking on this journey are:

Stay consistent - the course spans almost two years so I found that it's important to consistently complete the workbooks and portfolio tasks to a high standard right from the outset. You don't want to be playing catch-up when your portfolio is due at the end of the course. The same applies to off the job learning[2], make sure you are recording your progress from day one.

Speak to others - discussing the course content with your coach, colleagues and other apprentices will help to cement your understanding of what you're learning. I found it very helpful to speak to others about cases that they were working on and try to apply the relevant legislation. This helped me to remember how the course content applies to real-world investigations.

Prepare and practice - when it's time to complete your End Point Assessment

1 https://www.mylondon.news/news/south-london-news/south-london-fraudsters-who-conned-26780471

2 Off the job training must deliver new skills that are directly relevant to the apprenticeship standard. It includes: teaching of theory, practical training, learning support and time for writing assignments. https://www.apprenticeships.gov.uk/employers/training-your-apprentice

you'll need to set aside some time to revise. I would recommend you create a set of 'mock' questions which cover all the different topics in the course. Then prepare your answers using bullet points and practice answering these questions out loud. The professional discussion is a unique way to be tested, and if you're not used to this method of testing, it can be challenging to formalise your thoughts in a verbal answer. Practice makes perfect.

Attention to detail - when marking your portfolio of evidence, the main thing the assessor will be looking for is that it helps to demonstrate the knowledge, skills and behaviours (KSBs) you have learned. However, it will not hurt to spend a little more time giving your portfolio a professional finish. Consider checking that you have a consistent layout, headings and font size. You may also want to input your organisation's logo to complete the look.

Don't panic - remember that the professional discussion and presentation are underpinned by your portfolio and investigation report; you don't have to demonstrate all your knowledge in these sessions. For your investigation report and presentation, don't be tempted to just pick the most complex case you have worked on. Instead think about picking a case you had the most involvement in, you know inside out and can speak confidently about.

Lastly, remember that the assessor is on your side and will ask you probing questions which help you to meet any KSBs that have been missed from the marking criteria. This is when you can draw upon your experience from other more complex investigations that you've worked on.

As I continue honing my investigative skills and contributing to the fight against fraud, I find immense satisfaction in sharing lessons learned and supporting others on their paths to success. Here's to the pursuit of knowledge, the thrill of investigation and the collective effort in safeguarding against fraud.

If you wish to report an incident of fraud against the Royal Borough of Greenwich, please call our 24 hour helpline on 0800 169 6975 or email us at fraud@royalgreenwich.gov.uk

Editor's note:

Individuals from the public sector or local authority who successfully complete the Counter Fraud Investigator Apprentices are eligible for membership to the Government Counter Fraud Profession. This grants them privileges such as access to Continuous Professional Development events, exclusive access to GCFP events, opportunities to collaborate on and contribute to ongoing GCFP projects, and access to a vibrant counter fraud community.

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

ROYAL borough of GREENWICH

Identifying and tackling fraud in the heart of communities

Author:
Joseph Whitfield
Head of Strategy and Stakeholder Engagement
National Fraud Initiative
Public Sector Fraud Authority

The Public Sector Fraud Authority (PSFA) is committed to better understanding and reducing the impact of fraud against the public sector.

A vital element of the public sector is that of local government, and the services they provide for communities across the UK. From services such as waste management, education provision, transport and road maintenance and social housing, local authorities are at the core of how our communities operate. Just like any other public sector organisation - they are under the constant threat from the impact of economic crime and fraud.

Enter the National Fraud Initiative, a cornerstone of the PSFA's Data and Intelligence services.

National Fraud Initiative (NFI)

Established in 1996, the NFI supports c.1100 public and private sector organisations in enhancing their fraud response through the use of data and analytics. It works primarily with local authorities across the UK, working in partnership with Audit Wales, Audit Scotland and the Northern Ireland Audit Office.

The NFI specialises in data matching, using a range of products and data matching techniques to help detect and prevent fraud. The NFI's cutting edge data tools help identify businesses and people trying to steal public money, particularly from local government organisations.

The NFI utilises legislative powers for voluntary and mandatory data collection, processing and disclosure for fraud, in the Local Audit and Accountability Act 2014 and relevant devolved legislation.

The NFI is, and continuously aims to be cost neutral to government, funding its activities (including pay) through fees levied on participants and charged - for services, demonstrating exceptional value for money for the taxpayer.

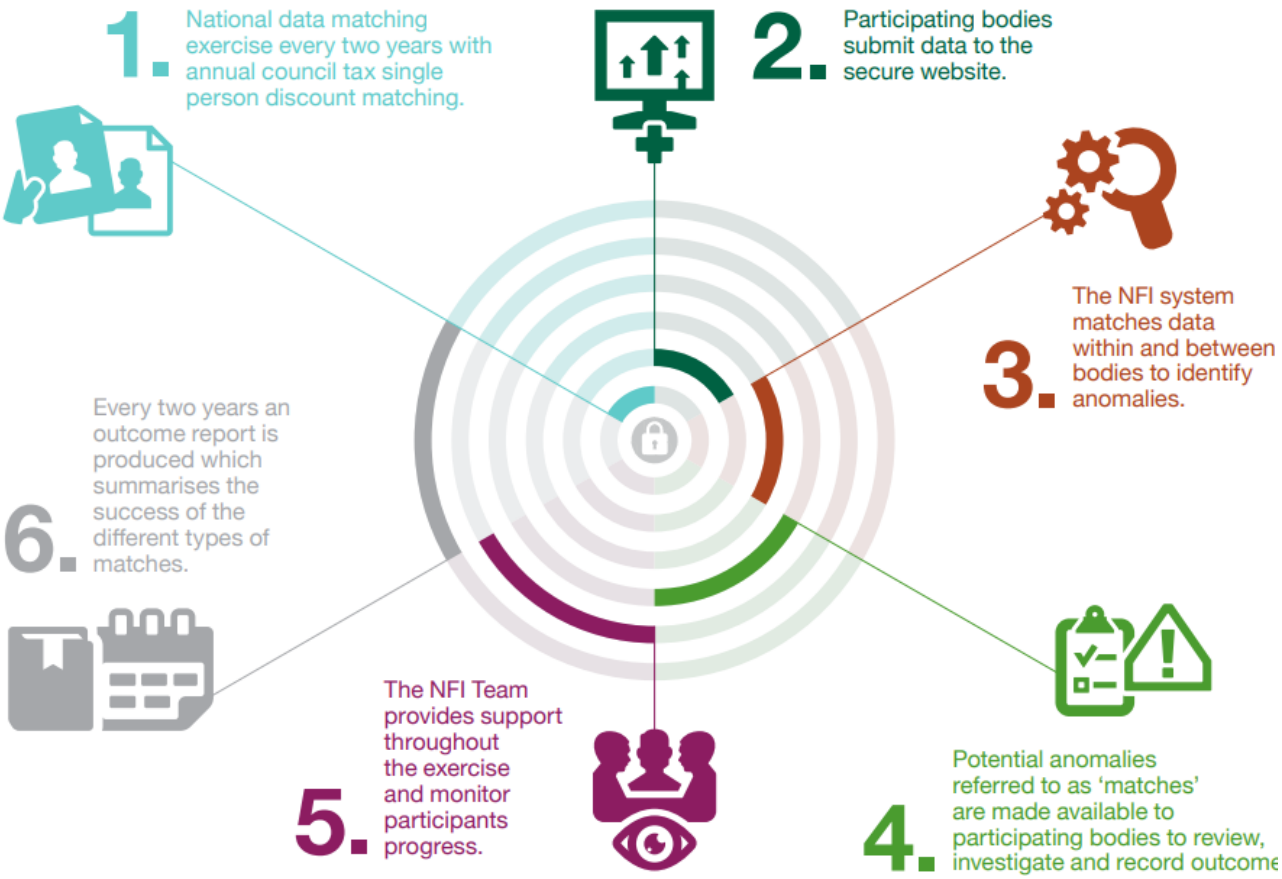
Data matching and intelligence

Data matching involves comparing sets of data electronically, such as the payroll or benefit records of a body, against other records held by the same or another body, to see to what extent they match. The NFI data matching identifies inconsistencies that require further investigation and allows potentially fraudulent claims and payments to be identified. Participating organisations receive the resulting data matches for consideration and investigation, where appropriate.

No assumption can be made as to whether there is fraud, error or another explanation for those matches until an investigation process is completed, and an organisation can then take the appropriate action. This may be to prosecute cases of fraud, recover overpayments, correct underpayments and update records as appropriate.

National Fraud Initiative

One of the primary methods in which the NFI undertakes national data - matching is through our National Exercise, which takes place every two years. A visualisation of the exercise can be found below:



As well as the National Exercise, the NFI operates three additional products which are focused on improving the access and utility of data in order to better detect and prevent fraud and error. Participants pay an additional fee in order to use any of these three services. See details below:

FraudHub enables individual organisations or groups of neighbouring organisations to regularly screen more than one dataset with the aim of detecting errors in processing payments, or benefits and services.

AppCheck is a fraud prevention tool that helps organisations to stop fraud at the point of application, thereby reducing administrative and future investigation costs.

ReCheck is a flexible batch matching tool that allows an organisation to repeat national batch matching at a time to suit them.

Our impact

Since it began, the NFI has delivered £2.4bn in audited cumulative savings. Of which, £443m was prevented and detected/recovered across the UK between April 2020 to March 2022 - the NFI's best result from a National Exercise period.

"Money stolen from the government through fraud is theft from every taxpayer. The NFI's [most recent] report shows we saved the taxpayer **£443m**. When the country is tightening its belt, government must do the same".

- Minister for the Cabinet Office, Jeremy Quin

Putting this into context

£443m alone covers average NHS healthcare costs for **129,000 UK citizens** in a year.

Some further examples of the NFI's recent achievements from the 2020-22 National Exercise period include:

- 102 local authorities identified c.7,000 people waiting on social housing waiting lists, despite being ineligible, were identified and removed, helping to open up affordable housing for those who need it;
- Over 225,000 concessionary travel passes were cancelled in England alone as the passholder was deceased;
- Over 42,000 blue badges were cancelled as the badge holder was deceased; and
- Over 32,500 incorrect claims for council tax single person discount were identified and resolved, with a further 3000 cases identified whereby council tax reductions had been claimed incorrectly.

What does the future hold?

Over the past two years, the NFI has initiated a comprehensive innovation programme. This has included a review of risk scoring, improved management information, undertaking pilots with new datasets and carrying out user engagement to provide input into the modernisation of the NFI's user interfaces.

This programme helps the NFI better understand how additional datasets can target fraud. Through this programme, the NFI will continue to innovate and seek to enhance NFI data matching techniques (e.g., refining matching rules, enhanced risk scoring through AI and predictive analytics) to improve accuracy and quality.

The NFI is also currently developing its future 2024-28 strategy to set out our vision and vital objectives for the future. We hope to announce more details on this ahead of the next edition of the Journal.

How to find out more?

If you have any questions, or if you want to know more about our work, please:
visit our website, where you can read our National Reports and case studies, by scanning our QR code on the below; or email us at nfiqueries@cabinetoffice.gov.uk

Unlocking billions through improved fraud and error reporting

Government could free up significant sums to spend on its priorities by continuing to embed more consistent financial reporting of fraud and error across the public sector.

Author:
Joshua Reddaway
Director Fraud and Propriety
National Audit Office (Fraud & Propriety Centre)

Author:
James Ball, Senior Auditor,
National Audit Office (Fraud & Propriety Centre)

Since the COVID-19 pandemic, the government has stepped up its efforts to tackle fraud and error in public spending by establishing the Public Sector Fraud Authority (PSFA), enhancing requirements around fraud risk assessment, and investing more in high - risk departments. Yet most areas of expenditure outside of tax and welfare are still not currently subject to robust fraud risk assessment or measurement - potentially costing the taxpayer billions of pounds a year. Clearly, there is much work to be done.

The pandemic exposed government to more fraud

The government's pandemic response involved making difficult decisions at pace that increased its exposure to fraud. At the National Audit Office (NAO), we saw a dramatic rise in the levels of fraud and error reported in the accounts that we audit, reflecting the nature of the response as public bodies found themselves under enormous pressure.

The government responded at speed to a virus that caused significant disruption to people's lives, public service provision and society as a whole. It had to continue delivering essential public services while reprioritising resources to respond to the pandemic and supporting staff in working from home. This was only possible because of the immense dedication of workers across the public sector, who had to adapt to new ways of working.

But it came at a cost. Departments and other public bodies were called upon to pay large amounts of money, at speed, in new ways, often to unfamiliar parties. This reduced the government's ability to minimise fraud, as it had to make difficult decisions involving trade - offs between speed of response and protecting propriety and the taxpayer.

Government upheld transparency by continuing to publish audited accounts

At the NAO, our role in auditing the accounts and reporting on government's use of resources remained largely unchanged throughout the pandemic. Despite the huge demands on departments' time and resources, government had committed to produce accounts in the normal way and, in the main, we received the accounts in reasonable time and were able to audit them despite the remote working. This meant that despite the risks being taken, the basic framework of sound financial management was maintained.

This was essential for understanding what was going on with fraud and error. For the most significant and high - risk areas of emergency spend - those where the risk was "material" to the organisation's expenditure - departments were required under government accounting rules to disclose estimates of the levels of fraud and error in their accounts.

The most significant areas of fraud and error in the government's emergency spending are now widely known: the Bounce Back Loan Scheme, furlough and self - employment support schemes, and a sharp rise in Universal Credit fraud.

Disclosing fraud and error estimates proved to be an essential backstop against public sector fraud and a crucial mechanism for holding the government to account over its emergency response. The sessions of the Committee of Public Accounts, where senior civil servants have been challenged to publicly justify their decision - making, have provided the basis for public scrutiny of these pandemic responses and a means to learn lessons for the future.

While there were clear shortcomings during the pandemic, proper accounting and audit ultimately succeeded in providing transparency, without which there would have been no way for the public to understand the extent of the public money lost to fraud and error. This was a key factor behind the government's decision to increase counter-fraud investment and establish the Public Sector Fraud Authority (PSFA).

Levels of fraud and error in public expenditure are still high…

The estimated level of fraud and error reported across the accounts we audit was at least £10 billion in 2022-23 - almost double the amount in the years before the pandemic.

This is for two reasons. First, there has been a sustained increase in benefit fraud – the area with the most mature reporting mechanisms. Second, even outside of benefits, public bodies now possess a greater awareness of fraud and error and have doubled their reporting of such cases in accounts.

This tallies with the experience of counter fraud teams. At the same time, we have seen an increase in the level of detected fraud and recoveries that they report.

…but fraud levels fall when there is sustained measurement and reporting over time

That said, as we reported to Parliament in March 2023, most areas still do not have proper risk assessment mechanisms and are unable to accurately measure the extent of fraud[1].

Actual levels of fraud and error are therefore likely to be far higher than what we see officially reported.

There are still too few examples outside of welfare and tax where there has been consistent reporting of robust fraud and error estimates over several years' worth of accounts.

But in the few examples where there has been consistent reporting, we have seen a fall in the levels of fraud and error reported. The evidence is building that where better and consistent measurement and reporting incentivises better management of the levels of fraud and error in an area of spending, public bodies can save money.

Effective fraud risk management

There is now broad consensus among experts that improved management can be achieved by embedding the 'fraud risk management cycle' into public spending initiatives.

Managing Public Money - the government's key guidance on spending rules - was updated in May 2021 with an expanded annex covering the management of fraud and how to implement this cycle. The NAO suggests using a slightly more detailed version where you have already identified a significant risk (see Figure 1 below).

At the same time, HM Treasury has also strengthened the requirements at the start of the cycle. As of 2022, departments must undertake an Initial Fraud Impact Assessment during the design phase of significant new areas of spend.

This means that public bodies are now required to undertake a rapid assessment of potential fraud risks in policies so that appropriate controls can be designed and put in place before implementation.

Where a higher risk of fraud and error is identified, the public body can then proceed to carry out a full fraud risk assessment, including an assessment of the effectiveness of those controls.

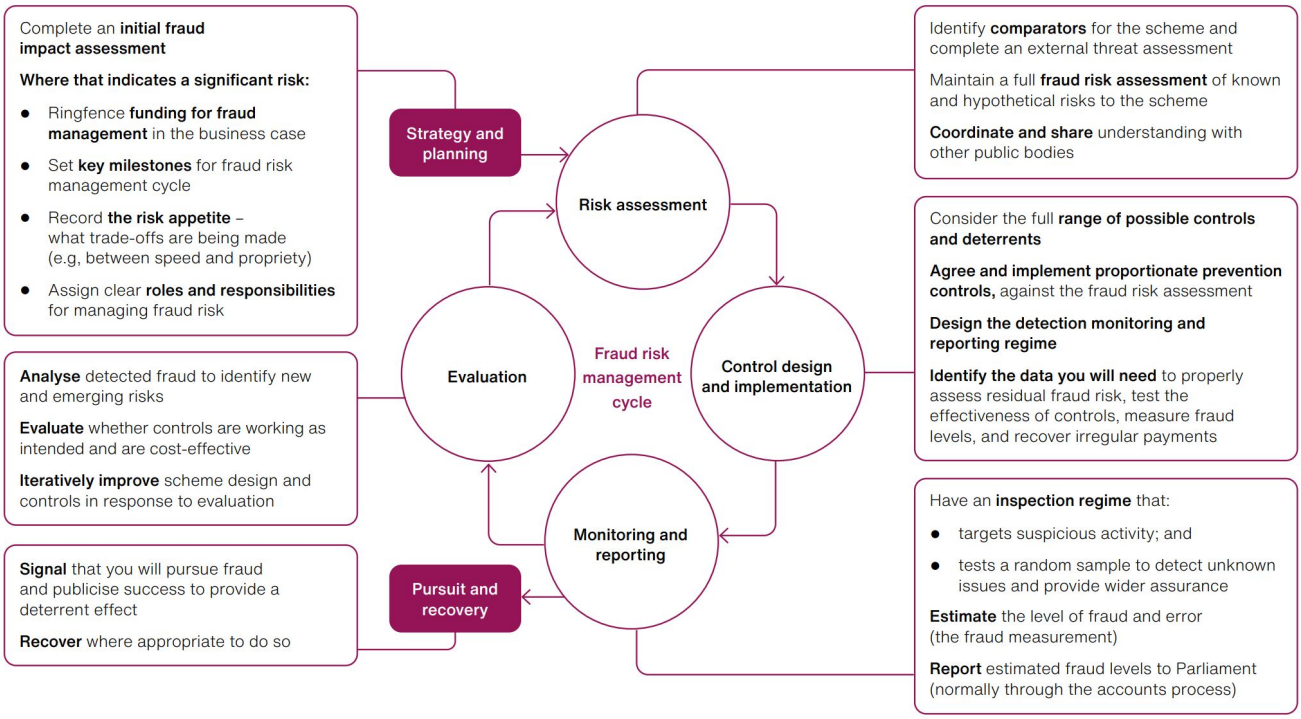
Improved implementation of the cycle will generally enable better, more consistent reporting in the form of fraud and error estimates in audited accounts.

This will provide a crucial incentive for public bodies to improve their management of fraud risk by continuing to work through the cycle.

1 NAO, Tackling fraud and corruption against government, HC 1199, March 2023. Available at: https://www.nao.org.uk/wp-content/uploads/2023/03/tackling-fraud-and-corruption-against-government.pdf

This, in turn, should result in better fraud outcomes over time, in a virtuous circle of improvement - representing a major opportunity for the government to generate significant savings which can then be spent on its priorities - a helpful boost during a difficult period for the public finances.

Figure 1: Fraud risk management cycle



Stumbling blocks

Despite the potential for billions of pounds in savings, there are a number of challenges that will make it difficult to embed more consistent reporting of fraud and error across government.

First, some areas of government may find it difficult to acknowledge that there is a fraud or error problem in their spending worth the investment necessary to manage it.

Second, where public bodies do not have a good understanding of their fraud risks, they may struggle to identify the areas of spending that need measuring. As we reported in March 2023, only 14% of government bodies both understand and have sought to measure the fraud risks they face. While mandating Initial Fraud Impact Assessments for significant new spend is welcome, there is still a long way to go.

Third, it is important that public bodies report on estimated levels of fraud, not just the amount that is directly detected. This is because an estimate can provide an indication of the total potential value of fraud across an area of spending, and incentivises a focus on prevention. Detected fraud, by contrast, is more straightforward to report as the examples of loss are known and recorded. However, at best, this does not represent the full extent of the problem. At worst, focusing on detected fraud and recovery creates perverse incentives not to address the root cause of the problem.

Finally, the skills needed to effectively measure fraud are in short supply across the whole of government. The production of robust estimates can be a complex business and typically requires the use of statistical sampling and large numbers of people to do the work. Analytical procedures to identify potential problems remain fairly under-developed.

Conclusions

Unlocking the full potential of the savings available through better reporting and management of fraud and error will not be easy. It will require a commitment to embed the right skills and to prioritise proper fraud management, not just in tax and welfare, but across the whole of the public sector.

But with so much on the table in terms of efficiencies, we are confident that significant sums can be released - ultimately making a substantial contribution to the overall public finances.

The Complex relationship between fraud and technology - Should we ignore or regulate online platforms?

Author:
Jack Whittaker: PhD Candidate (crim.) at the University of Surrey
j.m.whittaker@surrey.ac.uk

There is little doubt that throughout history there have been many frauds that have been committed with the aid of various technologies. For example, the invention of the printing press by Johannes Gutenberg in 1440 provided with it novel opportunities for offenders to create new means of committing economic fraud by flooding the literature market with the counterfeited works of early publishers. Likewise, the works of Heather Shore in her account of crimes in London from 1720-1930 describes an increase in organised syndicates of "swindlers, coiners and fraudsters" from at least the early 18th century, many of which possessed sophisticated technological know - how. One account provided by a police inspector in 1862 illustrates a particularly salient case whereby an individual called Joseph Jones, his wife Elizabeth Jones, and neighbour William Smith were found to be producing counterfeit florins by electroplating base coins with wires and galvanic batteries, a process which sought to create a silver outer coating on the coin (Shore, 2015, pp. 124). In contemporary society, by contrast, the majority of frauds committed are now perpetrated online in so-called 'cyberspace' (61%) (Ons.gov.uk, 2022).

The growth of online platforms is one such technology that has in the past twenty years provided ample opportunity for fraudsters. In one instance, we have seen the industrialisation of older frauds (Button & Cross, 2017). Academic researchers have uncovered how fraudsters have sought to move away from committing face-to-face frauds in the real world, such as consumer fraud and romance fraud, and that they have sought to perpetrate these crimes online in e-commerce and dating platforms to name but two notable examples. (Treadwell, 2012; Whittaker & Button, 2020; Gillespie, 2017). In addition to this, fraudsters have now sought to create new frauds (Button & Cross, 2017) such as tailor-made 'fraud-as-a-service' products (McGuire, 2017). The opportunity to bulk-buy fake reviews on e-commerce platforms and bank accounts used in laundering the stolen funds of victims on social media websites are two notable examples of this.

A natural question arising from this issue is "should we care that technology is used in the perpetration of fraud?" On the one hand, proponents of the instrumentalism perspective of technology argue that no we shouldn't care. Technology under the instrumentalism perspective is viewed as being neither good nor evil and that it should not be regulated. A notable example of instrumentalism can be attributed to a slogan commonly used by the US gun lobby to oppose the regulation of firearms, that "guns don't kill people, people kill people" (Henigan, 2016). On the other hand, technology can be viewed through the lens of extension theory (See Kepp, 1877; McLuhan, 1964; Brey, 2010) which argues that technology extends human agency by expanding the opportunities of what is capable without the use of technology. Therefore, under the extension theory perspective regulation is necessary because technology amplifies the modern fraudster's capabilities.

Extension theory can also be useful in explaining the growth in fraud victimisation on online platforms. Marshal McLuhan for example in his influential book 'Understanding Media' (1964) argues that in addition to extending capabilities, technology can also result in 'amputations' of various kinds. To use

a simple example of this, one could argue that the development and widespread adoption of guns resulted in a loss of archery skills. In the context of 'cyberspace', users arguably sacrifice their mental faculties like concentration or memory in favour of convenience, the speed at which transactions occur and the opportunity to create new interactions inside of a digital environment. For example, instead of consumers visiting a traditional "bricks and mortars store" to inspect a product and determine that what they are intending to buy actually exists and is of a sufficient quality, consumers that elect to use online retail platforms instead amputate their senses and are more willing to 'trust' that the seller is reputable and not intending to defraud them. Likewise, this is also the case in online dating whereby internet users 'trust' that the person they have met on a dating platform is who they claim to be. Arguably, as well as the increased vulnerability that internet users put themselves at when they are using the services of online platforms, there are also other issues that contribute to victimisation. For example, many online platforms have very little 'know your customer' (KYC) processes. Platforms often purposely open the proverbial floodgates as a means of attracting as many users as possible, particularly when they utilise a freemium business model. In the case of many online dating platforms for example, one can merely sign up for a free account without any formal checking procedures.

Additionally, one can argue that platforms can in fact benefit from fraudsters operating on them. For the purpose of this short article, I have unpacked these into three benefits which are by no means extensive.

1. To inflate user figures. For example, after the Ashley Madison data breach in 2015 it was discovered that nearly every female profile was either fake or dormant as a means of luring men onto the platform (Gallagher, 2015).
2. To generate income. A key component of the online fraud economy is that fraudsters need to spend money to make money. An example of this is how many fraudulent e-commerce websites reinvest their previous victims stolen funds onto search engine advertising campaigns as a means of attracting traffic to their website.
3. To decrease cost. It is simply easier and cheaper for platforms to ignore instances of fraud by not training a well-resourced abuse department.

In summary, this short article has sought to introduce the notion that there is a historical relationship between technology and fraud, that two opposing viewpoints argue whether technology is or is not capable of harm, and lastly that platforms can in fact benefit from fraudsters operating on them parasitically. Given that there is an ongoing tidal wave of online parasitic platform criminality, it is arguably not enough for platforms to continue ignoring the problem of online fraud or for this problem to be moderated haphazardly by abuse algorithms. After all, fraud is an inherently human - centric crime which in most instances relies on communication between the fraudster and their victim, meaning that a trained human is often needed to identify that a fraud is taking place. In the longer term, a suggestion is that 'know your customer' verifications should be a mandated part of any online platform's business model. It is not simply enough for platforms to play whack-a-mole with fraudsters by taking down some fraudulent content only for it to appear again later.

References:

Brey, P. (2010) 'Philosophy of Technology after the empirical turn', Techné: Research in Philosophy and Technology, 14(1), pp. 36–48. doi:10.5840/techne20101416.

Button, M. and Cross, C. (2017) Cyber frauds, scams and their victims. London: Taylor and Francis.

Gallagher, C. (2015) Ashley Madison and the ethics of disclosure! Chuck Gallagher. Available at: https://www.chuckgallagher.com/2015/08/21/ashley-madison-and-the-ethics-of-disclosure/ (Accessed: 27 October 2023).

Gillespie, A. (2017) 'The electronic Spanish prisoner: Romance frauds on the internet', The Journal of Criminal Law, 81(3), pp. 217–231. doi:10.1177/0022018317702803.

Henigan, D.A. (2016) 'guns don't kill people, people kill people': And other myths about guns and gun control. Boston: Beacon Press.

Kapp, E. (1877) Grundlinien einer Philosophie der technik: Zur Entstehungsgeschichte der cultur aus Neunen Gesichtspunkten. Braunschweig: Druck und verlag von George westermann.

McGuire, M. 2018. Into the Web of Profit: Understanding the Growth of the Cybercrime Economy. [online]BromiumInc.Availableat: <https://www.bromium.com/wp-content/uploads/2018/05/Into-the-Web-of-Profit_Bromium.pdf> [Accessed 26 March 2021].

McLuhan, M. (1964) Understanding media. McGraw-Hill.

Ons.gov.uk. (2022). Nature of fraud and computer misuse in England and Wales: Year Ending March 2022. Nature of fraud and computer misuse in England and Wales. Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/

Public Sector Fraud Model (PSFM): A new model to counter fraud designed

Author:
Chris Freeman, Head of Risk, Threat and Prevention, Public Sector Fraud Authority

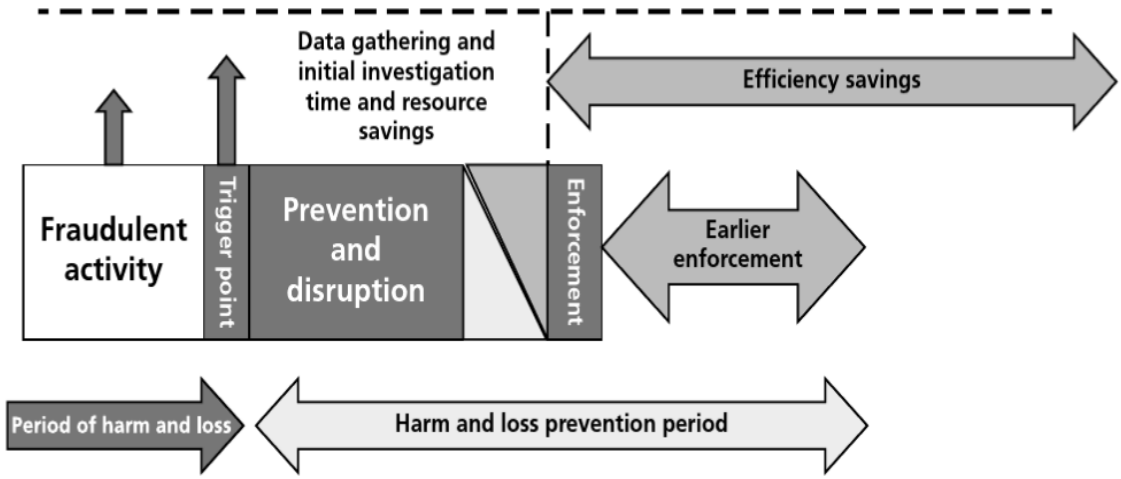
Author:
Michael Betts PSFA Head of Capabilityand Learning, Public Sector Counter Fraud Authority

In 2005, the Association of Chief Police Officers (ACPO) published 'Practice Advice on Core Investigative Doctrine' containing a 'model' of how investigations should be conducted (Association of Chief Police Officers, 2005, pp.48-53), which was developed as a definitive guidance for all investigators as part of the Professionalising the Investigation programme. In 2013, recognising the differences between fraud crimes and other crime types, the City of London Police (CoLP) Economic Crime Academy developed the Fraud Investigation Model (FIM).

The FIM is designed to help guide the process of all fraud-related investigations, from instigation through to prosecution.

It redefines the investigative process to "reduce the potential period of harm caused by the fraudster…" as "...following the instigation of the case, emphasis is placed upon opportunities for early disruption and prevention" (Betts, 2017, p.29). By reducing the time lag between the 'trigger point'—when the fraud was detected or reported—and subsequent enforcement action "...the loss caused is significantly mitigated by reducing the enablers and vulnerabilities that the fraudster uses to perpetrate their crimes" (Betts, 2017, p.29).

Figure 1, below, shows an overview of the FIM. The model itself is more detailed, but it is this summary view that is of use here.



Introducing the Public Sector Fraud Model

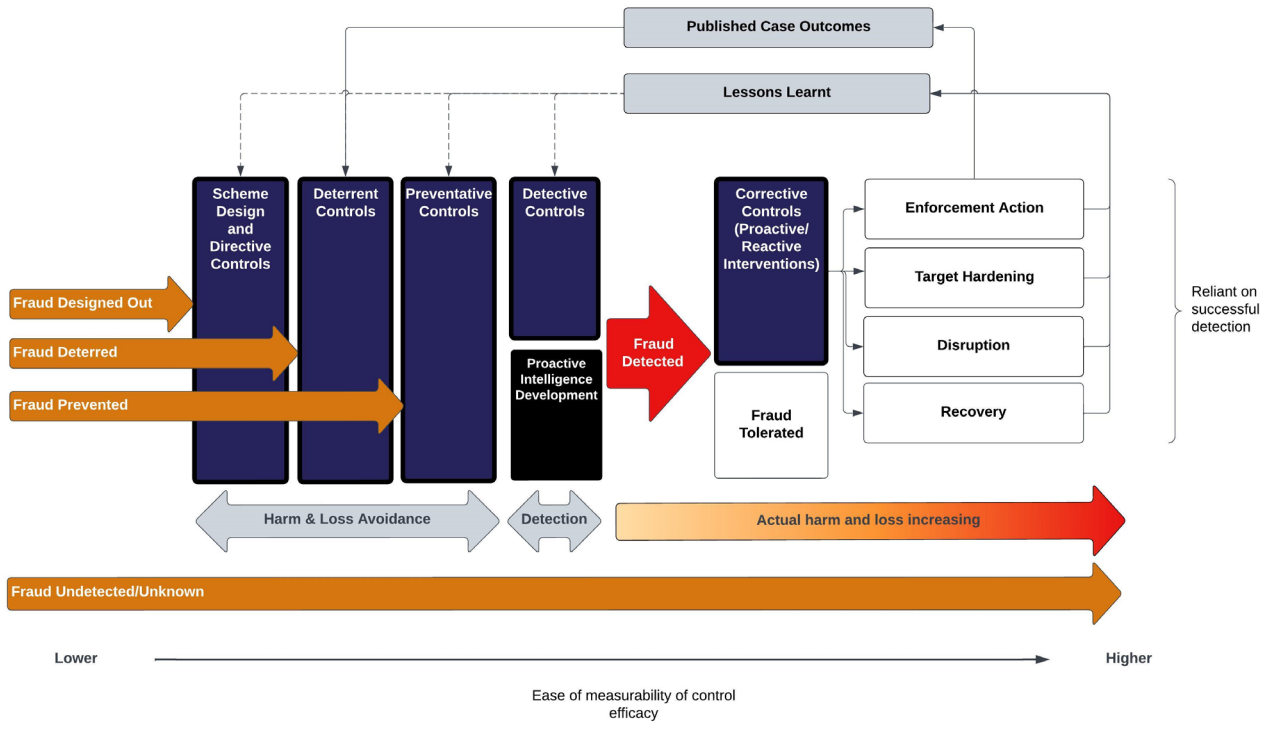
Just as the FIM was built upon the foundations of the model in the Core Investigation Doctrine, we now seek to build a new model upon the FIM, which recognises the wider counter fraud environment across the public sector and highlights the layers of defence designed to stop fraud before it can occur. The focus here is on fraud against the public sector, rather than that targeting individuals, businesses or charities, hence being called the Public Sector Fraud Model (PSFM), which is shown in Figure 2, below, although it may have some general applicability in combating fraud against other types of organisations. The model was not created as part of any formal design process, but as part of an assignment during a training course in which the FIM featured as an example of best practice, and further discussion with one of the authors and advocates of the FIM.

Further iterative development then occurred, including utilising the feedback of numerous colleagues with a deep understanding of public sector counter fraud.

The main elements of the FIM remain central to the new model, which continues to favour early interdiction wherever possible and - where fraud does happen - responding swiftly to deploy both fraud prevention and disruption techniques. This new model recognises that the investigation is only part of the counter fraud ecosystem, and only necessary where fraud has not been avoided or prevented.

The Model is, of course, incomplete: it is not possible to fully map the complex system that is a comprehensive counter fraud response but is a high - level representation of it. It does not appear in the standards or guidance published by the Government Counter Fraud Profession or Public Sector Fraud Authority.

Figure 2: The Public Sector Fraud Model



The elements of the new model

Below we explain the individual elements in detail, but firstly a quick explanation of the overall layout: The vertical blue columns represent the different categories of controls that can be used. The horizontal orange arrows list different ways that can be used to categorise fraud for reporting purposes - their length is representative of the relative degree of harm and loss of each category. If the head of an arrow meets an effective control the fraud stops at that point.

Designed-out fraud

Our model seeks to highlight that the most desirable state is where fraud can be 'designed out' and stopped before it is instigated. This is achieved through, for example, clear eligibility criteria and also directive controls, which "include guidance, policies and legislation [that] state the practice to be followed, but do not stop fraud and bad practice occurring…" (Government Counter Fraud Profession, 2023, p.34)

Deterred fraud

Deterrent controls "...aim to put people off of fraud" (Government Counter Fraud Profession, 2023, p.34). Organisations commonly attempt to deter would-be fraud criminals through making clear that detection is likely and the potential consequences of being caught. Part of this is the publicising of the outcomes of cases, such as press-releases following criminal conviction; note the feedback loop in the PSFM from the enforcement action cell back to the deterrent cell. It is perhaps arguable that the ordering of the cells containing deterrent controls and directive controls in the model could be interchangeable or parallel.

Prevented fraud

Preventative controls "...aim to stop the fraud entering the system or reduce its impact…". (Government Counter Fraud Profession, 2023, p.34). There is an interesting nuance here which is not always considered: preventative controls ideally make it impossible for fraud to happen, for example representing a barrier that a would-be criminal cannot overcome. But, once one of the actions described in the Fraud Act 2006 has occurred (false representation; abuse of position; failure to disclose information) then fraud has happened, regardless of whether the criminal is successful in gaining from it: There can be no 'attempted' fraud.

Detected fraud

Detective controls "...aim to find or identify fraud after it has happened and can impact on its duration and impact…" (Government Counter Fraud Profession, 2023, p.34). There are two possible scenarios here: fraud which has been detected after it has happened and ended prior to being uncovered (assuming it is a one-off event); or, fraud which has been detected whilst in progress and which has been allowed to continue for a period post-detection. The second case is what the previous FIM intended to address, favouring earlier intervention and disruption to limit the period of harm or loss (see below). In both cases efforts to recover any sum defrauded are corrective controls and criminal or civil sanction are the potential enforcement outcomes, although this does not necessarily follow: see below for more on this point.

Tolerated fraud

It is acknowledged that this may be the most controversial element of the model at first glance; fraud that is detected but no action is taken to recover any losses or penalise perpetrators. Yet this is a reality of some public sector fraud: resourcing does not allow for all data matches to be followed up, nor every hotline report to be subject to full investigation. This fraud is therefore considered 'tolerated'.

Undetected / or unknown fraud

Those familiar with the "Fraud Iceberg" metaphor will know that a significant proportion of fraud goes undetected and unknown. In 2023 the Public Sector Fraud Authority Cross Government this was estimated to total £2.9bn to £28.5bn annually, or 0.5% to 5.0% of public services expenditure. (Public Sector Fraud Authority, 2022, p.25)

Lessons learned

It is imperative that all parts of the system both feed into - and benefit from - an ongoing collation of insights across the whole model. Root cause analysis is a good example of this (Government Counter Fraud Profession, 2023, p.60), with outcomes used to improve the whole system where possible. Lessons are only learned when these insights are acted upon, although this point is often overlooked, and opportunities for improvement are lost.

Dependent controls

The PSFM shows that a control environment ideally comprises a range of measures to minimise fraud, or to mitigate its impact should it occur. The efficacy of types of control will depend on the nature of the threat: deterrent messaging is less likely to be effective against serious and organised crime, although can displace fraudulent activity; corrective controls aimed at recovering sums lost to fraud depend on an ability to repay. Ideally there will be more than one of each category of control in place, meaning that when an attempt evades one control there can be further opportunities to still avoid the fraud risk crystallising.

The new model also illustrates that some types of control are dependent on others being in place and operating correctly. For example, while corrective controls are a common part of fraud risk management approaches - such as clawback clauses in contracts - often there is no corresponding means of detecting that the fraud has happened. Consequently, there is no means of triggering the corrective control and the fraud will actually remain undetected.

Control efficacy

Criminal convictions provide an easy measure of counter fraud activity, but these only occur once the fraud has happened, has been detected and successfully prosecuted. To some degree this is a counterintuitive measurement as it is, in reality, measuring the level of failure of the control regime. These figures are also perhaps the weakest measure due to the failings in reporting, resourcing and prosecuting fraud offenders in England and Wales (House of Commons Justice Committee, 2022). Each successive step brings additional cost. While there may be some limited success in recouping these - and even confiscation of criminal proceeds - it can be slow and a positive result is not guaranteed and the costs involved can outweigh the recoveries made. It is demonstrably better for the fraud to be prevented or, even better, made impossible through the careful design of the scheme.

The best scenario is designing out opportunities for fraud to occur in the first place, where this is possible. But, as the model shows, the earlier in its life the fraud is stopped, the harder it is to measure the efficacy of the control that stopped it. But the absence of evidence of efficacy here is not necessarily evidence of absence: while it may be harder to show the direct impact of measures that reduce the likelihood of fraud from happening at all, the utilisation of counter fraud expertise during careful scheme design may obviate the significant cost of recovery later on.

Conclusions

The FIM was an important step forward in recognising the difference between most crime types and fraud with repeat offending of a corrosive nature; once detected interventions need to be speedy to limit the harm and loss period. The proposed Public Sector Fraud Model is intended to provide a more holistic way of looking at the counter fraud response in the public sector, including recognising the importance of a cohesive whole-system approach and to illustrate interdependencies that are not always well understood. The model is applicable internationally and is not affected by the increasing complexity of methods employed by criminals in perpetrating fraud. It draws together current practices: it is hoped that this will be the first step on the journey towards visualising how to model counter fraud in the public sector.

It also raises some interesting new questions: What proportion of fraud against the public sector falls into each of the categories? How can we better evidence the impact of the controls to the left of the model, to show how they work to reduce fraud while the harm and loss is minimised? How can the model be adapted to encompass fraud perpetrated against individuals, businesses and charities?

Most importantly, what might the next iteration of the model look like?

References

- Association of Chief Police Officers. (2005). Practice Advice on Core Investigative Doctrine. National Centre for Policing Excellence.
- Betts, M. J. (2017). Investigation of Fraud and Economic Crime (N. Court & D. Clark, Eds.). Oxford University Press.
- Government Counter Fraud Profession. (2023). Fraud Prevention Standard for Counter Fraud Professionals. Public Sector Fraud Authority. https://www.gov.uk/government/publications/government-counter-fraud-profession-standards-and-guidance
- House of Commons Justice Committee. (2022). Fraud and the Justice System. House of Commons. https://committees.parliament.uk/publications/30328/documents/175363/default/
- Public Sector Fraud Authority. (2022). Cross-Government Fraud Landscape Annual Report 2022. Public Sector Fraud Authority.

Notes

Government
Counter Fraud
Profession

Contact us:

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