



Government
Counter Fraud
Profession

THE PUBLIC SECTOR COUNTER FRAUD JOURNAL

ISSUE 16, SEPTEMBER 2025



ISSN 2755-1024



CONTENTS



Editor's Letter

David Whitehouse-Hayes

03



Help Shape Future Editions

05



How Companies House is Tackling Economic Crime

Matthew Pennell

06



Designing Controls with Behaviour in Mind: Addressing Insider Fraud -

Dr Rasha Kassem

11



Why a Fraud Control Apprenticeship?

Michael Betts & Dr Michael Gilbert

18



Why Fraud is a Global Business Opportunity for OCGs?

Laura Eshelby

23



Stammering and Fraud - Conflicts between Fraud Detection Controls and Customers Who Stammer

Claire Maillet

28



Ticket Scams: The Cost of Being a Fan?

Aisling Twomey

34



Serious Games for External Fraud Risk Analysis at the Canada Revenue Agency

Madeline Johnson

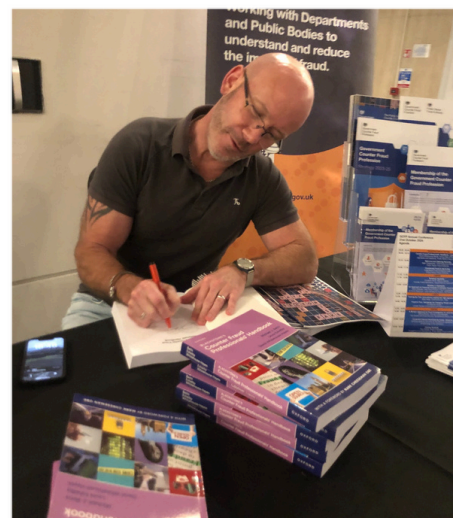
37



GCFP at Civil Service Live

42

EDITOR'S LETTER



Dear Readers,

I'm delighted to introduce this special edition of the **Public Sector Counter Fraud Journal (PSCF)**, which marks the **seventh anniversary** of the **Government Counter Fraud Profession (GCFP)**, a milestone that invites us to reflect on just how far we've come since our launch events back in **October 2018**.

The decision to formally establish the GCFP was years in the making. It began with committed individuals from across the public sector coming together around a shared belief: that counter fraud should be recognised as a profession in its own right, requiring a unique blend of skills, knowledge, and experience.

Even before our launch, we were laying the groundwork: shaping standards, developing proactive disciplines beyond investigation and intelligence, and engaging with a wide range of stakeholders, from central and local government, to the police, NHS, and the private and third sectors. Thanks to this early momentum, the GCFP was ready to hit the ground running.

At the time of our launch, we had a membership of around **3,000 professionals**, mostly from established areas like Investigation and Intelligence, representing a broad range of organisations. Looking back, that felt like a huge step and it was.

But what we've built since then is even more extraordinary. Seven years on, our membership now stands at over 9,500, representing more than 70 organisations. We've diversified entry routes, for example, through the Counter Fraud Investigator Apprenticeship, developed by GCFP Board members and Local Authorities. This opened the door to local government and coincided with our first birthday.

We've also broadened our professional disciplines adding Fraud Risk Assessment and Leadership, Management & Strategy through our Counter Fraud Functional Leaders Development course. The latter ensures that those accountable for fraud services are professionally equipped to deliver strategic counter-fraud outcomes.

EDITOR'S LETTER

Our work on Fraud Risk Assessment has laid the foundation for an emerging Fraud Control cluster and route to membership, recognising the essential links between risk, prevention, detection, culture and measurement. This new cluster is set to launch by 2026, alongside a dedicated apprenticeship scheme, echoing the success of the investigator programme, which has already brought over 400 highly skilled professionals into the profession.

All of this is underpinned by our commitment to robust, evolving standards. We've already published standards for **Fraud Risk, Culture, Detection, and Prevention**, with updated guidance on **Fraud Measurement** coming in 2026 to complete the Fraud Control cluster.

The train we set in motion seven years ago is gathering speed. But it's not just a journey we're taking, it's one you're shaping. Whether through your Practitioner Group, internal GCFP teams, Board representation, or secondments with the central team, there are multiple ways to influence where we go next.

This profession was built on the principles of Collaboration, Pace, Empowerment and Choice. So once again, we invite you to join us, not just as passengers, but as co-drivers of what comes next.
Here's to the journey ahead.



DAVID WHITEHOUSE-HAYES,
Head of Strategy Engagement and
Membership,
Government Counter Fraud Profession,
Public Sector Fraud Authority,
Cabinet Office

HELP SHAPE FUTURE EDITIONS

We're always looking for ways to improve the **Public Sector Counter Fraud Journal** and your feedback makes all the difference.

Scan the QR code below or **click on the link** to complete our short survey. It only takes a couple of minutes, and helps us make each edition better than the last.

Got an article idea?

If you'd like to be featured in a future issue, we'd love to hear from you.

Pitch us your article ideas at **gcfp@cabinetoffice.gov.uk**



<https://www.smartsurvey.co.uk/s/gcfpjjournal/>

Editorial oversight provided by the **Government Counter Fraud Profession (GCFP) Editorial Board**.

Special thanks to **Toni Sless** and **Mike Betts** for their contributions to this edition.

HOW COMPANIES HOUSE IS TACKLING ECONOMIC CRIME



**MATTHEW PENNELL,
HEAD OF INTELLIGENCE,
COMPANIES HOUSE**

Companies House is undergoing a significant transformation following the introduction of the **Economic Crime and Corporate Transparency Act 2023 (ECCTA)** to UK law. The legislative reform strengthens the UK's corporate environment which extends to Companies House to support the efforts in tackling economic crime and aiding economic growth.

The latest [progress report](#) on the ECCTA's implementation was published in June 2025 and offered a revealing update. As the regulatory and enforcement capacity of Companies House has expanded, it is

Companies House is evolving into a proactive fraud-fighting regulator. Backed by the Economic Crime and Corporate Transparency Act 2023, it now has stronger powers to verify identities, challenge suspicious data, and collaborate across enforcement agencies to safeguard the integrity of the UK's corporate register.

starting to see the first tangible results emerge.

This report charts and details the extent of the reforms and demonstrates the steps that the organisation is taking in its fight against fraud and criminal misuse of the register.

Enhanced Powers

One of the core objectives of the ECCTA is to ensure that information on the Companies House public register is accurate and reliable. As such, the legislation affords greater authority to Companies House to prevent the misuse of corporate entities and to contribute meaningfully to the UK's overall efforts to detect and deter fraud.



Consequently, Companies House is now able to query information that appears suspicious and can reject filings outright. Companies House also now has the capability to annotate entries that are misleading or under review and remove false or fraudulent data from the register entirely.

For instance, we are now exercising enhanced scrutiny over company names, actively querying and rejecting those that could mislead the public or imply a false association with established businesses. Where evidence suggests a name is being used fraudulently, or in a way which could be considered as intentionally misleading, we have the authority to intervene as a means of prevention, before any criminal activity can take place. In these cases, we now direct the company to adopt a different name and if it fails to comply, we can enforce a change.

These interventions are carried out by intelligence and enforcement teams which have been granted greater powers, allowing for rapid collaboration with law enforcement and other regulatory bodies such as the Insolvency Service, His Majesty's Revenue and Customs and the National Crime Agency protecting the integrity of the register and those most at risk which closes the gap between registration abuse and criminal prosecution.

Identity Verification and Transparency

Among the most consequential reforms being introduced under the ECCTA is the phased implementation of mandatory identity verification. For the first time, directors, people with significant control (PSCs) and those who file documents on behalf of companies will need to verify their identity through a robust, government-approved process.

Voluntary verification began in spring 2025. From autumn, it will become mandatory for new incorporations and filings, with a mandatory rollout expected to be completed by autumn 2026.

Once operational, the mandatory identity verification will limit the extent to which individuals can disguise themselves with fictitious identities or create convoluted ownership structures to conduct fraudulent or illicit activity.

A crucial step forward has been the establishment of Authorised Corporate Service Providers (ACSPs). Following a soft launch in 2025, third-party providers can now voluntarily carry out identity verification for clients. From spring 2026, ACSPs will also be empowered to submit filings on behalf of companies.

Such reforms are bolstered by additional requirements for companies to provide registered email addresses. They mark a shift toward a digital compliance framework which prioritises traceability and accountability, while enabling Companies House to integrate identity checks with its growing network of partner agencies.

Collaboration Across the Enforcement Ecosystem

The ECCTA does not simply empower Companies House in isolation, it embeds the agency within an anti-economic crime system and compounds our ability to share data, flag risks and support prosecutions. The new data sharing powers have allowed Companies House's Intelligence Hub to disseminate relevant intelligence to key partners, including the National Crime Agency, HMRC, the Insolvency Service and law enforcement. This collaborative work aims to further develop and co-ordinate efforts to tackle economic crime, identify threats to the integrity of the register and support civil and criminal enforcement.

Enforcement in Action

Companies House is targeting the fraudulent practice of identity theft and the creation of fictitious corporate identities which involves registering inappropriate or unauthorised addresses, often without the knowledge or consent of the legitimate individuals or organisations concerned. Notably, from 4 March 2024, it became unlawful for companies to list PO boxes as their registered office address. In advance of this change, Companies House issued 3,800 warning letters to affected entities. By 3 March 2025, this figure fell to 700 companies, of which fewer than 300 remain active and are in the process of being dissolved.

Furthermore, where companies have failed to provide a valid and authorised registered office, Companies House used its newly granted authority to substitute such addresses with a default address.

Since March 2024, this measure has been applied to 82,600 companies. The Companies House Registrar also made extensive use of powers to challenge and remove false or misleading information across the register. As of March 2025, corrective interventions have affected 100,400 companies. These actions included the removal or amendment of 82,600 registered office addresses, 66,900 officer addresses, 55,100 People with Significant Control (PSC) addresses, 49,800 incorporation documents and 11,200 additional filings.

With a view to improving data integrity, Companies House also engaged in collaborative initiatives with external data partners to identify instances where company records included deceased individuals.

Such discrepancies only represented 0.05% of the seven million records examined and were considered to have been present due to potential oversight or possible intent to mislead. In most cases, companies responded promptly and corrected the relevant records. We have also trialled a series of interventions designed to pre-empt high-risk registrations.

These initiatives led to the rejection of over 10,200 suspicious applications, often involving addresses that appeared inappropriate or linked to broader fraud patterns.

Company Clones

One area identified as high-risk since the implementation of the ECCTA has been the hospitality sector, where organised crime groups have sought to exploit the reputations of well-known restaurant brands. The organised crime groups have registered companies under names that appear deceptively similar with an aim to deceive suppliers, open bank accounts fraudulently and carry out illicit activity such as placing large orders or soliciting investment under a fabricated identity.



We're no longer a passive registrar of information. Companies House is now a proactive, risk-focused regulator, empowered to detect, prevent, and respond to economic crime.

There were a number of high-profile restaurant chains and known individuals in the public eye who operated in this sector that were among those who were targeted, and this resulted in substantial media attention. Between December 2023 and February 2024, Companies House intelligence and enforcement teams identified 786 suspected cloned companies linked to this kind of criminal activity.

In response to the identification of these suspected cloned companies, Companies House acted swiftly. Enhanced enforcement powers and improved intelligence-sharing with partner agencies enabled rapid investigation and intervention. The outcome was decisive: 2,895 fraudulent appointments were identified and removed and 965 cloned companies were struck off the register.

A More Transparent Corporate Landscape

The reforms are not limited to companies alone. The Act also extends to transparency requirements of limited partnerships and to the Register of Overseas Entities (ROE).

For overseas entities holding UK property, the ROE aims to improve beneficial ownership reporting and to allow the annotation of suspicious or non-compliant entries. These measures aim to tackle the issue of foreign individuals hiding assets in the UK via anonymous vehicles, a problem that has received increased attention since the Russian invasion of Ukraine.

What's next for the ECCTA?

Despite clear progress, the transformation of Companies House is not yet complete. The agency will continue to implement its new identity verification regime, roll out its digital filing infrastructure and expand its intelligence-sharing arrangements. The transformation of Companies House represents a significant evolution in the UK's corporate governance framework. No longer a passive registrar of information, it is now a pro-active, risk-focused regulator at the centre of the UK's effort to detect and prevent economic crime.

Through new powers, enhanced capabilities, inter-agency collaborations and early enforcement action, it is beginning to make a measurable impact on corporate integrity across the UK.



DESIGNING CONTROLS WITH BEHAVIOUR IN MIND: *ADDRESSING INSIDER FRAUD IN THE PUBLIC SECTOR*



**DR RASHA KASSEM,
SENIOR LECTURER IN ACCOUNTING &
LEADER OF THE FRAUD RESEARCH
GROUP,
ASTON UNIVERSITY**

Insider fraud is one of the most damaging and underestimated risks in the public sector, often enabled by weak controls but driven by deeper human behaviours like resentment, entitlement, rationalisation, and a lack of oversight. Dr Rasha Kassem explores how public bodies can design fraud controls that consider not just what people do, but why they do it.

Insider fraud presents a growing and often under-recognised threat within the UK public sector, where the stakes of trust, transparency, and public accountability are particularly high.

In government departments, local authorities, NHS bodies, and publicly funded organisations, insider fraud occurs when individuals entrusted with public responsibility, including civil servants, local government officers, finance staff, procurement teams, or senior managers, exploit their positions to deceive the organisation for personal benefit or to advantage others.



These personal benefits may be financial, such as falsifying expense claims for personal reimbursement, diverting public funds to personal accounts or fictitious suppliers, or manipulating procurement processes to award contracts to associates or entities offering bribes.

They may also be non-financial, including gaining unauthorised access to confidential data to benefit the dear and near (e.g., friends, family, or accomplices), abusing their position by interfering in regulatory or disciplinary processes to protect themselves or close colleagues from scrutiny, securing employment or promotions for relatives or friends through nepotism, or influencing decision-making for ideological or political motives rather than objective public interest.

Some perpetrators rationalise their actions, believing they are acting in the organisation's interest rather than for personal gain, for example, protecting jobs or preserving reputation — despite knowingly breaching ethical or legal boundaries.¹

In all cases, insider fraud is uniquely damaging because the threat comes from within and undermines public trust, weakens service delivery, and can have long-lasting reputational and financial consequences for public bodies. According to the Association of Certified Fraud Examiners' (ACFE) 2024 Global Fraud Report, insider fraud contributed to over \$3.1 billion in global losses, with organisations losing an estimated 5% of their annual revenue to fraud.² Recent Cifas data revealed a 14% rise in insider threat reported in 2023, with nearly half involving dishonest conduct by employees.

Alarmingly, 38% of those involved had been in post for less than a year, while 17% had held their positions for over a decade—showing that insider fraud can emerge at any stage of employment³. These threats now account for almost 30% of security breaches in the public sector, often involving misuse of sensitive data and manipulation of operational processes.⁴

Real-world cases underscore the damage insider fraud can cause. In 2024, Michael Paterson, a council tax team leader at Aberdeen City Council, was convicted of embezzling more than £1 million in public funds over a 17-year period. He manipulated his authority to process tax refunds, diverting hundreds of payments into his own accounts with no oversight.

The fraud persisted for nearly two decades due to critical control failures, including the absence of segregation of duties and passive enforcement of procedural safeguards. It was eventually uncovered when a colleague noticed an unusually large refund, prompting an internal review.

While Paterson did not reveal his motive, the longevity and sophistication of the scheme point to a calculated pursuit of personal gain, enabled by a perceived low risk of detection. The Accounts Commission described the case as a “cautionary tale” highlighting the dangers of relying on written controls without meaningful oversight or challenge.⁵

In 2024/25, a series of internal fraud cases within the Department for Work and Pensions (DWP) resulted in the loss of approximately £1.7 million in public funds. Investigations revealed that several civil servants exploited their access to benefit systems by manipulating identity verification procedures and approving claims without sufficient documentation or eligibility checks.



Insider fraud presents a growing and often under-recognised threat within the UK public sector, where the stakes of trust, transparency, and public accountability are particularly high.

In one instance, a staff member authorised multiple fraudulent payments despite the absence of supporting evidence. These cases illustrate how access to sensitive systems, coupled with weak internal scrutiny, created clear opportunities for abuse. The lack of real-time oversight and reliance on trust over verification enabled individuals to bypass standard procedures for personal gain.

While formal motives were not disclosed, the nature of the fraud suggests a mix of opportunism and rationalisation. Some individuals may have been driven by financial pressures, while others likely viewed the system's weaknesses as a low-risk opportunity to exploit. The relatively modest scale of individual offences, combined with the volume of cases, points to a broader cultural problem where systemic gaps in monitoring and control created a permissive environment for misconduct.

Former pensions minister Baroness Altmann described the behaviour as “shocking” reinforcing the need for stronger enforcement, cultural change, and mechanisms that both deter fraud and detect it early.⁶

In a separate case concluded in May 2025, Dean Armitage, a ward manager at a mental health unit in Bradford, was sentenced to 18 months in prison for fraud by abuse of position.

Between April 2020 and October 2021, he falsified and backdated 185 overtime shifts, fraudulently claiming over £72,000 in salary and holiday pay. Armitage used his position to both author and approve these claims, circumventing basic verification procedures.

Although no motive was formally identified, the timing during the height of the COVID-19 pandemic suggests opportunism, potentially driven by burnout, entitlement, or financial strain. The case exposed weaknesses in oversight during crisis periods and demonstrated how short-term insider fraud can flourish in high-trust environments lacking active controls and routine scrutiny. These cases underscore how insider fraud within the public sector can take both sophisticated and opportunistic forms, highlighting the critical need for robust internal controls, credential checks, and proactive fraud detection mechanisms.⁷

Insider fraud is not a singular offence but a broad category encompassing asset misappropriation, financial reporting fraud, and corruption. These include theft of cash or physical assets, falsification of financial records, and abuse of power for personal gain through bribery, nepotism, or conflicts of interest. Despite their variety, such acts are unified by an insider's exploitation of their trusted role, often facilitated by gaps in internal controls or inadequate oversight.⁸ While weak controls are often the primary enabler, insider fraud ultimately stems from human behaviour.



Even with advances in technology and concerns about AI-facilitated misconduct, the root cause remains human—whether through prompting, programming, or collusion. To build meaningful defences, public bodies must design controls that address not only procedural gaps but also the psychological and behavioural dimensions of fraud. Academic literature identifies five key behavioural factors that influence insider fraud: motive, opportunity, rationalisation, integrity, and capability.⁹ These form the basis of a behavioural risk lens that can strengthen control frameworks.

Motives are the personal drivers behind fraud, including financial need, greed, or non-financial triggers such as revenge, ego, or ideology. Opportunities arise when weak controls, poor oversight, or inadequate segregation of duties allow misconduct to go undetected. Rationalisation enables individuals to justify unethical actions—for instance, by claiming they are "borrowing" funds or "helping the organisation." Integrity refers to the moral character of individuals, and those with higher integrity are more likely to resist temptation.

Capability relates to the confidence, access, and skillset that allow certain individuals to commit fraud more effectively than others. This may include positional authority within the organisation, insider knowledge of accounting systems and control weaknesses, and a belief that they can evade detection or face minimal consequences even if exposed.¹⁰

To effectively reduce the motive to commit fraud, public bodies must address the human and emotional drivers that often underpin dishonest behaviour. While constrained pay is a reality in many parts of the public sector, transparency and fairness in pay structures can help minimise feelings of inequality or resentment. Equally important is ensuring fair access to promotion and career development.

When staff feel overlooked, undervalued, or perceive advancement to be based on favouritism rather than merit, frustration can build and, in some cases, be rationalised as justification for fraud.

Many instances of insider fraud are not motivated solely by financial gain, but by a sense of grievance or perceived injustice (e.g., where individuals feel mistreated, ignored, or disrespected). Treating employees fairly and with respect at every level through consistent management, transparent promotion processes, and serious handling of grievances helps reduce these revenge-based motives.


Involving staff in decisions that affect their roles and ensuring they feel heard can also prevent the kind of disengagement that fuels unethical behaviour. Providing access to employee assistance programmes, financial counselling, and mental health support can ease personal pressures that might otherwise lead to misconduct. Recognising ethical behaviour through praise, internal awards, or career development opportunities further reinforces a culture where integrity is both expected and rewarded. When staff feel respected, supported, and able to progress on merit, they are far less likely to justify fraud as a form of redress or survival. In this way, cultivating trust, fairness, and a sense of shared purpose becomes not only good organisational practice, but a powerful deterrent to fraud.

Reducing opportunities for fraud requires strong segregation of duties, even in small teams. Where staffing is limited, workarounds such as rotating responsibilities or peer reviews can serve as effective substitutes. Regular audits, including unannounced spot checks, and strict role-based access controls further limit the chances of fraud. The use of surveillance, data analytics tools, and fraud awareness training during onboarding and induction can enhance vigilance across the organisation. These measures should be supported by clear, well-communicated policies and procedures, particularly in high-risk areas such as finance, procurement, and recruitment, to eliminate ambiguity and close potential loopholes.

Monitoring and safeguarding physical and digital assets, including accurate inventory management and secure storage of sensitive records, are critical in preventing misuse or unauthorised access. Robust IT controls, including multi-factor authentication, system audit trails, and access reviews are essential, alongside regular data protection training to ensure staff understand their responsibilities in handling sensitive information.

Mandatory leave policies for employees in key roles can reveal suspicious activity during their absence, while exit procedures, such as prompt deactivation of accounts and review of recent activity help prevent last-minute misconduct by departing staff. Controls over system overrides, manual adjustments, and supplier relationships, like due diligence, conflict of interest declarations, and monitoring of payment patterns further reduce vulnerabilities.

Anonymous reporting channels empower staff to raise concerns early, even where direct oversight is limited. Crucially, fraud prevention must be underpinned by a clear framework of accountability, where consequences for fraud are consistently applied. This includes not only disciplinary action but, where appropriate, referral for criminal prosecution rather than quiet dismissal. Embedding fraud risks into organisational risk registers and ensuring senior oversight reinforces the message that fraud is a serious breach of public trust with real consequences.



Controls must address not only procedural gaps but also the psychological and behavioural dimensions of fraud

To challenge rationalisation, public bodies must embed a strong ethical culture as those with low integrity tend to rationalise their unethical behaviour. Codes of conduct should be regularly communicated and linked to real-world scenarios. Ethics training should go beyond legal compliance to include practical dilemmas in procurement or service delivery.

Consistent enforcement of ethical standards across all levels of staff reinforces accountability and discourages self-justifying behaviour. Promoting integrity starts with recruitment. Pre-employment checks and reference verification are essential, particularly for roles involving access to sensitive data or finances.

New employees should be asked to acknowledge the organisation's code of conduct during onboarding, with regular reaffirmations. Ethical performance can be reflected in appraisals, and whistle-blower protections aligned with the Public Interest Disclosure Act must be visibly upheld to ensure concerns can be raised safely.

Managing capabilities involves limiting the power of individuals to override controls. Dual approval processes, audit trails, and regular reviews of system access are critical. Managers should be trained to recognise behavioural red flags and understand how control frameworks apply in practice. Regular audits should assess not only compliance, but also how well fraud prevention mechanisms are embedded into daily operations. Ultimately, insider fraud is rarely just a failure of process; it is often the result of psychological drivers such as resentment, rationalisation, entitlement, or perceived injustice. Effective prevention must therefore incorporate insights into why individuals choose to betray organisational trust.

By embedding behavioural risk into the design of fraud control frameworks considering not only what people can do, but why they do it, public bodies can build more targeted, realistic, and resilient defences. This human-centred approach strengthens accountability, supports ethical culture, safeguards public funds, and ultimately reinforces trust in the institutions that serve society.



WHY A FRAUD CONTROL APPRENTICESHIP?



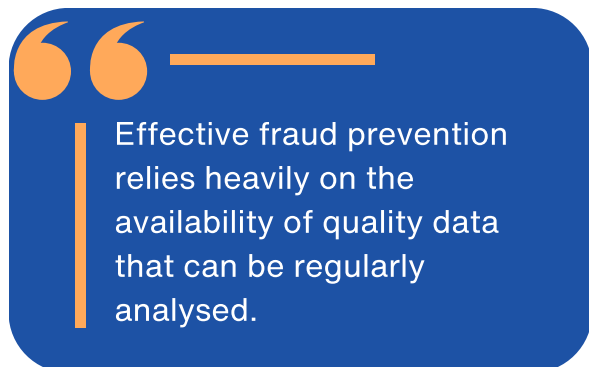
MICHAEL BETTS,
*HEAD OF CENTRE OF LEARNING,
GOVERNMENT COUNTER FRAUD
PROFESSION*

With fraud costing the UK economy an estimated £220 billion annually, the article contends for a proactive, prevention-first approach to economic crime. The authors introduce the new Public Sector Fraud Model and make the case for a multidisciplinary Level 4 Fraud Control Apprenticeship, designed to build specialist capability in prevention, detection, and risk management across organisations. By embedding fraud control as a core function, public bodies can better protect public funds and strengthen corporate governance.



DR. MICHAEL GILBERT,
*MEMBER OF THE PSFA EXPERT
TALENT POOL*

Fraud is an increasingly significant issue across all sectors of the UK economy.¹ According to the Office for National Statistics, approximately 4.2 million frauds occurred in the year ended March 2025. Consequential losses are significant; with the latest Annual Fraud Indicator, published in 2023, estimating that this was costing the UK economy around £220 billion² per year. Alarmingly, law enforcement allocates only about 2%³ of their resources to combat this problem, leading to less than 5% of reported frauds being investigated, and a judicial outcome rate of under 1%.⁴



Effective fraud prevention relies heavily on the availability of quality data that can be regularly analysed.

Given these troubling statistics, it is evident that organisations throughout the United Kingdom cannot rely solely on investigative methods to address fraud-related issues, particularly when many lack the necessary investigative powers. Therefore, it is essential to implement proactive strategies to prevent fraud and to detect it at an early stage, enabling swift intervention to minimise losses.

In 1736, Benjamin Franklin famously advised the residents of fire-threatened Philadelphia that "an ounce of prevention is worth a pound of cure." Similarly, the prevention of fraud, bribery, and corruption should be a primary focus for the counter-fraud profession as it moves forward, particularly by harnessing technology and artificial intelligence. Just as the fire service and public health responses are increasingly prioritising prevention, so too must the counter-fraud sector adopt a proactive approach to mitigate risks effectively.

This leads to a crucial question: what constitutes a proportionate response to the fraud threats facing organisations, and how much should they invest in their counter-fraud services? Determining this requires organisations to conduct thorough fraud risk

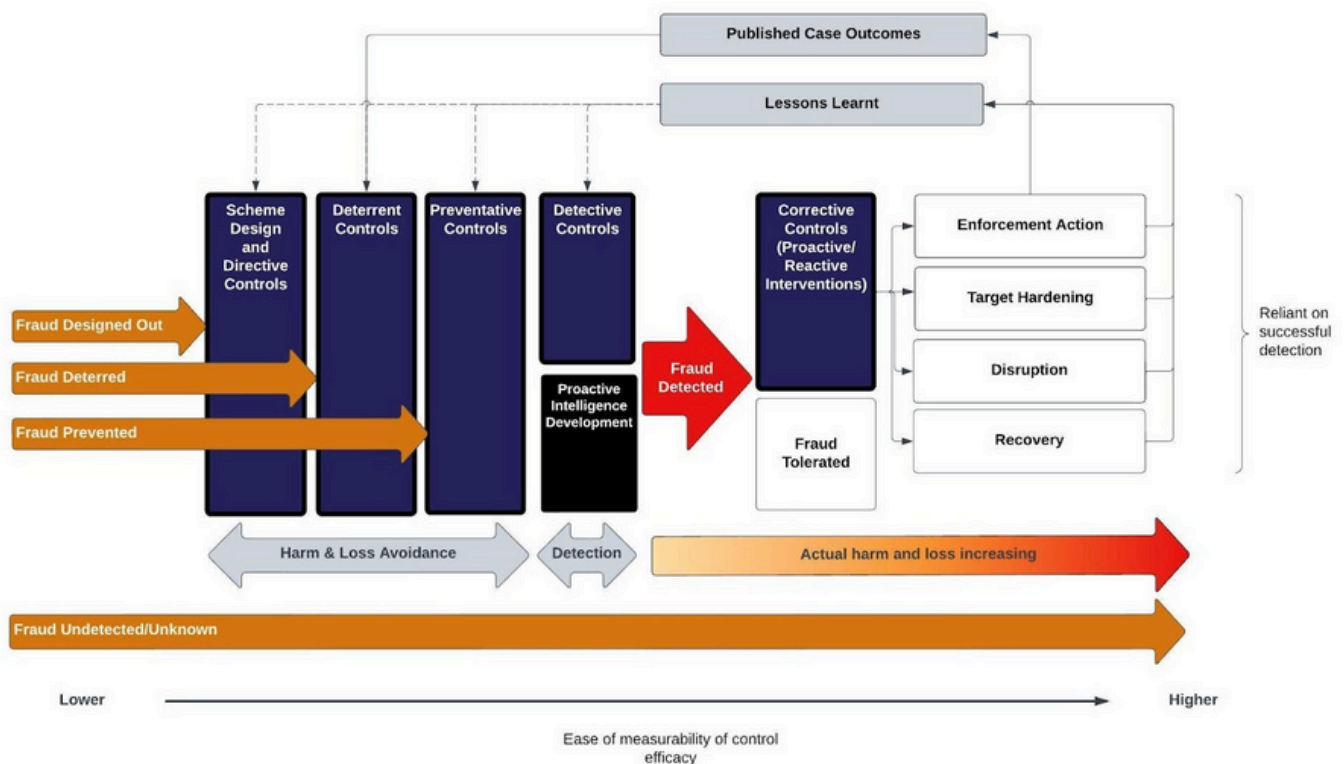
assessments to understand their potential losses associated with fraud. Consequently, integrating fraud risk management and loss measurement into organisational governance arrangements becomes paramount.

Effective fraud prevention relies heavily on the availability of quality data that can be regularly analysed. Without accurate data, organisations will struggle to identify and mitigate both current and emerging fraud threats effectively. Furthermore, safeguarding systems, procedures, and data against both internal and external threats necessitates robust cybersecurity measures.

The newly introduced '**Public Sector Fraud Model**' (Freeman/Betts, 2024) presented in the figure below, offers a comprehensive framework outlining the essential measures that an organisation should implement to establish a robust defence and response system against fraud, bribery, and corruption.

This model emphasises the importance of incorporating directive controls, such as embedding counter-fraud policies and procedures into scheme design, with the aim of preventing fraud from the conceptual stage. It also advocates for a variety of deterrent controls intended to discourage fraudulent activity, for example emphasising that fraudsters will face prosecution.

Furthermore, the model highlights the need for preventative measures, for example including split delegations



The New Public Sector Fraud Model (Freeman/Betts 2024)

across commercial, technical, and financial areas. Following this, it addresses the need for detective controls and outlines the appropriate responses should fraud be detected. Overall, this model encapsulates the critical components that constitute the cluster of activities known as 'Fraud Control'.

To tackle fraud and economic crime effectively, a multi-disciplinary approach is crucial. Counter-fraud teams must include personnel with varied expertise who can leverage these disciplines effectively, ensuring a cohesive and synergistic response. This expanded focus on fraud management beyond mere prevention, detection, and investigation, highlights the need for Fraud Control Specialists. The Fraud Control Specialist role is one of five membership categories within the Government Counter Fraud Profession (GCFP). The GCFP has

established five key standards to support the Fraud Control framework, which is regarded as a distinct cluster within the Profession. These standards address critical areas including **Fraud Prevention, Fraud Detection, Fraud Risk Assessment, Fraud Loss Measurement**, and the promotion of a **Counter Fraud Culture**.

If we accept the premise that organisations require Fraud Control Specialists to manage fraud risks and losses effectively, it is necessary to implement processes and pathways that support organisations in achieving this goal. While this represents a new methodology for fraud management, the complexity and scale of the issue demand innovative solutions.

Consequently, the Public Sector Fraud Authority has been working with Skills for England to introduce a multi-

disciplinary 2 year Level 4
Apprenticeship in Fraud Control.

Blending academic study and practical experience, this apprenticeship will equip the next generation of counter fraud specialists with the skills needed to: measure current fraud loss, and decide upon what is a proportionate response to it; and, identify and implement appropriate deterrent, preventative and detective measures that will drive this down and minimise future fraud loss. In doing so, it will make a successful contribution to an organisation's internal control framework - thereby leading to more effective corporate governance.

Many organisations may already have established investigative capabilities to supervise and mentor investigative apprentices. However, similar structures are often lacking in fraud control contexts. This void should not deter the establishment of new initiatives, especially given the substantial potential benefits. An interim solution is essential until fraud control becomes widely embedded within organisations.

It is likely that public sector organisations and larger private and voluntary sector employers, particularly those impacted by section 199 of the Economic Crime and Transparency Act 2023, a failure to prevent economic crime offence, should be early adopters of the Fraud Control Apprenticeship.



This apprenticeship will equip the next generation of counter fraud specialists with the skills needed to measure fraud loss and drive it down.

These entities typically possess established Cyber and Digital Teams, Risk Management Teams, and other relevant personnel who can actively contribute to fraud management through processes such as supplier due diligence and employee pre-employment screening.

While expertise may not be concentrated within a single team, larger organisations are likely to have the requisite knowledge distributed across various departments to supervise and develop Fraud Control Apprentices. Consequently, each Fraud Control Apprentice will need an appointed supervisor with the appropriate authority within the organisation, capable of coordinating the mentoring of apprentices across these different areas. This supervisor will play a crucial role in monitoring the apprentices' training journey, ensuring they gain a diverse array of experiences.

We anticipate that the relationship between employers and training providers for the Fraud Control Apprenticeship will mirror that of existing apprenticeship models, fostering collaboration that ultimately culminates in a more skilled and effective workforce in the fight against fraud.

In conclusion, a Fraud Control Apprenticeship represents a vital step in addressing the significant and growing issue of fraud across the United Kingdom. By cultivating a new generation of Fraud Control Specialists, organisations will be better equipped to manage fraud risks proactively, thus enhancing their ability to safeguard both their resources and the public interest.



WHY FRAUD IS A GLOBAL BUSINESS OPPORTUNITY FOR ORGANISED CRIME GANGS (OCGS)

Laura Eshelby explores how fraud has become a global business for organised crime groups, fuelled by AI, crypto, and international networks. With the rise of fraud factories and large-scale laundering operations, she calls for urgent, coordinated action to disrupt these threats and protect all victims, including those trafficked to commit the crimes.

I recently had the opportunity to present at the 14th Annual Counter Fraud, Cybercrime and Forensic Accounting Conference at the University of Portsmouth. The topic I explored was how fraud has evolved into a global business opportunity for organised criminals - and the considerable challenges this presents for disruption and prevention efforts. Below is an exploration of this live and troubling global issue.

The scale of the challenge

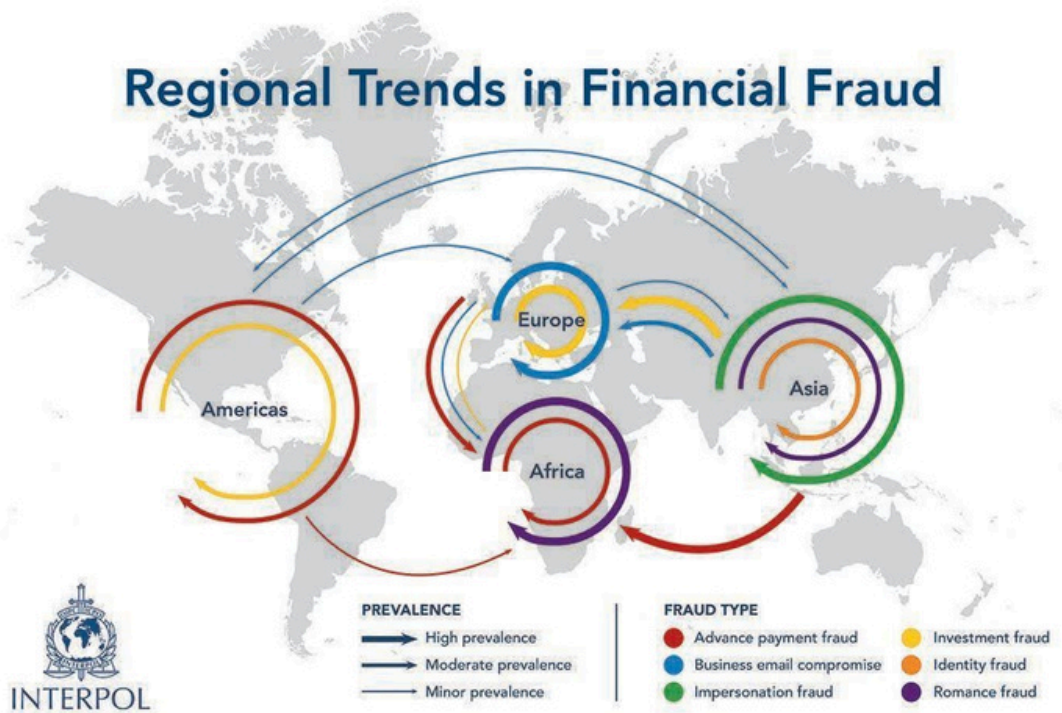
Fraud now accounts for 43% of all crime in the UK, with 1 in 14 adults falling victim (Office of National Statistics¹). Of the frauds reported, 70% have an international element (City of London Police²), with total



**LAURA ESHELBY,
HEAD OF ECONOMIC CRIME,
CLUE SOFTWARE**

annual losses estimated at £219bn across all sectors (Crowe³), including £55bn in the public sector alone (NAO⁴).

On a global scale, the Global Anti-Scam Alliance (GASA) estimates losses could exceed \$1 trillion, with half the world encountering fraud weekly.



Regional trends in financial fraud. Credit: INTERPOL

These figures may still be underestimated - 70% of global victims and 86% of UK victims are believed not to report fraud, often due to shame, embarrassment, or a belief that little will be done in response.⁵

Regional trends in fraud

According to Interpol⁶, fraud patterns vary by region. In Europe, business email compromise and investment fraud dominate, while in Africa, romance scams and advance-fee frauds are more prevalent. Interpol has referred to the situation as an 'epidemic', pointing to rapid technological change and the industrial scale of organised crime operations. Criminals increasingly leverage AI to enhance fraudulent activity, and use cryptocurrencies to move illicit proceeds globally, complicating law enforcement efforts.⁷

The rise of fraud factories

One of the most striking illustrations of organised criminality is the emergence of global fraud factories - highly structured criminal operations functioning like corporations. These are often staffed by trafficked individuals who believed they were applying for legitimate jobs in marketing or IT but were instead taken to compounds across Southeast Asia.

Since the COVID-19 pandemic the traditional money laundering routes (e.g., casinos) have been disrupted and criminals have shifted focus. It's estimated that over 220,000 people are being held in "fraud compounds" in Asia, with global losses exceeding \$75bn between 2022 and 2024.

These factories train individuals to run romance and investment scams targeting victims across the USA, UK,

Europe, and China. Interpol and the UN On Drugs and Crime (UNODC⁸) report strong links between these activities and other organised crimes such as human trafficking and narcotics.

The latest reports from agencies, such as Interpol, also offer insights into the shift in global presence of these factories, and the facilitators behind them. Scam or fraud factories have increasingly been observed beyond Asia where they started, to other regions including the Middle East and West Africa. It's estimated that 90% of human trafficking facilitators are from Asia, 11% South America or Africa. In terms of gender, 80% are male and predominantly aged 20-39 years (61%, Interpol).

The staffing of such fraud factories is mostly through false job opportunities, applicants are then trafficked to perform social engineering activity. They are subjected to torture, sexual exploitation and extortion via debt bondage and kept against their will. The victims of the socially engineered fraud, whether romance, investment or other methods deployed, will then be left with emotional and financial damage. This demonstrates the layers of victims involved, such as those there due to false advertising, as well as those defrauded, in these complex and organised criminal centres.

“The reach of online scam centres spans the globe and represents a dynamic and persistent global challenge”.
Cyril Gout, Interpol

Since 2023, Interpol has documented the trend of this criminal activity and issued orange notices to signal the imminent and serious threat posed to public safety. The work since then, by Interpol and other agencies to disrupt where possible the factories and organised crime groups, has produced evidence to show that the routes used to traffic victims to fraud factories, are then used to also traffic drugs, firearms and even protected wildlife species. Interpol acting Director of Police Cyril Gout commented, “The reach of online scam centres spans the globe and represents a dynamic and persistent global challenge”.



Organised threat in the UK

The UK is not immune to this sophisticated threat landscape. For example, Operation Destabilise, led by the National Crime Agency (NCA) and international partners, disrupted a global money laundering network that used crypto assets to facilitate luxury lifestyles for sanctioned individuals. The international investigation uncovered a money laundering ring with links to organised criminals in the UK, drug cartels in South America, and sanction avoidance. The criminal activity involved collection of cash proceeds from street level drug deals

and exchanging it for cryptocurrency, which was then used by the gangs to purchase drugs and firearms. The crypto currency used may also have originated from crime, such as ransomware, enabling the criminals to exchange the proceeds of crime for cash.

The scale of the laundering in Operation Destabilise was vast with reports of £12m being laundered in 74 days. The groups used the funds to offer services to sanctioned oligarchs, Russian elites, ransomware operators and organised crime groups.

The Royal United Services Institute (RUSI) have in their research commented on the clear links between organised crime, sanctions evasion and hostile state activity.

In their commentary of Operation Destabilise specifically, they highlighted the links to state threats, with reports that funds laundered were used to conduct Russian espionage activity in Europe and to further the spread of Russian misinformation and disinformation. This is backed up by the Director of General Operations for the NCA, Rob Jones, who commented, *“for the first time we have been able to map out a link between Russian elites, crypto rich cyber criminals and drugs gangs on the streets of the UK”*.

International law enforcement partners working alongside the NCA to dismantle the criminality included agencies from Ireland, France, the US and UAE.

The results were significant:

- 84 arrests including 71 in the UK
- 6 individuals and companies sanctioned
- £700m in assets seized
- £200m in crypto assets recovered

This and other operations led by the NCA and law enforcement agencies across the UK, demonstrate the corporate structure of organised crime, with UK links to multi-national syndicates conducting phishing, trafficking, and large-scale fraud.



Fighting back with technology and collaboration

To counter these threats, we must match criminals in their use of technology and innovation. This includes:

- **AI-powered analytics** to detect anomalies in financial systems
- **Cross-jurisdictional intelligence sharing**
- **Data-driven resource prioritisation**

Successful disruption efforts, such as those by Interpol, the NCA and others, underscore the importance of partnerships between law enforcement, industry, and government. Equally critical is the protection of trafficked workers in fraud compounds, some of whom are victims themselves. Support services and, where possible, rehabilitation efforts must be prioritised, despite the complexities posed by varying legal systems and approaches to justice.

Conclusion

Fraud remains the most widespread crime in the UK, and it's growing in both complexity and scale globally. The United Nations Office on Drugs and Crime (UNODC) have sought to highlight the professional and agile approach taken by criminals, with rapidly expanding cyber operations and using illicit marketplaces to traffic victims to further their criminality. Law enforcement and intelligence agencies need continued support from government, industry, and technology providers to remain agile and effective. It is recognised how the convergence of technologies and other major crimes could further transform and grow global fraud centres as this trend continues. This includes the use of AI, being harnessed to execute fraud by criminals.



Law enforcement and intelligence agencies need continued support from government, industry, and technology providers to remain agile and effective.

Meanwhile, technology and social media platforms must take greater responsibility to remove fraudulent content - whether false job adverts, bogus investment schemes, or crypto scams. To enable success in this aim, continued intelligence sharing is key to prioritise and target the highest harm areas and most serious and organised perpetrators. The acting Executive Director of Police Services at Interpol summarised the need for coordinated action, stating, "Tackling this rapidly globalising threat requires a coordinated international response. We must increase the exchange of information between law enforcement in the growing number of countries affected and strengthen partnerships with NGOs that help victims and technology companies whose platforms are being exploited". With corruption reaching state levels in some regions, coordinated, multinational pressure is more essential than ever. Only by working together - with the right tools and intelligence - can we turn the tide on this global business of fraud.

STAMMERING AND FRAUD - *CONFLICTS BETWEEN FRAUD DETECTION CONTROLS AND CUSTOMERS WHO STAMMER*



**CLAIRE MAILLET,
CERTIFIED FRAUD EXAMINER,
FELLOW OF THE INSTITUTE OF
LEADERSHIP**

**Imagine st... st... starting a sentence,
nnnnnot knowing if you're going to f-f-
finish it.**

Then imagine being in a situation where you must respond to this question: "I'm going to ask you a few security questions..."

'Stammering' and 'fraud' are words that are rarely featured in the same sentence - unless you're on my LinkedIn profile. The overlap between these two topics has been the focus of my most recent keynote presentation which I've had the pleasure of delivering across the country in recent months.

In this article, Claire Maillet explores how common fraud detection practices can disadvantage customers who stammer, and what organisations must do to balance security with accessibility. From voice recognition to biometric checks, systems need to be redesigned with empathy, inclusion, and legal duty in mind.

Whilst a very niche subject, it is essential for organisations to understand not only disability in more detail and how it can impact its customers, but also how customers will respond to various anti-financial crime controls.

For people who stammer, passing through a company's identity verification process can be unexpectedly stressful. Many individuals with speech disorders find themselves unintentionally flagged by fraud detection systems - not because they're suspicious, but because the strategies they use to manage or hide their stammer can appear inconsistent or unusual to automated or scripted systems.

As a counter-fraud professional who stammers, I've encountered this first-hand. I've failed security checks - not due to incorrect answers, but because my speech didn't conform to the expected pace or delivery. What seems like a straightforward process for most can become a barrier for those with a speech disorder.

Organisations face a critical challenge: how to maintain strong fraud prevention measures without excluding or penalising legitimate customers, particularly those with disabilities. Compliance with equality and accessibility laws is not just a legal obligation - it's a customer care imperative. But beyond compliance, we must also ensure that people with disabilities, visible or hidden, have a dignified and fair experience when accessing products and services.

Stammering is often written about in the media as a condition that needs to be treated or "cured", or worse still, a source of comedy. Reflected in popular culture and the media, for example Porky Pig (*Looney Tunes*), Ken Pile (*A Fish Called Wanda*), Albert Arkwright (*Open All Hours*), Jim Trott (*The Vicar of Dibley*) and Professor Quirrell (*Harry Potter and the Philosopher's Stone*).

There are many myths and misconceptions associated with stammering, including that it's caused by bad parenting or anxiety and that it's contagious. Moreover, people who stammer are often considered less intelligent than fluent speakers and shy or nervous. These are misconceptions, but for someone who stammers, a



I've failed security checks— not because I gave the wrong answers, but because my speech didn't conform to the expected pace or delivery.

fraught experience trying to use products or services can reinforce many of the negative emotions that people who stammer often have in public interactions like embarrassment, anger, frustration, shame, and panic because of their disability. According to the World Health Organization (WHO), an estimated 1.3 billion people, 16% of the world's population, live with some sort of disability¹. In the U.K., there are approximately 16 million people with disabilities, accounting for 24% of its population².

Of those estimated 1.3 billion disabled people worldwide, it's estimated that nearly 80% are living with a "hidden" disability, one that might not be readily obvious to others. These disabilities include neurological, cognitive and neurodevelopmental disabilities as well as physical, visual, auditory, and sensory and processing difficulties. Diseases and chronic conditions such as asthma and diabetes also fall under the hidden disability umbrella. Stammering (or stuttering) is also considered a hidden disability. Globally, it's estimated that 1% of the adult population stammers. Consider this: If your organisation has an international customer base of one million people,

you could have 10,000 customers who stammer.

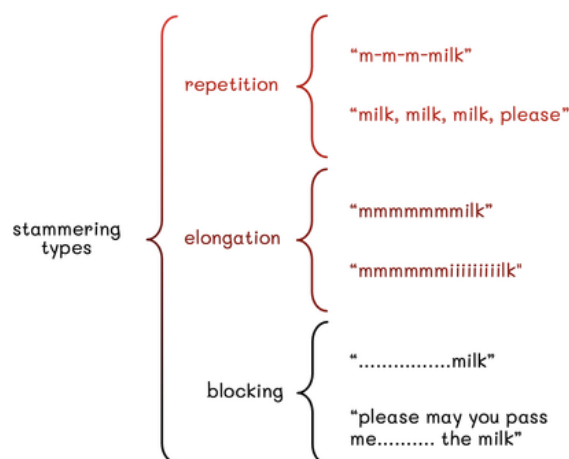
In recent years, scientists have begun to understand stammering as a neurological condition in which connections between the left and right side of the brain and the connections between hearing and speaking are weak, resulting in dysfluent speech.³ According to the National Health Service, most stammering is developmental, starting in childhood, disappearing in adulthood. Although rare, people can develop a stammer later in life, usually due to a head injury or stroke.

Stammering can either be overt or covert; someone who's a covert will go to great lengths to conceal their stammer by substituting words or avoiding situations in which they might stammer. The nature of stammering can change over time, and it can occur with only certain sounds or words, or randomly, and this too can change over time.

Using filler words such as "um" or "er" often help people launch into pronouncing words that tend to be more difficult for them. Stammering presents itself in three different ways: through elongation of words, repeating letters and words, and blocking (pauses in speech):



Fraud detection shouldn't come at the cost of accessibility.



People who stutter often display secondary behaviours, including:

- Physical tension in the jaw or anywhere else on the body.
- Facial grimacing.
- Movement of a body part such as the hand or foot.
- Avoiding eye contact or turning away.
- Using fillers (e.g. "um", "er") to help launch into words.

Stammering often leads to feelings of shame and embarrassment; displaying these secondary behaviours can compound those feelings.

Operational Impact - Onboarding

When a customer begins your organisation's onboarding process or tries to access one of your applications, they typically must pass an identity verification check. This often includes tasks like repeating a set of numbers displayed on screen or reciting a sentence such as, *"Hi, I'm Claire and I'd like to open an account."* For most, this is a simple and seamless process. But for individuals who stammer, it can be anything but.



People who stammer are often excluded by systems never designed with them in mind

Take, for example, biometric verification. People who stammer often avert their gaze, close their eyes, or look away during moments of speech difficulty - behaviours that can interfere with facial recognition technology. After contacting four biometric verification providers, I learned that iris and retina features account for 10% to 20% of facial scan weighting, meaning open eyes are essential for the scan to succeed. If a user looks away or cannot complete the spoken prompt, the system may repeatedly prompt them to retry and ultimately resulting in verification failure.

Operational Impact - Ongoing Monitoring

In my early days as a counter-fraud professional, I was taught that one of the most effective protective steps is to contact a customer directly to verify their account activity. This typically involves a series of security questions to confirm identity. If a caller fails to answer with immediate confidence and clarity, fraud teams are trained to treat it as a red flag, often resulting in blocked transactions and restricted accounts.

For individuals who stammer, particularly covert stammerers who

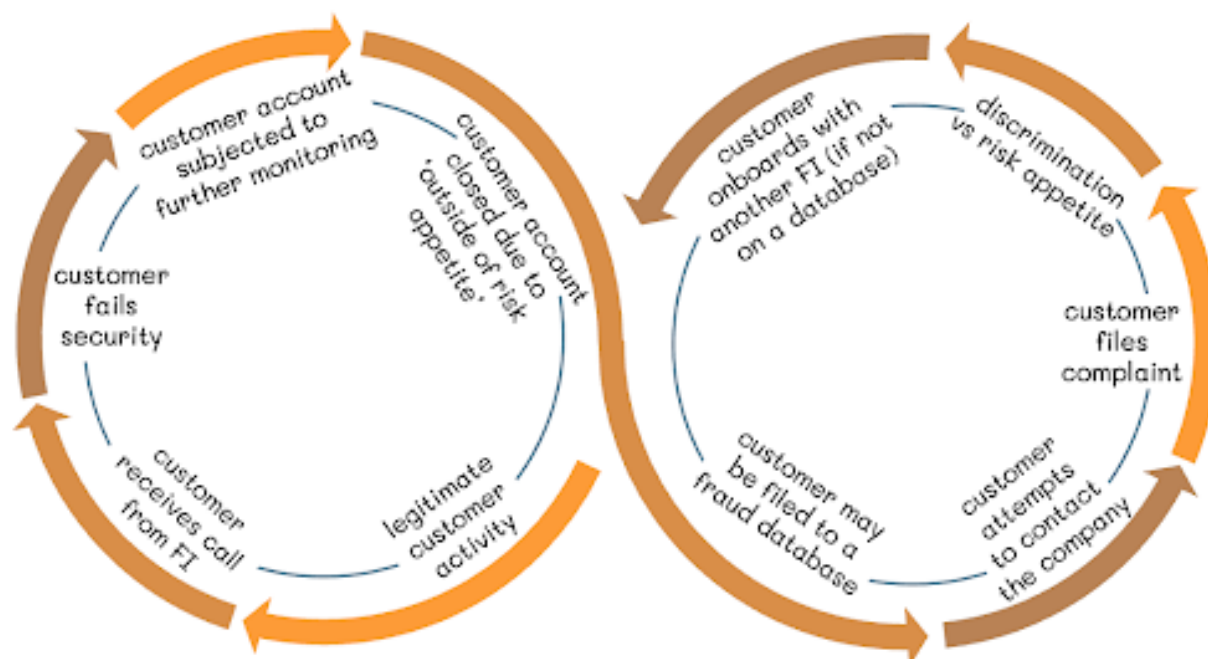
rely on word substitution to manage speech, this presents a major hurdle. Security questions usually require exact answers: full name, date of birth, address, payment method, and recent transaction details. These answers cannot be paraphrased or substituted. As a result, the pressure of needing to give precise responses increases the likelihood of blocking or dysfluency during the call.

In my own experience, I believe I've failed phone-based security checks at multiple financial institutions due to prolonged pauses before answering, an effect of stammering, not deception. Yet according to research from the American Psychological Association, people are perceived as less sincere and credible when they pause before replying to a question.⁴

Voice Recognition and AI: A Double-Edged Sword

Voice recognition software is another technology that often excludes people who stammer. While effective for fluent speakers, these systems are generally not trained on dysfluent speech and struggle to recognise or authenticate it accurately.⁵

However, when it comes to artificial intelligence, stammering may offer a surprising layer of protection. In 2023, Microsoft announced that it could replicate someone's voice with just three seconds of audio⁶, raising serious concerns about synthetic voice fraud. But because stammering involves unpredictable pauses and speech blocks, capturing a clean and



consistent audio sample becomes far more difficult. Ironically, this may make people who stammer less vulnerable to voice-cloning scams than fluent speakers.

A Worst-Case Scenario

The image demonstrates a worst-case scenario to show what can happen when an organisation doesn't have a system that balances fraud controls and accessibility for customers and speech disorders. In the worst-case scenario for the customer, they might end up debanked.

Improving Accessibility While Managing Fraud Risk

How can organisations strike a balance between effective fraud prevention and ensuring a positive, accessible experience for customers with speech disorders such as stammering? Below is a step-by-step approach to making security processes more inclusive without compromising protection.

1. Re-evaluate First-line Processes and Training

Start by reviewing all frontline and customer-facing procedures to ensure they do not unintentionally disadvantage individuals with speech disabilities. It's critical that organisations offer multiple channels of communication, such as telephone, email, and live chat, so that customers can choose the method that best suits their needs. A phone-only model may alienate those who stammer, potentially deterring them from engaging with your services.

Ensure your staff have access to clear guidance and training specifically focused on interacting with customers who have speech disorders. Additionally, make support for disabled customers highly visible on your website and within communications, so customers know it exists and how to access it.

2. Provide Targeted Disability Awareness Training

All first-line-of-defence staff, including teams in fraud prevention, customer service, and complaints handling - should receive tailored training on stammering. This training should include practical advice, such as:

- Not hanging up if there's a moment of silence.
- Avoiding interruptions or finishing the customer's sentences.
- Listening patiently and focusing on what the customer is saying, rather than how they say it.

Such practices foster respectful communication and prevent misinterpretation of stammering as suspicious behaviour.

3. Implement Accessible Communication Tools

Consider integrating services like Relay UK or equivalent accessibility platforms, which enable people with speech and hearing difficulties to engage in conversations via text, with the help of an intermediary. These tools enhance accessibility by allowing customers to communicate without the pressure of speaking directly over the phone, all the while maintaining data security and confidentiality.

“Stammering isn't suspicious behaviour—it's human behaviour.”

Inclusion by Design: A Voice at the Table

Technology firms and academic institutions increasingly involve people who stammer in designing and testing accessible tools like collecting voice samples, giving feedback on interfaces, or contributing to user experience studies. Fraud control systems should be no different.

When building or revising fraud policies and training for frontline staff, organisations should actively seek the input of individuals with speech disabilities. This ensures fraud detection efforts are not only legally compliant but also empathetic, inclusive, and reflective of real-world diversity. Including diverse voices at the design table doesn't just meet regulatory expectations - it improves the overall experience for every customer.

TICKET SCAMS: *THE COST OF BEING A FAN?*

As ticket demand surges for concerts, festivals, and live events, so does the risk of fraud. From fake resale listings to phishing scams, fraudsters exploit fan desperation with increasing sophistication. This article explores the fine line between touting and fraud, the emotional toll on victims, the role of enforcement bodies, and the limitations of banks and platforms in protecting consumers.

A few months ago, I logged in to Ticketmaster to get tickets to a festival. While I waited in the interminable queue and got kicked out several times, I searched the festival hashtag and social media. I read the usual array of complaints about queue times, missing out on tickets, software not working under pressure — but amidst all of these, there were posts offering guaranteed tickets for resale. Scam after scam after scam, and most of them were verbatim copies of each other, posted by sock puppet accounts.

The festival is popular every year, and a Facebook group has been set up for buyers and sellers. No doubt some of the 7,000 people in the group are genuine, but messages seeking tickets are frequently replied to by accounts



**AISLING TWOMEY,
SENIOR FINANCIAL CRIME MANAGER,
MONZO BANK LTD.**

saying ‘message me x’ with no other details, pushing people into DMs (Direct Messages) where they might be scammed.

Tickets for the festival are on sale solely through Ticketmaster and when I last checked, transfers aren’t yet available, so anyone claiming to sell tickets has nothing to deliver right now. There’s a strong chance that many of the people seeking tickets and expecting their dreams to come true will instead find themselves down several hundred quid. And that’s just one festival; there are many over the summer period, not to mind the concerts and gigs played by the world’s most popular performers.



I've worked in Financial Crime and Fraud in different banks for over ten years and fraud has become a pervasive, all-encompassing problem, and ticket fraud is a constant.

Customers are upset when banks challenge payments which look like they could be fraudulent and they are also upset when they lose funds to fraud and feel the bank should have done more; it's a hard balance.

Fraud makes people feel ashamed and they may not want to tell the bank the full story, but that full story is critical to helping us work out what happened. That information can eventually lead law enforcement to launch prosecutions.

People may not even realise that they've been a victim, and they pursue a dispute instead of reporting fraud, resulting in a longer process that rightly causes frustration. Ticket fraud sounds simple, but it's far from it.

When does touting become fraud?

Re-selling tickets is not illegal (though in the UK, re-sale of football tickets is), but the market is vulnerable to fraudsters, especially for high profile events.

According to Action Fraud, ticket re-selling becomes fraudulent where the tickets you bought either don't arrive, or turn out to be fake, and a buyer is not refunded.

On top of the ticket fraud, there's an associated phishing fraud. Fraudsters may set up fake ticket websites and collect information from buyers including names, emails, payment information and addresses. This leaves consumers open to being defrauded for tickets but also being further defrauded in the future.



Ticket fraud sounds simple, but it's far from it.

Not Fraud, but...

In 2024, Taylor Swift tickets were listed for resale at over £7000 for a concert at Wembley, 46 times the face value, a price tag that preys on the superfans who feel a deep connection with their favourite performers. If those tickets arrive, it's not fraud, but the desire in us to protect consumers might indicate that it's not *right*.

Many readers will remember the Oasis ticket debacle from last year, in which resale tickets were listed on Viagogo, Stubhub and Gigsberg despite the fact that tickets weren't supposed to be offered on those sites; in October, Ticketmaster cancelled 50,000 tickets sold on unofficial websites, leaving legitimate fans unsure if they'd be refunded, and if they'd be able to secure the tickets a second time. It

feels like we're trying to protect consumers, but it's getting harder instead of easier.

Who's responsible for stopping it?

Trading Standards, the Competition and Markets Authority, the Advertising Standards Authority and the Police all play a role in enforcement when it comes to ticket fraud. In 2024, a family of ticket touts in Norfolk were found guilty of fraudulent trading offences at Leeds Crown Court. They had set up TQ Tickets Ltd and harvested tickets using several illegal methods. They used multiple identities to buy tickets — names, addresses and emails — and used the Insomniac browser (a web browser extension/addon that is designed to prevent websites from putting users' devices to "sleep" or going into idle mode) to purchase many tickets at the same time. They then used fake identities to resell them on secondary ticket sites, and in some instances listed tickets for sale that they didn't own.

While banks aren't enforcers, they often have access to evidence that can support law enforcement efforts to detect crime. For the banks that had TQ Tickets as customers, the ticket scam would have been hard to spot. Banks can see transactions coming in and going out but would have no way of knowing how the tickets had been sold. Fraud reports from victims help to contextualise what banks can see in transaction monitoring processes and are critical to a bank's success in identifying this type of fraud. But in order to get those fraud reports, we need to make sure consumers

understand when touting becomes fraudulent to make those reports, and that they're not ashamed when this happens to them.

Government Action

After the Oasis situation, the government introduced plans to tackle touting, including capping resale markups to 30% over the original asking price, obliging platforms to ensure listing accuracy and updating consumer protection legislation. The plan was put forward for public consultation as well as a call for evidence, both of which closed in April.

Avoid the Scam: Tips for Buying Tickets

Consumers should always be vigilant buying tickets — but high-profile events in the summer season carry the highest risk of fraud. Buyers should only buy tickets from the designated sale points. If buying on the secondary market, consumers should check the T&Cs to make sure they're buying from an authorised one, to save them the disappointment of tickets being voided. Buyers should pay for tickets with a credit card wherever possible, as this may offer some protection in the event something goes wrong.

A research briefing from February 2025 provides a summation of how the ticket re-sale market works, the issues to be solved and how the government plans to achieve its goal of putting "fans back at the heart of events."

If you want to know more about steps you can take to protect yourself when buying tickets, National Trading Standards has a great checklist [on their website](#).

SERIOUS GAMES FOR EXTERNAL FRAUD RISK ANALYSIS AT THE CANADA REVENUE AGENCY



**MADELINE JOHNSON,
SENIOR ANALYST,
FRAUD RED TEAM,
EXTERNAL FRAUD RISK MANAGEMENT
DIVISION, CANADA REVENUE AGENCY
(CANADA)**

An innovative approach for external fraud risk management decision makers can improve their responses and management of external fraud risks by drawing on prior experience and learning from their past mistakes and successes.^{1 2} However, risk practitioners face limits in relying on past experience when trying to stay a step ahead of threat actors who are infinitely creative with their never-ending supply of new schemes. Consequently, effective fraud risk management requires new techniques that will enable risk practitioners to anticipate and manage an unknown present or future.

To stay ahead of ever-evolving fraud threats, the Canada Revenue Agency is using serious games, immersive role-playing exercises that simulate real-world fraud scenarios. These games allow staff to step into the shoes of fraudsters and frontline agents, helping them uncover system vulnerabilities, challenge assumptions, and collaboratively design better risk controls. With 11 games delivered since 2021, this innovative method is helping to predict, prevent, and prepare for fraud risks before they strike.

What if there already were such a technique that could help decision makers gain experience about fraud risks that have not (yet) occurred in real life? This technique exists and it is called serious games.

Serious games are scenario-based, role-playing exercises designed to incorporate the perspective of the opposing side or adversary. Their application has expanded from wargames, which explore problems of armed conflict, to encompass other subjects.³ In the external fraud context, serious games give players a chance to explore any fraud risk or problem, whether real or imagined.

Players are required to create or detect fraud schemes, make decisions to address risks, live the outcomes of their decisions within the game, and finally reflect on the entire experience to apply new insights to their business.



Serious games give players an experience of a real-life situation—without the real-life consequences.

How do serious games work?

In a serious game, players assume actor roles and try to achieve certain goals within their role's abilities. For example (Figure 1), in the Canada Revenue Agency's (CRA) context, some players assume the role of callers (threat actors) who impersonate honest taxpayers, contact the CRA, and try to pass authentication procedures to gain unauthorised access to a tax account.

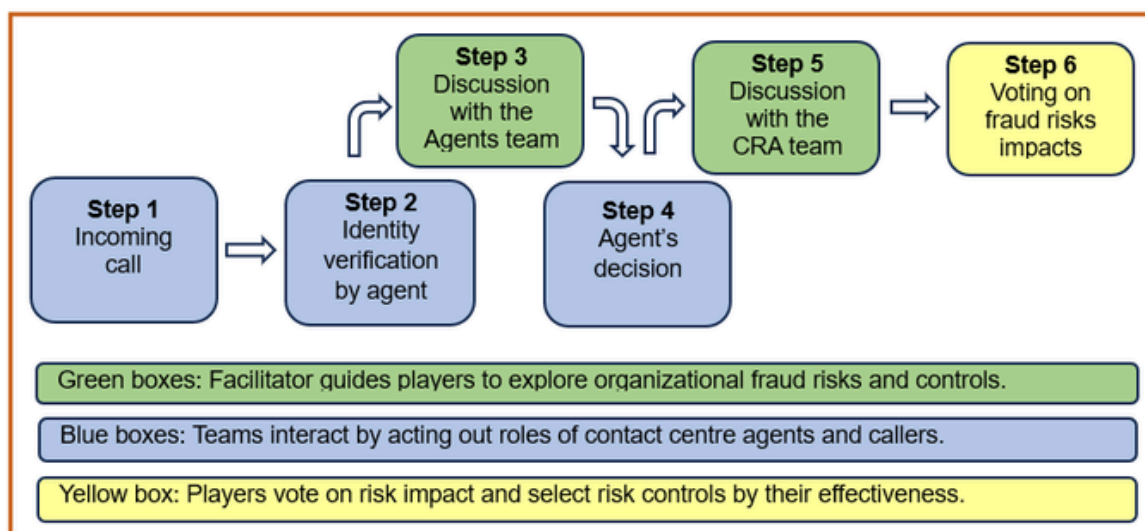
Other players play CRA contact centre agents who try to detect fraudulent callers by following their authentication procedures, which helps them identify vulnerabilities in their business.

Like in entertainment games, such as *Dungeons & Dragons*, players play their roles in an alternate reality responding to a scenario that is

prepared by game designers. Players propose actions and make decisions, either alone or within a team. They justify their decisions and determine whether their action will be successful by taking into account counter arguments from other players and the likelihood of success. As the game continues, players live the outcomes of their decisions but still have the opportunity to modify their approach.

Serious games have a unique ability to address complex challenges such as external fraud threats to public sector organisations. According to Perla and McGrady (2011), when executed well, serious games emulate a “lived” experience that no other method is able to replicate.⁴

Figure 1: Caller authentication game design



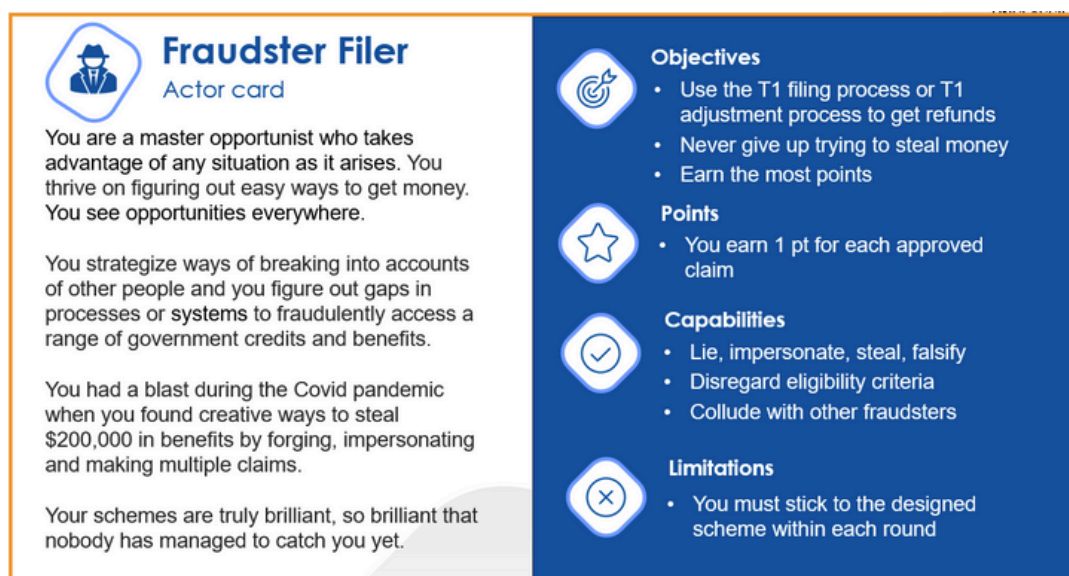


Figure 2: Actor card, fraudster

Traditional methods of assessing and addressing fraud risks, such as reading reports or participating in a discussion require “passive” consideration of ideas, and do not immerse participants in the reality of the situation in quite the same way. Serious games have the power to give players an experience of a real-life situation, but without the real-life consequences.⁵

Serious games at the CRA

The increase in overall fraud trends compelled the CRA to innovate in the realm of external fraud prevention techniques to address them. Since 2021, the CRA has sought to be proactive and preventative against external fraud, especially in trying to anticipate where threat actors may strike next by identifying risks and vulnerabilities in the processes used for administering tax and benefits programmes.

As an example, a recent serious game assessed external fraud risks related to tax refunds issued to individuals and businesses in Canada. Players were

divided into two opposing teams for head-to-head competition. One team assumed the role of tax filers (both honest and fraudsters) who submitted two seemingly identical income tax and benefits returns. Fraudsters were disguised as honest tax filers who designed a fraud scheme to exploit a particular tax credit or benefit (Figure 2). The other team acted as CRA tax officers who had to detect anomalies in the tax filers’ requests, suspecting fraud. This team also designed risk controls to prevent threat actors from obtaining unwarranted tax refunds. All players had to explain their strategies and justify their decisions.

By generating effective risk controls in the game, participants understood, first hand, the criticality of cross-functional collaboration for successful detection and management of fraud risks. Players highlighted how the game helped them understand various methods that external fraud could take within their programmes. The game enabled players to appreciate the high level of sophistication that threat



Threat actors will strike quickly and will not hesitate. Our readiness to innovate should be just as decisive.

actors can achieve with their schemes. Consequently, they realised how comprehensive their risk responses must be. This game also revealed players' biases and assumptions that can influence their decisions in real life, such as their desire to provide good client service.

Post-game survey results confirmed that players valued participating in a serious game and found it relevant for their day-to-day work. They also reported gaining significant insight by playing with their colleagues from related programs with whom they do not normally interact.

To date, the CRA has delivered 11 games, assessing fraud risks in taxpayer authentication, business registration, issuing tax refunds, verifying tax claims, and assessing requests for information under the Canadian Privacy Act. With a team of five employees, each game requires approximately three months for development, execution, and a final report.

Serious games at the CRA have generated a large amount of data, identified fraud risks clearly, and proposed multiple recommendations at both strategic and operational levels.

Strategic recommendations address organisational decisions, such as CRA's roles and responsibilities in external fraud, fraud training for CRA employees, and legislative gaps in defining, investigating, and prosecuting external fraud. Operational recommendations focus on concrete risk controls that CRA programs can implement to detect or prevent fraud.

Benefits of serious games

Serious games have multiple beneficiaries. First, they directly benefit players who learn about fraud first hand, and who generate and test solutions before implementing them. Second, they benefit game observers who could include program partners or other functions in the organisation to define strategic approaches to fraud management. Finally, games benefit recipients of the final report by helping them consider various risk controls and make decisions in real life with greater confidence.

There are many reasons why public sector organisations should use serious games in risk management. Games:

- Provide a safe and a non-judgemental space for learning about external fraud, identifying risks, exploring controls, and considering outcomes.
- Are engrossing, creative, and stimulating; they encourage risk practitioners to go beyond "thinking outside the box" into formulating unique and inventive solutions.

- Enable risk practitioners to anticipate risk events or impacts before implementing a change and before a risk event occurs.
- Allow for ethical and safe exploration of risk vulnerabilities.
- Can be used to develop and stress-test existing or new fraud strategies and policy instruments.
- Build foresight to anticipate actions of threat actors.
- Facilitate risk communications internally and externally to the organisation to consolidate fraud strategies at the organisational, government, or international level.
- Always educate. Understanding external fraud risks that are unique to an organisation is the starting point to effective risk management.

As threat actors evolve, so must fraud risk management techniques. Serious games is one such new technique that enables public sector organisations to anticipate fraud schemes and to integrate preventative controls before threat actors exploit public programmes and services. Threat actors will strike quickly and will not hesitate. Our readiness to innovate in fraud risk management should be just as decisive.

We welcome opportunities to collaborate on the use of serious games to explore shared external fraud risks. If your organisation is interested in learning more or discussing how

serious games could support your work, please reach out at FraudRedTeam-EquipeRougeFraude@cra-arc.gc.ca.

CALL TO ACTION

We encourage greater use of serious games in the management of external fraud risks. Games are of particular value to public sector organisations because they stimulate innovation and a safe exploration of options in a risk averse environment. Games can identify unique fraud management approaches by capturing both known and unknown threats.

GCFP AT CIVIL SERVICE LIVE 2025

Civil Service Live is always a highlight of the government calendar. It is a chance for colleagues from across departments and professions to come together, share expertise, and spark new ideas.

This year was no exception, and the Government Counter Fraud Profession (GCFP) made a strong impression with two interactive, engaging sessions that reflected the diversity, expertise, and innovation within our field.



Session 1: Counter Fraud Careers – Inside Stories

Fraud prevention and detection may sound like something out of a novel, but for our panellists, it's their day-to-day reality. In "Counter Fraud Careers: Inside Stories", attendees got an authentic, behind-the-scenes look at the profession.

The panel brought together experienced practitioners from different parts of counter fraud, each with a unique route into the field. They spoke candidly about what drew them to the work, the skills that have been most valuable in their careers, and the real-life scenarios they've navigated. From fascinating case examples to honest reflections on both the rewards and challenges, the discussion struck a chord with the audience. Many commented afterwards that they hadn't realised just how varied the profession could be or how many different ways there are to build a career within it.

The session also shone a light on the collaborative nature of the work, and the role that cross-government partnerships play in tackling fraud and creating opportunities for career progression. The room was buzzing, with attendees leaving inspired and better informed about the paths available in counter fraud.



Session 2: Digital Defenders: Innovating Against Fraud

If the first session was about personal journeys, the second was all about teamwork and practical problem-solving. Rob Malcolmson, Deputy Director of Data & Analytics at the PSFA, led Operation Data Shield, an interactive, gamified experience that placed attendees in the role of “fraud detectives.”

Participants were given a realistic scenario involving a spike in sophisticated attempts to defraud public funds. Working in mixed teams from across departments, they used a suite of experimental Data Analysis tools to sift through information,

spot patterns, and identify which cases posed the highest risk. The exercise incorporated real analytical methods, including Single Network Analytics, data matching, and data sharing, while keeping the pace high and the atmosphere engaging.

While fun on the surface, the activity reinforced a serious point: counter fraud analytics isn't just for data specialists. Everyone has a role to play in spotting fraud indicators and applying a questioning mindset in their work.

The session wrapped up with an insightful talk from Rob on the future of counter fraud analytics, including the opportunities and challenges presented by AI and other emerging technologies. Feedback was enthusiastic, with participants praising the collaborative atmosphere, the creative use of game elements, and the practical takeaways they could bring back to their own roles.

Alongside the sessions, the GCFP team hosted a stand where attendees could learn more about membership, standards, and development opportunities. Colleagues from across the profession were on hand to answer questions, share resources, and connect with potential new members.

From quick conversations sparked by the stand's displays to in-depth discussions about career progression, the event reinforced the sense of community that lies at the heart of GCFP.

Civil Service Live 2025 was a reminder of the breadth and energy of the counter fraud profession, from personal stories that inspire, to innovative tools that equip us for the challenges ahead. Both sessions demonstrated what makes the GCFP unique: a commitment to collaboration, the sharing of expertise, and a drive to protect public services through both tried-and-true methods and forward-thinking innovation.

We left the event energised, proud of our profession, and looking forward to welcoming new colleagues into the journey.



REFERENCES

Designing Controls with Behaviour in Mind: Addressing Insider Fraud in the Public Sector

1. <https://www.sciencedirect.com/science/article/abs/pii/S1363412710000488> & <https://www.tandfonline.com/doi/full/10.1080/01639625.2023.2244116#d1e198>
2. <https://legacy.acfe.com/report-to-the-nations/2024>
3. <https://www.cifas.org.uk/insight/fraud-risk-focus-blog/insider-threat-in-public-sector>
4. <https://www.openaccessgovernment.org/addressing-insider-threats-in-the-public-sector/187801/>
5. <https://www.theguardian.com/uk-news/2015/mar/30/a4e-welfare-work-company-workers-sentenced-fraud>
6. <https://www.thetimes.com/uk/scotland/article/url-aberdeen-city-council-michael-paterson-fraud-6d2xbgns8>
7. <https://www.miaa.nhs.uk/news-publications/miaa-news/former-mental-health-nurse-jailed-for-defrauding-his-nhs-employer>
8. Wells, J. T. (2021). Principles of fraud examination (6th ed.). Wiley, US
9. <https://www.scholarlinkinstitute.org/jetems/articles/The%20New%20Fraud%20Triangle%20Model.pdf> & https://link.springer.com/rwe/10.1007/978-3-319-23514-1_216-1
10. <https://www.sciencedirect.com/science/article/pii/S0278431923002049?via%3Dihub>

Why a Fraud Control Apprenticeship

1. Office for National Statistics. 2025. Crime in England and Wales: year ending March 2025. Retrieved from: <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2025#fraud>
2. Annual Fraud Indicator. 2023. Retrieved from <https://www.crowe.com/uk/insights/annual-fraud-indicator>

3. House of Commons Justice Committee. 2022. Fraud and The Justice System. Paragraph 75. Retrieved from: <https://publications.parliament.uk/pa/cm5803/cmselect/cmjust/12/report.html#heading-2>
4. Home Office. 2024. Crime outcomes in England and Wales 2023 to 2024. Table 4.2.1. Retrieved from: <https://www.gov.uk/government/statistics/crime-outcomes-in-england-and-wales-2023-to-2024/crime-outcomes-in-england-and-wales-2023-to-2024#section1>

Why fraud is a global business opportunity for Organised Crime Gangs (OCGs)

1. [Crime and justice - Office for National Statistics](#)
2. [Fraud Strategy: stopping scams and protecting the public \(accessible\) - GOV.UK](#)
3. [Peters & Peters and Crowe report shows fraud is costing UK £219 billion a year - Peters & Peters](#)
4. [The impact of fraud and error on public funds 2023-24 - NAO overview](#)
5. [Resources | Global Anti Scam Alliance \(GASA\)](#)
6. [\(8\) Regional Trends in Financial Fraud: Insights from the Interpol Global Financial Fraud Assessment Report | LinkedIn](#)
7. [Our analysis reports- Interpol](#)
8. [UNODC Corruption and Economic Crime](#)
9. [Operation Destabilise: Russia, Organised Crime and Illicit Finance | Royal United Services Institute](#)
10. [Inside INTERPOL's probe into cyber-enabled human trafficking](#)

REFERENCES

Stammering and Fraud- Conflicts between Fraud Detection Controls and Customers Who Stammer

1. “Disability” (<https://tinyurl.com/msj946xy>), The World Health Organization, March 7, 2023.
2. UK disability statistics: Prevalence and life experiences(<https://tinyurl.com/3ww2c8c4>), UK Parliament, House of Commons Library, Oct. 2, 2024.
3. “The mysterious cause of stuttering in the brain (<https://tinyurl.com/3xzdmmamc>), by Amber Dance, BBC, Sept. 22, 2020.
4. “Answer quickly to be believed (<https://tinyurl.com/4xdka3hz>), Feb. 16, 2021.)
5. “Analysis and Tuning of a Voice Assistant System for Dysfluent Speech (<https://tinyurl.com/vt47he4r>),” by Vikramjit Mitra, Zifang Huang, Colin Lea, Lauren Tooley, Panayiotis Georgiou, Sachin Kajarekar and Jeferey Bigham, Apple Machine Learning Research, July 2021.
6. Microsoft’s AI Program Can Clone Your Voice From a 3- Second Audio Clip (<https://tinyurl.com/3hka8uvf>), by Michael Kan, PC Mag, Jan. 10, 2023.)

5. <https://www.legislation.gov.uk/ukpga/1994/33/section/166>

6. <https://www.nationaltradingstandards.uk/news/ticket-tout-family-guilty-of-online-ticket-fraud/>

7. <https://www.journaloftradingstandards.co.uk/consumer/taking-on-the-ticket-scam-touts/>

Serious Games for External Fraud Risk Analysis at the Canada Revenue Agency

1. Edmondson, Amy. The Right Kind of Wrong. New York, Simon Element/Simon Acumen. 2023
2. Dörner, Deitrich. The Logic of Failure. New York, Basic Books. 1997
3. The author and the CRA team learned to design and deliver serious games from multiple sources, especially: Defence Research and Development Canada, Department of National Defence, Global Affairs Canada, and Dr. Rex Brynen at McGill University.
4. Perla, P. and McGrady E. “Why Wargaming Works” *Naval War College Review*, Vol. 64 [2011], No. 3, Art. 8
5. “Why Wargaming Works”

Ticket Scams: The Cost of Being a Fan?

1. <https://www.standard.co.uk/news/politics/taylor-swift-eras-wembley-show-london-resell-ticket-touts-lib-dems-election-b1165901.html>
2. <https://www.theguardian.com/money/article/2024/sep/07/oasis-ticket-touts-named-resale-sites>
3. <https://www.cityam.com/government-announces-post-oasis-ticket-resale-clampdown/> <https://find-and-update.company-information.service.gov.uk/company/05699662>
4. <https://researchbriefings.files.parliament.uk/documents/SN04715/SN04715.pdf> <https://www.actionfraud.police.uk/a-z-of-fraud/ticket-fraud>

© Crown Copyright 2025

This publication is licensed under the terms of the Open Government License 3.0 except where otherwise stated.

To view this license, visit nationalarchives.gov.uk/doc/open-government-license/version/3 or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gsi.gov.uk.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned. This publication is available from khub.net/group/government-counter-fraud-profession/group-library.

Contact us:

Email: gcfp@cabinetoffice.gov.uk

Web: <https://linktr.ee/CounterFraud>