Business Fraud Alliance

Report

Business Fraud Initiative: Understanding the threat and enabling action

A report for The Fraud Advisory Panel

Dr Janice Goldstraw-White

May 2026

FRAUD ADVISORY PANEL

perpetuity research

Copyright

Perpetuity Research & Consultancy International (PRCI) Ltd
11a High Street · Tunbridge Wells · TN1 1UL · United Kingdom
www.perpetuityresearch.com prci@perpetuityresearch.com
Tel: +44 (0)1892 538690

Acknowledgements

This project has been made possible by the invaluable contributions of a wide range of stakeholders. We are sincerely grateful for their engagement, as well as for the time and insights they so generously shared.

We would like to extend our particular thanks to Matt Field, Head of the Fraud Advisory Panel, alongside trustees Lee Fitzgerald, Jonathan Holmes, and Brendan Weekes. We are also grateful to Barclays Bank for their financial support in funding this research.

Dr Janice Goldstraw-White

Executive Summary

Fraud has become one of the most significant and widespread threats affecting businesses in the United Kingdom. Advances in digital technology (including AI), the increasing use of online financial systems and communication platforms, and the growing sophistication of organised criminal groups have transformed the nature and scale of fraud risks facing organisations. While fraud has long been recognised as a major issue for individuals, it is increasingly clear that businesses across the economy are also significant and frequent victims.

National evidence illustrates the scale of the challenge. Fraud now represents the most common category of crime in the UK, with substantial economic consequences. The UK Government has estimated that fraud costs the UK economy approximately £219 billion annually. Within this broader picture, businesses represent a major group of victims. The UK *Fraud Strategy 2026–2029* notes that approximately one in four UK businesses with employees experienced fraud in the previous year, representing around 389,000 businesses and more than six million fraud incidents. For organisations, the consequences of fraud extend beyond direct financial loss and can include operational disruption, reputational damage, diversion of staff time, increased security and compliance costs, and reduced confidence in commercial relationships.

The research undertaken for this report indicates that fraud is widely experienced within the business community and is increasingly viewed as a routine operational risk. Businesses encounter a broad range of fraud threats including payment diversion and invoice fraud, business email compromise, identity impersonation, procurement fraud, insider misconduct, cyber-enabled fraud and emerging AI-enabled deception techniques such as deepfake impersonation. These threats often combine technological exploitation with social engineering, enabling criminals to manipulate employees, financial processes and digital systems.

Technological change is also accelerating the pace at which fraud methods evolve. The growing availability of artificial intelligence tools allows fraudsters to generate highly convincing phishing communications, automate large-scale scam campaigns and impersonate individuals through synthetic audio or video. These developments are increasing both the scale and sophistication of fraud attacks and making them more difficult for organisations to detect. Businesses must therefore operate in an environment where fraud risks are not only widespread but also rapidly changing.

Organisational resilience to fraud varies significantly across the business community. Larger organisations and businesses operating in sectors such as financial services and insurance often benefit from established fraud prevention infrastructures, specialist expertise and collaborative intelligence-sharing arrangements. In contrast, many small and medium-sized enterprises operate with more limited internal resources and may have less access to specialist fraud

knowledge or external support networks. These organisations may therefore face greater challenges both in preventing fraud and in responding effectively when incidents occur.

Primary research undertaken as part of this study provides additional insight into how businesses experience fraud in practice. This included surveys of both fraud specialists and non-specialist staff, alongside interviews with subject matter experts. It is important to note that the survey samples were relatively small and the findings should therefore be interpreted as indicative rather than statistically representative. They are used to highlight themes and directional insights rather than to provide definitive evidential conclusions.

Within this context, the research suggests that fraud is widely recognised as a genuine and growing risk within organisations, although levels of awareness and preparedness remain uneven. While many organisations report positive anti-fraud cultures, training programmes and internal reporting arrangements, there are still gaps in staff awareness, access to training and clarity about reporting processes.

The research also identified a strong desire among businesses for clearer guidance, practical examples and more accessible information about fraud risks. Respondents frequently highlighted confusion around terminology, particularly where fraud overlaps with cybercrime, scams and other forms of economic crime. Many businesses expressed a preference for practical guidance materials, case studies and role-specific examples that could help staff recognise fraud risks in everyday operational settings.

Another key finding concerns the complexity of the current support landscape. The UK has developed an extensive network of organisations and initiatives involved in fraud prevention, intelligence sharing and enforcement. These include law enforcement agencies, industry bodies, professional organisations and specialist fraud prevention initiatives. While this ecosystem demonstrates substantial activity in addressing fraud, it can also appear fragmented from the perspective of businesses seeking assistance. Businesses may encounter multiple organisations with differing responsibilities, reporting processes and support services.

Survey findings (noting their indicative nature) suggest that internal reporting arrangements within organisations are often clearer and more accessible than external reporting pathways. By contrast, experiences of external reporting and support were frequently described as inconsistent. Businesses reported difficulties navigating reporting systems, limited feedback following reports and uncertainty about where to seek practical assistance following a fraud incident (note: the surveys were carried out before the launch of Report Fraud). These perceptions highlight the importance of clearer signposting and more accessible guidance.

Taken together, the findings suggest that while fraud prevention efforts are well developed in some sectors, support for businesses affected by fraud remains

uneven across the wider economy. Businesses appear to benefit most where fraud awareness is embedded within organisational culture, where staff receive regular and relevant training, and where reporting mechanisms are clear and accessible. However, many organisations, particularly SMEs, may require additional support to strengthen these capabilities.

The analysis also highlights that businesses require assistance not only with prevention but also with response and recovery. Practical guidance on how to respond to fraud incidents, preserve evidence, engage with financial institutions, consider legal options and restore normal operations can be particularly valuable. At present, this type of support is not always readily accessible or clearly signposted.

The recommendations set out in this report (see Section 5) have been developed in response to these findings and to inform the Fraud Advisory Panel's *Business Fraud Alliance* initiative. They are designed to strengthen business resilience to fraud by improving awareness, supporting organisations in implementing proportionate prevention measures, clarifying reporting pathways and strengthening coordination across the wider fraud support landscape. The recommendations recognise that businesses differ significantly in size, capability and sector context, and therefore propose a combination of short-term actions aimed at improving awareness and accessibility alongside longer-term measures designed to strengthen organisational capability and collaboration.

The recommendations are organised under five broad themes:

- Improve fraud awareness and understanding
- Bolster prevention and internal controls
- Enhance fraud response and recovery
- Expand sector engagement and capability
- Strengthen coordination and the wider fraud ecosystem

Together, these measures aim to support businesses in better understanding fraud risks, improving their ability to prevent and detect fraud, and accessing clearer and more coordinated support when incidents occur. By strengthening organisational resilience and improving the accessibility of fraud-related guidance and support, the initiative can play an important role in helping businesses respond more effectively to the evolving fraud threat.

Table of Contents

Section 1. Introduction

Background

1.1 The Fraud Advisory Panel continues to champion best practices in the prevention, detection, and deterrence of fraud through its unwavering commitment to education, collaboration, and research. Building on the momentum of the successful *Future Counter Fraud Community* (FCFC) initiative launched in 2024, and the impactful *Love Business Hate Fraud* campaign of 2023, the Fraud Advisory Panel launched its latest initiative, the *Business Fraud Alliance* in June 2025, aimed to further empower businesses of all sizes across various sectors in their fight against fraud.

1.2 The findings set out in this report are based on research commissioned by the Fraud Advisory Panel and carried out by Perpetuity Research. The work was undertaken to inform and support the broader aims of the initiative, providing a basis to guide its development and delivery.

Aims of the research

1.3 The overall aim of this research was to develop a comprehensive understanding of the fraud landscape as it affects businesses. This included examining the scale and nature of fraud experienced by organisations, as well as its operational and financial impacts, alongside emerging and future threats, particularly those associated with developments in artificial intelligence and deepfake technologies. The research also considered levels of awareness among personnel (not limited to those in fraud-specific roles), regarding the prevention and management of fraud in their organisations.

1.4 In addition, the study assessed the types of support currently available to organisations and identified gaps in provision, exploring what tools, resources, and interventions are needed, and for whom, to strengthen organisational capability. The findings and recommendations are intended to support the Fraud Advisory Panel in developing targeted initiatives to improve organisational decision-making and risk management in relation to fraud. They also aim to inform government policy and enhance the ability of support organisations to deliver more relevant, targeted, and impactful guidance, equipping businesses with the knowledge, language, and tools needed to address fraud effectively and build long-term resilience.

Research approach

1.5 The research drew on a combination of methods to address the study objectives. Two surveys were conducted with fraud personnel (n=55) and non-fraud personnel (n=52) across organisations; however, response

rates were limited, and the findings should therefore be treated as indicative. This was complemented by a review of relevant literature and existing reports to provide context. In addition, consultations with fraud experts were undertaken to capture practical insights and perspectives. Together, these approaches helped to build a rounded understanding of the issues explored in this study.

Section 2. The scale and nature of frauds affecting businesses

Introduction

2.1 Fraud is widely recognised as one of the most significant and rapidly evolving threats affecting businesses in the United Kingdom (UK) and internationally. Technological developments, the rapid expansion of digital financial services and the increasing interconnectedness of global supply chains have created new opportunities for criminals to target organisations. The growth of online transactions, remote working practices and digital communication platforms has further expanded the range of vulnerabilities that may be exploited by fraudsters (Home Office, 2023;[1] Deloitte, 2023).[2] As a result, fraud has become both more prevalent and more sophisticated, affecting organisations of all sizes and across a wide range of economic sectors.

2.2 In recent years fraud has come to represent a substantial proportion of crime. The UK Government's 2023 *Fraud Strategy: stopping scams and protecting the Public* identifies fraud as the most common crime experienced by both individuals and organisations, highlighting the scale of the challenge facing law enforcement, regulators and businesses (Home Office, 2023).[1] The strategy emphasises that advances in technology have enabled criminals to scale fraudulent activity rapidly while reducing the risks associated with traditional forms of crime.

2.3 Fraud affecting businesses can take many forms, including payment diversion scams, cyber-enabled fraud, procurement fraud, identity impersonation and insider misconduct. These offences may involve external actors, organised crime groups or individuals operating within organisations. In addition to direct financial losses, fraud can cause operational disruption, reputational damage and erosion of trust within commercial relationships. Businesses affected by fraud may also incur substantial costs associated with investigation, legal proceedings, system remediation and the

[1] Home Office (2023). *Fraud Strategy: Stopping Scams and Protecting the Public.* London: Home Office. Available at: https://assets.publishing.service.gov.uk/media/69ae77ddc78869bf8eb8a509/fraud-strategyweb.pdf

[2] Deloitte (2023). *Fraud and Financial Crime Trends 2023.* London: Deloitte. https://www.deloitte.com/uk/en/Industries/financial-services/perspectives/regulatory-outlookfinancial-crime.html

implementation of strengthened control measures (Association of Certified Fraud Examiners, 2024;[3] PwC, 2024).[4]

2.4 Evidence suggests that fraud represents a significant risk for organisations globally. The Association of Certified Fraud Examiners (ACFE) estimates that organisations lose approximately five percent of annual revenue to fraud, illustrating the substantial financial impact of fraudulent activity across industries.[5] At the same time, international surveys indicate that a large proportion of organisations experience some form of fraud during their operations, demonstrating that fraud is not a rare or exceptional event but a recurring operational risk for many businesses.[6] Evidence from fraud prevention organisations also highlights the scale and evolving nature of business fraud. For example, analysis published by Cifas indicates continuing increases in fraud risks affecting organisations, including identity misuse, account takeover and insiderenabled fraud, reflecting the growing sophistication of criminal activity targeting businesses.[7]

2.5 Small and medium-sized enterprises (SMEs) appear to face particular vulnerabilities in relation to fraud. Unlike larger corporations, many SMEs lack specialist fraud prevention expertise, dedicated compliance functions or advanced cybersecurity capabilities. Limited financial resources may also constrain the ability of smaller organisations to invest in fraud detection systems or specialist risk management support. As a result, SMEs may be disproportionately affected by fraud and may face greater challenges recovering from financial losses or operational disruption.[7]

2.6 Research conducted by the Federation of Small Businesses highlights the scale of crime affecting smaller firms, including fraud, cybercrime and financial scams. The report, *Cracking the Case: Uncovering the Cost of Small Business Crime*, notes that criminal activity against small businesses can have significant economic and operational consequences, particularly

[3] Association of Certified Fraud Examiners (ACFE) (2024). *Occupational Fraud: A Report to the Nations.* Austin, TX: ACFE. https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2024/2024report-to-the-nations.pdf

[4] PwC (2024). *Global Economic Crime and Fraud Survey.* London: PwC. https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html

[5] Association of Certified Fraud Examiners (ACFE) (2024). *Occupational Fraud: A Report to the Nations.* Austin, TX: ACFE. https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2024/2024report-to-the-nations.pdf

[6] PwC (2024). *Global Economic Crime and Fraud Survey.* London: PwC. https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html [7] Cifas (2026). *Fraudscape 2026.* London: Cifas. Available at: https://www.cifas.org.uk/newsroom/fraudscape2026

[7] Federation of Small Businesses (2024). *Cracking the Case: Uncovering the Cost of Small Business Crime.* London: FSB. Available at: https://www.fsb.org.uk/resources/policy-reports/cracking-the-case-uncovering-the-cost-of-small-business-crime-MCFNQDUF7BPRB6VCHHFKKJICCISI

where organisations lack access to effective support or recovery mechanisms following an incident.[8]

2.7 Despite the scale of fraud affecting organisations, much public policy and victim support activity has historically focused on individuals rather than businesses. While recent policy initiatives, including the new UK fraud strategy, recognise the importance of strengthening resilience among organisations, there remains limited evidence regarding the specific needs of businesses affected by fraud and the types of support that may be most effective in assisting them.

2.8 Understanding the scale, nature and emerging trends of fraud affecting businesses is therefore an important step in developing targeted initiatives aimed at strengthening organisational resilience, improving awareness of fraud risks and identifying effective mechanisms to support businesses that experience fraud incidents.

The scale of fraud affecting businesses

2.9 Fraud represents one of the most prevalent forms of crime in the UK. Data from the Office for National Statistics indicate that fraud accounts for a substantial proportion of offences recorded in England and Wales, with millions of incidents occurring each year.[8] The increasing digitalisation of financial services, widespread use of online communication platforms and the growth of remote transactions have significantly expanded the opportunities for fraud to occur.

2.10 The economic impact of fraud is considerable. The UK Government estimates that fraud costs the UK economy approximately £219 billion annually, affecting individuals, businesses and public sector organisations.[9] These losses include both direct financial harm and wider economic impacts, such as disruption to business operations, increased security expenditure and reduced confidence in digital financial systems.

2.11 Businesses represent a significant proportion of victims of fraud Evidence from the UK Economic Crime Survey provides insight into the prevalence of fraud experienced by businesses. The survey found that 27% of businesses with employees experienced fraud within a 12-month period,

[8] Office for National Statistics (ONS) (2025). *Crime in England and Wales.* London: ONS. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingseptember2025

[9] Home Office (2023). *Fraud Strategy: Stopping Scams and Protecting the Public.* London: Home Office. Available at: https://assets.publishing.service.gov.uk/media/69ae77ddc78869bf8eb8a509/fraud-strategyweb.pdf

equating to approximately 389,000 organisations across the UK economy.[10] These findings indicate that fraud is not an isolated risk but a common challenge affecting a substantial proportion of businesses.

2.12 Evidence from fraud prevention organisations reinforces these findings. Analysis published in the latest Cifas *Fraudscape* report highlights the continuing growth in fraud risks affecting organisations, including identity misuse, account takeover and insider-enabled fraud. The report emphasises that businesses increasingly face fraud threats linked to digital identity compromise and organised criminal activity targeting corporate systems and financial processes.[11]

2.13 SMEs appear particularly vulnerable to fraud. Research conducted by the Federation of Small Businesses indicates that many smaller organisations lack the specialist knowledge, dedicated personnel and financial resources required to implement comprehensive fraud prevention strategies. As a result, SMEs may face greater exposure to fraud risks and may experience greater difficulty recovering financially following fraud incidents.[12]

2.14 Industry surveys also demonstrate the widespread nature of fraud affecting organisations globally. PwC's *Global Economic Crime and Fraud Survey* found that approximately 41% of organisations experienced fraud within the previous two years, highlighting the extent to which fraud represents a routine operational risk across sectors and jurisdictions.[13]

2.15 Taken together, these findings indicate that fraud affecting businesses is both widespread and economically significant. The evidence suggests that a substantial proportion of organisations experience fraud during their operations, while many businesses, particularly SMEs, may face challenges in preventing, detecting and recovering from fraud incidents. These issues highlight the importance of developing targeted initiatives aimed at strengthening business resilience and improving the support available to organisations affected by fraud.

[10] Home Office (2024). *UK Economic Crime Survey.* London: Home Office. https://www.gov.uk/government/publications/economic-crime-survey-2024/economic-crimesurvey-2024

[11] Cifas (2026). *Fraudscape 2026.* London: Cifas. Available at: https://www.cifas.org.uk/newsroom/fraudscape2026

[12] Federation of Small Businesses (2024). *Cracking the Case: Uncovering the Cost of Small Business Crime.* London: FSB. Available at: https://www.fsb.org.uk/resources/policy-reports/cracking-the-case-uncovering-the-cost-of-small-business-crime-MCFNQDUF7BPRB6VCHHFKKJICCISI

[13] PwC (2024). *Global Economic Crime and Fraud Survey.* London: PwC. https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html

Evidence from major fraud studies

2.16 One of the most comprehensive global studies examining fraud affecting organisations is the ACFEs *Report to the Nations*.[14] The 2024 edition analysed 1,921 occupational fraud cases across 138 countries, providing detailed insights into how fraud occurs within organisations and the factors that enable it.

2.17 The report estimates that organisations typically lose approximately five percent of annual revenue to fraud, illustrating the potentially substantial financial impact of fraudulent activity across industries. The cases analysed involved total losses exceeding $3.1 billion, with an average loss

per case of approximately $1.7 million (approximately £1.3m. These findings highlight the significant financial risks that fraud can pose to organisations, particularly where fraudulent activity remains undetected for extended periods.

2.18 The research also identifies a number of common organisational vulnerabilities that enable fraud to occur. Weak internal control systems, inadequate oversight and management override of established control procedures were identified as key contributing factors in many cases. These findings reinforce the importance of strong governance frameworks and internal control mechanisms in reducing fraud risks within organisations.

2.19 In terms of detection, the ACFE report highlights the critical role of internal reporting mechanisms. Approximately 43% of fraud cases were detected through tips, most frequently from employees, making whistleblowing and internal reporting systems the most effective detection method identified in the study.[15] This finding emphasises the importance of organisational cultures that support transparency and encourage the reporting of suspected wrongdoing.

2.20 Evidence from other international and industry studies reinforces these findings. Professional services firms and fraud prevention organisations consistently identify a range of emerging risks affecting businesses. For example:

[14] Association of Certified Fraud Examiners (ACFE) (2024). *Occupational Fraud: A Report to the Nations.* Austin, TX: ACFE. https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2024/2024report-to-the-nations.pdf

[15] Association of Certified Fraud Examiners (ACFE) (2024). *Occupational Fraud: A Report to the Nations.* Austin, TX: ACFE. https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2024/2024report-to-the-nations.pdf

- PwC's *Global Economic Crime and Fraud Survey* identifies cybercrime, procurement fraud and payment diversion scams as among the most significant threats facing organisations globally.[16]
- Deloitte highlights the increasing role of digital technologies in enabling fraud schemes, including business email compromise, identity impersonation and cyber-enabled financial fraud targeting corporate systems.[18]
- KPMG emphasises the importance of robust internal control systems, risk governance frameworks and organisational oversight in preventing fraud and white-collar crime within businesses.[17]
- EY identifies organisational culture, transparency and effective whistleblowing mechanisms as key factors influencing the detection and prevention of misconduct and financial crime.[18]

2.21 Evidence from fraud prevention organisations in the UK also highlights evolving risks affecting businesses. For example, the recently published Cifas *Fraudscape* reports increasing levels of identity fraud, account takeover and insider-enabled fraud, demonstrating the growing role of digital identity compromise and organised criminal activity targeting organisations.[19]

2.22 Taken together, these studies demonstrate that fraud affecting businesses is both widespread and increasingly complex, often involving a combination of technological exploitation, social engineering and weaknesses in organisational controls.

Types of fraud affecting businesses

2.23 Fraud affecting businesses occurs through a range of schemes involving both external criminals and individuals operating within organisations (or a combination of both). While the specific techniques used by fraudsters continue to evolve, research and industry reporting consistently identify several common fraud types that affect organisations across multiple sectors.

2.24 Understanding the mechanisms through which fraud occurs is important when developing initiatives aimed at improving business resilience and

[16] PwC (2024). *Global Economic Crime and Fraud Survey.* London: PwC. https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html [18] Deloitte (2023). *Fraud and Financial Crime Trends 2023.* London: Deloitte. https://www.deloitte.com/uk/en/Industries/financial-services/perspectives/regulatory-outlookfinancial-crime.html
[17] KPMG (2025). *Fraud Barometer 2024: A snapshot of fraud in the UK.* London: KPMG.
[18] EY (2024). *Global Integrity Report 2024.* London: EY. https://www.ey.com/en_uk/insights/forensic-integrity-services/global-integrity-report
[19] Cifas (2026). *Fraudscape 2026.* London: Cifas. Available at: https://www.cifas.org.uk/newsroom/fraudscape2026

supporting organisations affected by fraud. Evidence from major studies and fraud prevention bodies indicates that many fraud incidents exploit weaknesses in organisational processes, digital systems or communication channels.[20]

2.25 Recent intelligence from fraud prevention organisations highlights how the fraud landscape is evolving rapidly as criminals exploit digital technologies and online systems. For example, data reported by Cifas this year indicates that nearly 445,000 fraud risk cases were recorded to the National Fraud Database in 2025, representing a record level of reported fraud activity among participating organisations. Identity fraud remains the most common type of fraud recorded, accounting for approximately 59% of all cases.[21]

2.26 Based on reviews of major industry and government reports the ten most common forms of frauds affecting businesses include:

- insider fraud
- payment diversion/invoice fraud
- business email compromise
- AI-enabled and deepfake fraud
- cyber-enabled fraud
- data and intellectual property theft
- identify and business impersonation fraud
- account takeover fraud
- procurement and supplier fraud
- goods and services fraud

2.27 Descriptions of each of these categories can be found in Appendix A.

Emerging threats – AI-enabled fraud

2.28 While many forms of fraud affecting businesses are well established, the methods used by fraudsters continue to evolve rapidly in response to technological developments. Digitalisation, increased reliance on online communication and the growing use of automated systems in business operations have expanded the opportunities for criminals to target organisations. Researchers and policy bodies have highlighted that fraud is increasingly enabled by digital technologies that allow offenders to operate across borders, target large numbers of victims and exploit weaknesses in organisational systems.[21]

[20] Association of Certified Fraud Examiners (ACFE) (2024). *Occupational Fraud: A Report to the Nations.* Austin, TX: ACFE. https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2024/2024report-to-the-nations.pdf

[21] https://kpmg.com/ca/en/insights/2026/03/fraud-in-the-age-of-ai.html

2.29 One of the most significant developments in recent years has been the emergence of artificial intelligence (AI)-enabled fraud. Advances in generative AI technologies have made it easier for criminals to produce convincing scam communications, automate fraudulent activity and impersonate individuals or organisations with increasing realism. As a result, AI is increasingly recognised as a major emerging threat within the fraud landscape affecting businesses.

2.30 AI technologies enable fraudsters to increase both the scale and sophistication of fraud attacks. Generative AI tools can rapidly produce highly convincing phishing messages, fraudulent invoices and social engineering communications that mimic legitimate business correspondence. These communications may be tailored to specific organisations or employees, increasing their credibility and reducing the likelihood that they will be recognised as fraudulent.[22]

2.31 Researchers have also highlighted the increasing role of automation in fraud operations, allowing criminals to launch large-scale campaigns targeting thousands of organisations simultaneously. This capacity to scale fraud attacks significantly increases the overall volume of fraud

attempts faced by businesses and increases the probability that some attacks will succeed.[23]

2.32 Another emerging threat involves the use of deepfake technologies, which allow criminals to generate synthetic audio or video that convincingly imitates real individuals. These technologies have already been used in several reported incidents involving corporate fraud.

2.33 In one widely reported case in 2019, criminals used AI-generated voice technology to impersonate the chief executive officer of a German energy company, persuading a senior employee to transfer approximately €220,000 to a fraudulent account. The employee believed the request to be genuine because the voice closely resembled that of the CEO.[24]

2.34 More recently, in 2024, fraudsters reportedly used deepfake video technology to impersonate senior executives during an online meeting, convincing a finance employee of a multinational company to authorise multiple transfers totalling more than £20 million. The attackers used

[22] https://www.ncsc.gov.uk/report/impact-ai-cyber-threat-now-2027
[23] https://www.weforum.org/stories/2026/02/ai-supercharging-global-cyber-fraud-crisis-couldalso-solve-it/
[24] https://www.icaew.com/insights/viewpoints-on-the-news/2025/jan-2025/how-to-guardagainst-voice-cloning-and-deepfake-scams

AIgenerated video and audio to create convincing digital representations of company executives during the call.[25]

2.35 These cases illustrate how AI technologies can be used to exploit organisational hierarchies and trust structures within businesses. Employees may be particularly vulnerable to these attacks where requests appear to originate from senior colleagues or where communications appear authentic.

2.36 Fraud prevention organisations have warned that the increasing availability of generative AI tools may significantly increase the volume, speed and credibility of fraud attempts. Intelligence published by Cifas *Fraudscape* highlights the growing role of identity fraud and digital impersonation in fraud cases recorded by UK organisations.[26]

2.37 Similarly, international law enforcement bodies, including Europol, have warned that generative AI technologies may enable criminals to create more convincing and scalable fraud schemes. AI-generated content, such as synthetic text, voice cloning and deepfakes, can enhance social engineering by increasing realism and reducing the effort required to target victims. This lowers barriers to entry while enabling organised groups to automate attacks at scale, making fraudulent communications harder to detect and increasing the risk of successful deception.[27]

2.38 Academic research on cyber-enabled fraud also highlights the importance of understanding the interaction between technology and organisational vulnerability. Studies indicate that fraud attacks are often successful where criminals exploit behavioural factors such as trust, authority and urgency within organisational decision-making processes. These dynamics are increasingly amplified by digital technologies, which enable attackers to tailor communications more precisely and convincingly to organisational contexts. As a result, vulnerabilities are not solely technical but are embedded within everyday practices, routines and communication flows,

[25] https://www.theguardian.com/technology/article/2024/may/17/uk-engineering-arupdeepfake-scam-hong-kong-ai-video

[26] Cifas (2026). *Fraudscape 2026.* London: Cifas. Available at: https://www.cifas.org.uk/newsroom/fraudscape2026

[27] Europol (2023). *Facing Reality? Law Enforcement and the Challenge of Deepfakes.* The Hague: Europol. https://www.europol.europa.eu/publications-events/publications/facingreality-law-enforcement-and-challenge-of-deepfakes

creating opportunities for fraud to occur even where formal controls are in place.[28][29]

2.39 These developments suggest that the fraud landscape facing businesses is becoming increasingly complex and technologically driven. Businesses may therefore require new approaches to fraud prevention, including stronger verification procedures, improved employee awareness training and enhanced authentication mechanisms for financial transactions. The impact of these emerging threats may vary across organisations depending on their size, sector and available resources. Smaller organisations may face particular challenges in responding to technologically sophisticated fraud threats due to limited access to specialist expertise or advanced fraud prevention systems.

Fraud risks by business size and sector

2.40 Organisations differ significantly in terms of their size, resources, governance structures and operational activities, all of which influence both their vulnerability to fraud and their capacity to respond effectively when fraud occurs. These variations mean that a one-size-fits-all approach to fraud prevention and response is unlikely to be effective. Instead, strategies must be appropriately tailored to reflect the specific risks, capabilities and operating contexts of each organisation.

Business size and organisational capability

2.41 Research consistently indicates that smaller businesses may face particular challenges in preventing and responding to fraud. Compared with large organisations, SMEs often have fewer financial and human resources available to invest in fraud prevention systems, cybersecurity

infrastructure or specialist risk management expertise.[30] Many smaller firms do not employ dedicated compliance or fraud prevention personnel, and financial management responsibilities may be concentrated among a small number of staff or business owners.

[28] Schmitt, J., & Flechais, I. (2024). Generative AI in social engineering: A systematic review. *Artificial Intelligence Review*. https://doi.org/10.1007/s10462-024-10973-2

[29] Gonzaga, J. (2026). Exploiting trust: AI and deepfakes in social engineering. *Computers*. https://www.mdpi.com/2073-431X/15/2/128

[30] See for example: Adeboye, E. O. (2024). Strengthening fraud prevention in small businesses: An analysis of effective accounting and auditing practices. *International Journal of Science and Research Archive, 11*(1), 123–131.; Hess, M. F. (2016). Fraud risk management: A small business perspective. *Business Horizons, 59*(6), 635–643.; and Chand, I. (2022). *Strategies small-business leaders use to prevent employee fraud* (Doctoral dissertation, Walden University). Walden University ScholarWorks.

2.42 Evidence from the Federation of Small Businesses (FSB) highlights the scale of crime affecting smaller firms in the UK. The FSB report *Cracking the Case: Uncovering the Cost of Small Business Crime*[31] notes that criminal activity, including fraud and cyber-enabled offences, can have significant financial and operational consequences for small businesses. Smaller firms may face particular difficulties absorbing financial losses or operational disruption following fraud incidents, particularly where businesses operate with narrow margins or limited financial reserves.

2.43 In addition to limited internal resources, smaller businesses may also face barriers to accessing external fraud prevention support. Owners and managers may lack awareness of available support networks, may not have time to engage with training or industry initiatives, or may perceive fraud prevention as a lower priority compared with other operational pressures. Smaller organisations may also lack established relationships with industry bodies or professional networks through which fraud intelligence is shared.

Sector differences and established fraud prevention ecosystems

2.44 Fraud risks also vary significantly across different parts of the economy. In areas with longstanding exposure to financial crime, more mature prevention infrastructures have often been established. These typically include well-developed collaborative networks, shared intelligence systems, and industry-led initiatives designed to strengthen the detection and prevention of fraud.

2.45 The banking and financial services sector represents one of the most mature environments for fraud prevention. Financial institutions have historically been major targets for fraud and have therefore invested heavily in fraud detection technologies, internal control systems and collaborative intelligence sharing. Organisations such as UK Finance, the Joint Fraud Taskforce, Cifas, and the National Economic Crime Centre (NECC) support coordination between financial institutions, law enforcement agencies and government bodies in addressing fraud threats. Financial institutions also operate extensive transaction

monitoring systems and fraud reporting mechanisms that allow suspicious activity to be identified rapidly.

2.46 Similarly, the insurance sector has developed specialised initiatives aimed at addressing fraud risks. The Insurance Fraud Bureau (IFB) and Insurance Fraud Enforcement Department (IFED) coordinate intelligence gathering, investigation and enforcement activity relating to insurance fraud. These

[31] https://www.fsb.org.uk/resources/policy-reports/cracking-the-case-uncovering-the-cost-ofsmall-business-crime-MCFNQDUF7BPRB6VCHHFKKJICCISI

organisations facilitate collaboration between insurers, law enforcement and regulators in identifying organised fraud networks and detecting fraudulent claims.

2.47 The retail sector has also developed collaborative responses to crime affecting businesses. Organisations such as the British Retail Consortium (BRC), the National Business Crime Centre (NBCC) and local Business Crime Reduction Partnerships (BCRPs) support information sharing, intelligence gathering and coordinated responses to retail crime. These initiatives often involve collaboration between retailers, police forces and local authorities in addressing criminal activity affecting retail businesses.

Sectors with more limited fraud support structures

2.48 In contrast, many other sectors do not benefit from comparable fraud prevention ecosystems. Businesses operating in sectors such as construction, hospitality, professional services, manufacturing and smaller digital enterprises may have less access to coordinated fraud intelligence networks or industry-led fraud prevention initiatives. These sectors often consist of large numbers of small or medium-sized firms with diverse operational models and limited centralised coordination. As a result, opportunities for collective information sharing and coordinated fraud prevention activity may be more limited.

2.49 For example, construction businesses frequently operate through complex supply chains involving multiple subcontractors and suppliers, which can create vulnerabilities to procurement fraud, invoice fraud and payment diversion schemes. However, the sector does not typically benefit from the same level of coordinated fraud intelligence infrastructure seen in financial services.

2.50 Similarly, small professional service firms and hospitality businesses may rely heavily on digital communication and online transactions but may not have access to industry-wide fraud intelligence sharing networks. This may leave organisations reliant on internal knowledge or general guidance when responding to fraud incidents.

Implications for business support initiatives

2.51 These size and sector variations highlight that the level of fraud resilience across the business community is uneven. While some sectors benefit from mature fraud prevention infrastructures and collaborative networks, many businesses, particularly SMEs operating outside the financial services or retail sectors, may have limited access to comparable support mechanisms.

2.52 Recognising these differences is important when designing initiatives aimed at supporting businesses affected by fraud. Effective support mechanisms may therefore need to consider variations in organisational size, sector and

existing fraud prevention capacity when developing guidance, reporting pathways and collaborative support structures.

Policy and institutional response to fraud against businesses

2.53 Fraud has become a major policy priority in the UK due to its scale and increasing impact on individuals, businesses and the wider economy. Under the previous government, the *Fraud Strategy: Stopping Scams and Protecting the Public*[32] published in 2023 set out a national framework focused primarily on protecting individuals from scams, while also introducing measures relevant to businesses. In March 2026, the UK Government published the *Fraud Strategy 2026–2029*,[33] which updates this approach in response to an evolving threat landscape, including the growth of large-scale, digitally enabled and AI-driven fraud.

2.54 While both strategies recognise fraud as the most prevalent crime in the UK, the 2026 strategy places greater emphasis on system-wide resilience, prevention at scale and the role of organisations in both enabling and preventing fraud. This reflects a shift towards recognising businesses not only as victims of fraud, but also as critical actors in its prevention, particularly in sectors such as banking, telecommunications, e-commerce and digital platforms. The strategy is structured around three principal objectives:

1. **Pursuing fraudsters:** Strengthening the ability of law enforcement agencies to investigate and prosecute fraud remains a central priority. Building on measures introduced under the 2023 strategy, the updated approach focuses on improving intelligence capabilities, targeting organised fraud networks and enhancing coordination across agencies. For businesses, this is particularly relevant in addressing large-scale and repeat fraud targeting organisations, as well as fraud facilitated through corporate structures, supply chains and organised criminal networks.
2. **Blocking fraud at source:** The 2026 strategy places stronger emphasis on preventing fraud before it reaches victims, with a clear expectation that organisations play a more active role in reducing fraud risk within their systems and services. This includes improving identity verification, strengthening controls across digital platforms and

reducing opportunities for fraud within payment systems and online environments. Compared to the 2023 strategy, there is a more explicit

[32] https://www.gov.uk/government/publications/fraud-strategy/fraud-strategy-stopping-scamsand-protecting-the-public

[33] https://assets.publishing.service.gov.uk/media/69ae77ddc78869bf8eb8a509/fraud-strategyweb.pdf

focus on upstream intervention, particularly in response to the scalability of fraud enabled by technologies such as artificial intelligence.

3. **Empowering individuals and organisations:** Improving awareness of fraud risks and strengthening reporting and support mechanisms remains a key objective. The 2026 strategy places increased emphasis on ensuring that organisations are better equipped to identify, prevent and respond to fraud, including through improved access to guidance, enhanced reporting systems and better use of shared data to identify emerging threats.

2.55 The 2026 strategy continues to emphasise the importance of public–private collaboration, recognising that much of the data required to detect and prevent fraud is held by private sector organisations. For businesses, this reinforces their dual role as both targets of fraud and key partners in its prevention, particularly through intelligence sharing and coordinated action with government and law enforcement.

2.56 Alongside these strategic developments, legislative reforms such as the Economic Crime and Corporate Transparency Act (ECTA) 2023 continue to underpin the UK's response to fraud, including the recently introduce Failure to Prevent Fraud (FTPF) offence. These measures are particularly relevant to businesses, as they aim to improve corporate transparency, strengthen the integrity of company registration processes and reduce the misuse of corporate structures for fraud and other economic crimes.

2.57 In addition to national policy frameworks, a wide range of organisations and partnerships contribute to the prevention, investigation and disruption of fraud affecting businesses. Many of these bodies were strengthened or expanded following the 2023 strategy and continue to operate within the updated 2026 framework.

2.58 At the national level, organisations such as the National Economic Crime Centre (NECC), the City of London Police (as the national lead force for fraud), the National Fraud Intelligence Bureau (NFIB) and the National Crime Agency (NCA) play key roles in coordinating intelligence, analysing fraud reports and supporting investigations into serious and organised fraud. These organisations are particularly relevant to businesses that are victims of complex, high-value or organised fraud.

2.59 Industry-led initiatives also play a critical role in preventing fraud through collaboration and information sharing. Organisations such as Cifas, UK Finance, National Hunter and the Joint Money Laundering Intelligence Taskforce (JMLIT) enable businesses to share intelligence on suspected fraud and financial crime. These initiatives are particularly important in sectors where organisations face sustained and high-volume fraud risks.

2.60 Professional bodies and industry associations contribute by providing guidance, training and support to help organisations strengthen their

resilience. Organisations, beyond your own, such as Cifas, the Institute of Chartered Accountants in England and Wales (ICAEW) and the British Chambers of Commerce support businesses in improving internal controls, developing fraud risk management frameworks and responding effectively to incidents.

2.61 At a regional level, fraud forums and collaborative partnerships provide opportunities for organisations to share information about emerging threats and prevention strategies. These networks complement national initiatives and contribute to improving overall resilience. Cyber-enabled fraud risks are addressed through specialised initiatives such as the National Cyber Security Centre (NCSC), Cyber Aware, Cyber Resilience Centres and regional police cybercrime units, which provide guidance, threat intelligence and incident response support to organisations affected by cyber-related fraud.

2.62 Appendix B presents a preliminary, non-exhaustive overview of organisations at local, regional, national and international levels that may be available to support businesses in addressing fraud-related issues, outlining relevant sectors, forms of assistance, and contact details.

Adequacy of the strategy and gaps in support for businesses

2.63 While the UK's fraud response demonstrates a high level of activity across government, law enforcement and industry, the effectiveness of this landscape for businesses depends on how far current policy translates into clear, accessible and coordinated support. The *Fraud Strategy 2026– 2029* signals a more explicit recognition of the role of businesses in the fraud ecosystem compared to the earlier fraud strategy published in 2023. In particular, it places greater emphasis on:

- upstream prevention within business systems and services
- enhanced data sharing and intelligence collaboration between organisations
- stronger expectations on sectors that enable or facilitate fraud
- improved reporting and information flows to identify emerging threats

2.64 This represents a significant shift from the 2023 strategy, which was more heavily focused on consumer protection, with businesses primarily positioned as delivery partners rather than as direct beneficiaries of structured support.

2.65 From a business perspective, the current approach offers several strengths, including a strong focus on prevention, continued investment in enforcement capability and an emphasis on public–private collaboration. These elements are important in reducing overall fraud risk. However, the extent to which this translates into practical, accessible support for organisations experiencing fraud is less clear. Much of the strategy remains

focused on system-level prevention and disruption, rather than on the operational needs of businesses dealing with fraud incidents.

2.66 However, several gaps remain evident:

1. **Limited focus on post-incident support:** There remains no clearly defined, coordinated pathway for organisations seeking support after experiencing fraud, requiring engagement with multiple bodies.
2. **Fragmentation of the support landscape:** The number of organisations and initiatives creates complexity, with overlapping roles and responsibilities that may reduce accessibility and clarity for businesses.
3. **Increased expectations without equivalent support structures**: The strategy places greater responsibility on organisations to prevent fraud, but this is not always matched by proportionate tools, guidance or coordinated support mechanisms.
4. **Limited visibility of outcomes for businesses:** There is relatively little emphasis on measurable outcomes such as reduced business losses, improved recovery or enhanced support experiences.
5. **Lack of an end-to-end business-focused response:** Prevention, enforcement and support functions remain distributed across multiple entities, with limited integration into a single, coherent journey for businesses affected by fraud.

2.67 Overall, the 2025 fraud strategy represents a progression from the 2023 one, particularly in recognising the systemic, technology-driven nature of fraud and the central role of organisations in prevention. However, from a business perspective, the approach remains weighted towards prevention and system-level intervention, with comparatively less emphasis on coordinated, user-centred support for organisations affected by fraud.

2.68 These gaps indicate a clear opportunity for initiatives that focus on:

- simplifying access to support for businesses
- providing clearer pathways following fraud incidents
- improving coordination across existing organisations
- complementing regulatory expectations with practical, operational support

2.69 Addressing these areas would strengthen the effectiveness of the UK's fraud response and better align national strategy with the needs of organisations operating in an increasingly complex fraud landscape.

Section 3. Stakeholder perspectives on business fraud

Introduction

3.1 The preceding section has examined the scale, nature and evolving landscape of fraud affecting businesses, drawing on international and national statistics, policy documents, academic and industry research. While this evidence provides an important overview of the problem, there remains comparatively limited insight into how businesses themselves experience fraud in practice and what forms of support organisations consider most useful when incidents occur.

3.2 To help address this gap, this section presents findings from primary research undertaken as part of this study. The research sought to capture perspectives from within the business community as well as from professionals with expertise in fraud prevention, investigation and business support. Two short surveys were conducted: one targeting individuals with specific responsibilities for fraud prevention, investigation or risk management within organisations, and a second aimed at employees without direct fraud-related roles in order to explore broader levels of awareness and experience of fraud within businesses. These survey findings are complemented by interviews with subject matter experts drawn from relevant professional, industry and policy backgrounds.

3.3 The survey element of the research was exploratory and involved a relatively limited number of responses. Consequently, the findings presented here should not be interpreted as statistically representative of the wider business population. Rather, they provide illustrative insights into current experiences, perceptions and challenges relating to fraud within organisations.

3.4 It is also possible that individuals and organisations who chose to participate in the surveys were those already more engaged with fraud prevention or fraud risk management issues. As a result, respondents may represent businesses that are comparatively more aware of fraud risks and proactive in addressing them. If this is the case, the experiences captured in the survey responses may in fact understate the challenges faced by parts of the wider business community, particularly organisations with more limited awareness or fewer resources dedicated to fraud prevention.

3.5 Despite these limitations, the survey responses and expert interviews provide valuable practical insights into how businesses encounter fraud, how organisations currently respond to incidents and where gaps may exist in available support mechanisms. These perspectives help to contextualise the earlier evidence and inform the development of

recommendations for strengthening support for businesses affected by fraud.

Findings

3.6 This section summarises the key findings emerging from the surveys and expert interviews, highlighting common themes in how businesses experience, manage and respond to fraud. The points below provide an overview of the most significant insights:

- Fraud is recognised as a significant business risk, but awareness is uneven across organisations
- Businesses are exposed to a broad and evolving range of fraud threats
- The impact of fraud extends beyond direct financial loss
- Fraud prevention and preparedness are shaped by organisational culture, training and resources
- Reporting pathways and external support are experienced as uneven and, at times, inadequate
- The need for practical guidance, consistent terminology and better information sharing
- Emerging threats and legal developments are increasing the need for organisational readiness

3.7 These are explored in further detail in the sections that follow.

Fraud risk and awareness

3.8 Across both surveys, fraud was consistently presented as a genuine and significant issue for businesses rather than a remote or exceptional concern. Respondents with fraud-related responsibilities described direct experience of a wide range of fraud types and, in many cases, conveyed a strong awareness of how frequently fraud risks arise in practice. For this group, fraud appeared to be understood as an operational reality requiring ongoing vigilance, internal controls and organisational commitment.

3.9 Among non-fraud personnel, awareness was also generally evident, although it appeared less consistent and less embedded. Many respondents reported feeling confident in identifying suspicious or potentially fraudulent behaviour in their role, and a substantial majority said they knew how to report a suspected fraud within their organisation. Many also reported receiving training or guidance on fraud. However, this broader picture of awareness was qualified by signs of uneven understanding. A notable minority said they had never received fraud training, were unsure whether such training was provided, or were not aware that their organisation had a fraud policy or reporting procedure. This suggests that awareness of fraud is present in many organisations but is not yet universal or equally distributed across the workforce.

3.10 A clear distinction emerged between specialist and non-specialist perspectives. Fraud personnel were more likely to describe fraud as complex, adaptive and difficult to contain fully. Their responses often reflected familiarity with specific typologies, operational weaknesses and external barriers to prevention or enforcement. Non-fraud personnel, by contrast, more often framed fraud in terms of confidence, training exposure and clarity of internal systems. This difference is important because it indicates that organisations may have relatively strong awareness among those closest to fraud risk, while broader understanding among the wider workforce depends heavily on communication, guidance and organisational culture.

3.11 The findings also suggest that confidence should not be taken as an indicator of comprehensive preparedness. Fraud personnel generally reported being somewhat or very confident in their organisation's ability to prevent fraud, and many rated their anti-fraud culture, leadership tone and staff awareness measures relatively positively. Yet the same group also identified major barriers to effective prevention and detection, particularly the complexity of fraud threats, limited resources and gaps in awareness or expertise. The picture that emerges is therefore one of partial confidence rather than complete assurance: organisations may feel they are doing many of the right things, while still recognising that the threat environment is difficult to manage and constantly changing.

3.12 Several responses capture this sense of unevenness particularly well. One respondent noted that, in their organisation, phishing attempts were reported quickly because "*the internal culture is such that they reported it immediately and action was taken before any loss was experienced*". This illustrates how training and culture can translate awareness into action. At the same time, another fraud respondent acknowledged that while those working in risk management have learned the relevant terminology, it "*is confusing for regular businesses*", especially where different sectors use different language. Together, these comments underline a central finding of both surveys: fraud is widely recognised as an important issue, but levels of understanding, confidence and practical readiness remain uneven across different roles and organisations.

3.13 Overall, the surveys suggest that fraud is increasingly seen as a mainstream business risk. However, they also indicate that organisations cannot assume that awareness among specialists automatically translates into organisation-wide understanding. Strengthening resilience is therefore likely to depend not only on technical counter-fraud capability, but also on ensuring that all staff are given clear, accessible and regular information about fraud risks, what they look like in practice and what to do when concerns arise.

Business fraud threats

3.14 The fraud personnel survey suggests that businesses encounter a diverse and expanding range of fraud-related threats. Respondents reported experience of internal fraud, external fraud, cyber-enabled fraud and identity theft, alongside a series of more detailed incidents involving false invoicing, expenses fraud, theft of stock, phishing, ransomware, forged contracts, impersonation of clients or bank staff, grant fraud and business email compromise. These responses indicate that fraud against businesses is not confined to one category of offence and is rarely experienced in isolation. Instead, respondents described a threat landscape that is varied, opportunistic and often blended across traditional fraud, cybercrime and abuse of position.

3.15 The examples provided show that businesses may be affected through both internal and external routes (or a mixture of both through coercion of employees or by planting fake personnel in organisations). Some incidents involved employees or managers abusing trust, such as the collection of client payments that were not remitted, overstatement of expenses, theft of petty cash, failure to bank takings and theft of stock for resale. Others involved external actors using deception, impersonation or cyber compromise to target business processes and relationships. Particularly notable were examples of forged documentation, hacked email accounts, fraudulent grant applications, deepfake impersonation and vendor email compromise leading to misdirected funds. These cases suggest that businesses are vulnerable at multiple points: through staff, systems, communications, supplier relationships and public-facing activity.

3.16 The non-fraud personnel survey supports this broader picture, albeit from a different angle. While that survey was not designed to gather detailed incident data, respondents demonstrated awareness of a wide spectrum of threats, particularly phishing, fraudulent emails, impersonation and social engineering. The types of training and guidance described by respondents also indicate that cyber-enabled fraud has become one of the most visible and commonly communicated areas of risk within many organisations. This may reflect the relative prominence of phishing and cyber awareness training compared with other forms of fraud, especially those involving procurement, internal abuse or more complex financial manipulation.

3.17 A notable theme across the fraud personnel responses is that fraud is seen as increasingly dynamic and adaptive. Several comments highlighted the speed with which fraud methods evolve, particularly through digital channels. One respondent described how an unknown third party destabilised the organisation’s integrated IT system in pursuit of a ransom, resulting in five days of downtime. Others referred to AI

deepfakes of staff contacting customers, hacked emails being used to impersonate clients, and the need to anticipate the intersection between AI, cyber security and fraud. This suggests that businesses are no longer dealing solely with familiar fraud typologies, but with increasingly sophisticated methods that exploit trust, urgency and digital dependence.

3.18 This perception is reinforced by the survey responses on future threats. Fraud personnel expressed particular concern about phishing and social engineering, business email compromise, identity fraud and AI-enabled deception. Concern about insider threats and supply chain fraud was also evident, though slightly less pronounced. By contrast, crypto-related fraud and QR-code fraud appeared to generate more mixed views, perhaps reflecting variation in sector exposure or uncertainty about their relevance to particular organisations. Overall, the pattern suggests that businesses are most concerned about threats that directly exploit routine communication channels, financial authorisation processes and digital identities.

3.19 Importantly, the responses also imply that fraud types should not be treated as discrete and unrelated categories. Several comments described incidents that combined social engineering, cyber compromise and impersonation, while others highlighted the way that fraud may begin in one area and spread into another. One non-fraud respondent, for example, commented that risk types are often dealt with in isolation, whereas "*in reality they are cross-border, always*". Another fraud respondent referred to "*social AI-enhanced engineering*" as a distinct emerging threat. These observations point to the need for organisations to think about fraud in a more integrated way, recognising that fraudsters are likely to exploit the gaps between teams, systems and categories of risk rather than operating within neatly defined boundaries.

3.20 Taken together, the findings suggest that businesses face a broad and evolving mix of fraud threats, combining traditional internal and external misconduct with increasingly sophisticated digital and impersonationbased methods. This has important implications for support provision. Any initiative aimed at helping businesses affected by fraud is likely to be most useful where it recognises the diversity of threats facing organisations and avoids focusing too narrowly on one form of offending at the expense of others.

The impact of fraud on businesses

3.21 The findings of the surveys also indicate that the effects of fraud on businesses reach beyond direct monetary loss. While some respondents reported no financial loss, and others reported comparatively lowervalue losses. The operational and organisational consequences described in the surveys suggest that fraud can have a much wider impact on businesses than financial figures alone might imply. This is particularly

important to note, as headline loss values do not necessarily capture the full burden placed on an organisation when fraud occurs.

3.22 Operational disruption was another important theme. One respondent described a ransomware incident that left systems down for five days, while others referred to downtime, time pressure in restoring systems and the burden of paperwork and court processes following a fraud incident. These comments suggest that the consequences of fraud can include diversion of staff time, interruption to service delivery and cause a strain on core business functions. Even where organisations are able to act quickly and contain losses, the effort involved in responding, investigating and recovering may still be substantial.

3.23 The survey also indicates that the emotional and cultural effects of fraud should not be overlooked. Reduced staff morale was selected by a number of respondents, and some of the comments imply frustration, fatigue and disillusionment in dealing with fraud and its aftermath. In practice, fraud can create anxiety among staff, weaken confidence in systems and processes, and generate a sense of vulnerability or mistrust within the organisation. For smaller organisations in particular, where staffing and resources are limited, the impact of a fraud incident may be felt more acutely because there is less organisational capacity to absorb disruption.

3.24 The non-fraud personnel survey supports this broader understanding, albeit indirectly. Responses around communication, confidence in reporting, and the importance of clear terminology suggest that the way fraud is framed internally can shape whether staff feel able to raise concerns or understand the seriousness of an issue. Some respondents pointed to the risk of behaviour being dismissed as "*a joke or a trick on the organisation*", while others stressed that people do not always realise that certain activities are fraudulent. This suggests that the impact of fraud may be compounded where organisations lack a shared understanding of what fraud is and why it matters, potentially reducing the speed and seriousness of the response.

3.25 One fraud respondent made the broader point that a "*major problem was downtime*", while another emphasised that the challenge lay in restoring all systems quickly in the cloud. These examples illustrate that the practical consequences of fraud often involve urgent operational recovery rather than simply accounting for financial losses after the event. Similarly, some of the strongest criticisms of external support were not only about the fact of fraud itself, but about the organisational effort required to seek help, pursue justice or stabilise systems, while formal responses remained slow or limited.

3.26 Collectively, the findings suggest that fraud should be understood as a business resilience issue as much as a financial one. Direct losses are clearly important, but businesses may also face disruption, stress,

reputational damage, administrative burden and erosion of trust. This has implications for support design. Initiatives aimed at helping businesses affected by fraud are likely to be more effective where they recognise the full range of consequences that organisations may experience, including the practical and organisational pressures associated with response and recovery.

Prevention and preparedness

3.27 A central theme across both surveys is that fraud prevention is not experienced simply as a technical or procedural issue. Rather, respondents consistently linked preparedness to organisational culture, the quality and frequency of training, leadership commitment and the resources available to support prevention and detection activity. These factors appear to shape whether businesses feel able to respond confidently to fraud risk and whether staff understand fraud as part of their everyday responsibilities.

3.28 Among fraud personnel, confidence in organisational ability to prevent fraud was generally positive, and many respondents assessed their antifraud culture, staff training and policies reasonably favourably. Leadership tone and culture set "*from the top*" appeared particularly important, with many respondents indicating that anti-fraud expectations were strongest where they were supported by senior leadership and embedded in organisational values. Several free-text responses reinforced this. One respondent argued that organisations should "*start from the top and talk openly and frequently*", while another stressed that induction training should not be treated as a "*tick-box exercise*". These observations suggest that prevention is seen as most effective where it is active, visible and sustained rather than purely procedural.

3.29 The non-fraud personnel survey supports this conclusion. Most respondents reported that their organisation communicated its stance on fraud and unethical behaviour clearly or somewhat clearly, and a substantial majority said they would feel comfortable reporting a concern. Many also said they had been encouraged, at least occasionally, to speak up. This points to the existence of positive cultures in many organisations. However, these findings were again qualified by evidence of inconsistency. A smaller but still important proportion of respondents said communication was unclear or absent, that they were rarely or never reminded to raise concerns, or that they would feel uncomfortable reporting a potential issue. This suggests that organisational culture can vary significantly, even where formal policies or training exist.

3.30 Training emerged as a particularly important factor in both surveys. Fraud personnel identified staff awareness and training as relevant measures for prevention, while non-fraud respondents frequently called for regular training, better onboarding, practical refreshers and more interactive approaches. There was a clear sense that one-off or minimal training is

unlikely to be sufficient in the face of evolving fraud risks. Respondents wanted training that is engaging, understandable and relevant to the realities of their work rather than generic or compliancedriven. One fraud respondent commented that "*ongoing training that is engaging and not simply delivered as mandatory*" would help prepare organisations for future risks, while a non-fraud respondent called for "*guidance for new starters in an onboarding guide and regular refreshers for existing staff*".

3.31 The role of resources was equally prominent. Fraud personnel identified limited resources and budgets as one of the biggest barriers to effective fraud prevention and detection, alongside the complexity of threats and lack of awareness or expertise. Some comments reflected the practical limits smaller organisations face, including the cost of investing in specialist tools, devoting staff time to fraud prevention activity, or participating in data-sharing schemes. One respondent observed that certain services were "*prohibitive for SMEs*", while another noted that more time and staff were needed to assess new and evolving risks. These findings suggest that even organisations with a positive culture and strong intent may struggle to implement comprehensive prevention measures where resources are constrained.

3.32 The surveys also indicate that preparedness varies by function and control area. Fraud personnel were generally more positive about antifraud culture, training, policies, pre-employment vetting and access to consultancy when required than about proactive data analysis, insurance and some reporting mechanisms. This may suggest that many organisations have developed basic governance structures and staff awareness measures but are less advanced in more specialised forms of prevention and detection, such as analytics, intelligence-led monitoring or dedicated fraud technology. Non-fraud respondents' calls for practical examples, role-specific guidance and clearer reporting routes further support the view that preparedness often depends on translating high-level policies into day-to-day understanding.

3.33 In summary, the findings suggest that fraud prevention is shaped by a combination of leadership, culture, training and practical capacity. Businesses appear more resilient where fraud is discussed openly, staff are trained regularly, reporting is encouraged and expectations are clear. However, these strengths may be undermined where threats are complex, resources are limited or fraud awareness is not embedded consistently across the organisation. This implies that support for businesses should focus not only on formal controls, but also on helping organisations build and sustain an active anti-fraud culture that reaches beyond specialist roles.

Reporting pathways and external support

3.34 The findings from the surveys suggest a notable contrast between internal reporting arrangements and perceptions of external support. Within

organisations, many respondents in the non-fraud personnel survey said they knew how to report a suspected fraud and would feel comfortable doing so. Many also reported that their organisation communicated its stance on fraud clearly and encouraged staff to raise concerns. Although these findings are not uniform, they suggest that internal reporting routes are often more visible and better understood than the wider external landscape of reporting, enforcement and support.

3.35 By contrast, responses from fraud personnel reveal significantly weaker confidence in the usefulness and responsiveness of external help following a fraud incident. Most respondents who had experienced fraud said they had sought some form of external support, including from the former Action Fraud, local police, legal advisers, specialist police units and external consultants. However, the qualitative comments attached to these responses were frequently critical. While a small number of respondents described support as "effective" or "helpful" in securing prosecution, recovery or technical remediation, many others expressed frustration at delays, bureaucracy, limited follow-up and an apparent lack of meaningful action.

3.36 The strongest criticism was directed at national reporting and policing arrangements. Several respondents described the former Action Fraud in highly negative terms, characterising it as a "*black hole*", "*a one way street*" and, in one comment, "*non-action fraud*", however, some were more optimistic about the new Report Fraud body. Local policing was also described by some as disengaged or unlikely to follow up reports.[34]

3.37 The challenge described here appears to be both practical and symbolic. On a practical level, respondents referred to long delays, administrative burdens, lack of expertise and the cost of accessing legal support. In a broader sense, some comments suggested that businesses feel fraud is not taken seriously enough by enforcement bodies, particularly where incidents do not involve very high values or where cyber-enabled and financial harms fall across multiple agencies. One respondent argued that fraud requires a more centralised and authoritative response structure, while another emphasised the need for better signposting for victims of identity fraud. These responses imply that businesses may struggle not only to obtain action, but also to navigate a fragmented support landscape.

3.38 At the same time, some respondents reported using internal expertise or consultants rather than relying heavily on public bodies. This may indicate that organisations with greater resources or specialist capability are more able to manage incidents through in-house functions, legal advisers or technical support. However, such options are unlikely to be equally

[34] These comments should be treated cautiously given the modest sample size and selfselecting nature of the surveys, but they nevertheless point to a strong perception among respondents that the current response system does not always meet business expectations after a fraud incident.

accessible to all businesses, particularly SMEs. The result may be a two-tiered experience in which some organisations can mobilise private support quickly, while others depend more heavily on public reporting systems that are perceived as slow or ineffective.

3.39 The non-fraud personnel survey adds an important complementary perspective. Calls for simpler reporting systems, stronger whistleblowing procedures and dedicated reporting routes indicate that ease of reporting matters not only externally but also internally. One respondent noted that reports currently have to be made to the CFO, which "*can be quite daunting for some staff*". This suggests that even where formal routes exist, perceived seniority, accessibility and confidence in response can shape whether people come forward. In this sense, the issues raised in the two surveys are connected: internal reporting depends on trusted and usable processes, and external reporting depends on confidence that action will follow.

3.40 Taken as a whole, the findings suggest that reporting and support arrangements are inconsistent. Internal systems may be clearer in many organisations than external support routes, but neither can be assumed to be working effectively in all settings. Businesses appear to want reporting mechanisms that are visible, straightforward and responsive, alongside external support that offers meaningful follow-up, practical advice and confidence that fraud incidents will be treated seriously. This has clear implications for any initiative aimed at supporting businesses affected by fraud, particularly in relation to signposting, navigation of available services and managing expectations about what support can realistically be provided. It should be noted that the surveys were carried out prior to the introduction of the UK's Report Fraud service, and has therefore, not been included in this report.

Guidance, terminology and information sharing

3.41 Across both surveys, respondents placed considerable emphasis on the importance of clarity: defining exactly what fraud is, how it differs from related concepts, what organisations are expected to do, and how information can be shared safely and effectively. This theme emerged strongly in relation to terminology, guidance materials and data sharing, and points to a broader need for communication that is accessible, consistent and practically useful.

3.42 Both surveys found a substantial level of concern about confusing or inconsistent fraud-related terminology. Fraud personnel and non-fraud personnel alike reported that language varies across sectors and sources, with overlaps between fraud, cybercrime, corruption, scams and related concepts. Respondents referred to jargon, abbreviations, competing definitions and inconsistency across government, regulators

and professional communities. Some also suggested that the language currently used can minimise the seriousness of fraud or deter people from reporting it. One fraud respondent argued that victims should be treated as victims of crime and that terms such as "*scam*" may undermine the seriousness of what has occurred. Another observed that different sectors "*have their own set of terms, own language*", which creates confusion for regular businesses.

3.43 This matters because terminology is not a merely trivial issue. Respondents in both surveys overwhelmingly considered it important that fraud-related language and definitions are conveyed clearly and consistently. The reasons given were practical as well as conceptual. Clear language was seen as essential for helping staff recognise fraud, understand reporting routes, compare policies and collaborate across sectors. Several respondents linked inconsistency in language to weaker reporting, reduced understanding and opportunities for non-compliance. As one non-fraud respondent put it, "*clear, understandable language communicates more easily and avoids people getting bogged down and giving up*".

3.44 The desire for more practical and accessible guidance was equally evident. In the fraud personnel survey, respondents highlighted the need for practical toolkits, sector-specific information and tailored staff training. In the non-fraud survey, the strongest preferences were for regular alerts and updates on emerging frauds, plain-English case studies, interactive or visual materials, simpler official guidance, glossaries of key terms, role-specific guidance and sector-specific examples. This combination suggests that organisations do not simply want more information; they want information that is easier to use, more relevant to their setting and better aligned with the realities of different roles.

3.45 The survey comments reinforce this point. Fraud personnel noted that much fraud information is too general and that more sector-specific advice would be more useful in training staff. Non-fraud respondents called for tangible examples, storytelling, current-event reporting, onboarding materials and annual refreshers. These responses indicate that practical examples are valued because they help staff connect abstract warnings to real situations. They also suggest that organisations may be more likely to build fraud awareness where guidance is concrete, role-relevant and communicated repeatedly rather than delivered as a one-off exercise.

3.46 Information sharing emerged as a closely related issue. Fraud personnel generally viewed data and information sharing between organisations, and between the public and private sectors, as important for fraud prevention, though opinions on current effectiveness were mixed. The qualitative responses suggest strong support for better collaboration, but also significant frustration with the barriers that currently impede it. These barriers included misunderstanding of data protection rules, uncertainty about the legal basis for sharing, lack of trust, reputational concerns,

confidentiality issues, lack of central leadership and reluctance among organisations to admit they have been victims of fraud.

3.47 One of the strongest comments captured this clearly: "*Without private/public collaboration with regards to data sharing we are making life very difficult for ourselves and missing vital frauds*". Others argued that cross-sector and cross-border information sharing should be a priority because fraudsters do not respect organisational or geographic boundaries. At the same time, respondents repeatedly pointed to fear of reputational damage and confusion about what is legally permissible as major constraints. This suggests that there is both appetite for sharing and uncertainty about how to do it with confidence. The recent call for evidence about economic crime information sharing by the Home Office[35] may start to pave the way to overcome some of these issues.

3.48 Overall, the findings indicate that clarity, practicality and communication are central to fraud resilience. Businesses appear to want simpler language, more usable guidance and more confident information sharing, not as abstract improvements, but as means of enabling recognition, reporting, prevention and collaboration. This implies that support for businesses should include not only expert advice after incidents, but also accessible materials, shared language and clearer frameworks for lawful and effective data sharing.

Emerging threats and legal developments

3.49 The final theme running across the surveys is the extent to which businesses are trying to adapt to an environment shaped by both evolving fraud threats and changing legal expectations. Respondents with fraud responsibilities expressed clear concern about the future direction of fraud risk, especially in relation to technologically enabled methods. At the same time, the non-fraud survey suggests that awareness of recent legal developments, including the ECTA, is uneven outside specialist roles. While the FTPF offence applies only to a relatively small subset of larger organisations at present, the broader principles it reflects, strong governance, clear accountability and effective controls, are relevant to organisations of all sizes. Together, these findings point to a growing need for organisations to strengthen their forward-looking approach to fraud risk.

3.50 Fraud personnel responses indicate particular concern about phishing, social engineering, business email compromise, identity fraud and in particular AI-enabled deception and the use of deepfakes. These concerns align with the broader pattern in the incident data, where respondents described impersonation, hacked communications,

[35] https://www.gov.uk/government/calls-for-evidence/economic-crime-informationsharing/economic-crime-information-sharing-accessible

deepfake activity and ransomware as part of the current threat picture. There was a clear sense that fraud is becoming harder to detect because it increasingly exploits routine business communications, trusted identities and the speed of digital transactions. Several respondents referred explicitly to the need to understand the relationship between fraud, cyber security and AI, and to prepare for risks that are likely to become more sophisticated over time.

3.51 Although many fraud personnel considered their organisation somewhat or very prepared for new and evolving fraud tactics, the qualitative responses again suggest that this preparedness is qualified rather than absolute. Respondents referred to the use of phishing simulations, multifactor authentication, password controls, encrypted back-ups, verification processes, staff training and participation in various fraud networks. These are important signs of proactive thinking. However, respondents also identified additional support needs, including more security staff, additional software, ongoing engaging training, better notification of new fraud types, more time to assess emerging risks and mechanisms for sharing best practice. This implies that many organisations see future readiness as an ongoing process rather than a settled position.

3.52 The non-fraud survey introduces an additional dimension by highlighting uneven awareness of legal change. Almost half of respondents had not heard of the ECTA, and only a minority reported both awareness and understanding of how it applied to them. Awareness of FTPF requirements were somewhat stronger, but a substantial proportion of respondents were still unaware of it. When asked whether their organisation had communicated these legal requirements effectively, only a minority answered positively, while many said they were unaware of the requirements or felt communication had been ineffective. These findings suggest that significant parts of the workforce may not yet understand the implications of new fraud-related legislation for organisational governance and responsibility.

3.53 This gap matters because legal change is likely to affect organisations most effectively where it is translated into clear internal expectations, responsibilities and training. If awareness remains concentrated among legal, compliance or fraud specialists, the wider organisation may not fully understand why certain controls are changing or what new responsibilities mean in practice. The broader findings of the non-fraud survey reinforce this point, with respondents calling for clearer explanations, simpler guidance and examples that make fraud risks and responsibilities easier to understand.

3.54 When considered together, the findings suggest that organisational readiness now has two dimensions. The first is operational: the capacity

to anticipate and respond to new fraud methods, especially those enabled by digital technologies and AI. The second is institutional: the ability to understand and implement changing legal expectations in a way that reaches beyond specialist teams. Businesses appear to recognise the growing sophistication of fraud threats but may be less consistent in how far they have embedded awareness of the changing regulatory environment across the organisation.

.

Conclusion

3.55 Viewed together, the two surveys provide a useful, if indicative, picture of how fraud is currently experienced and understood within businesses. The findings suggest that fraud is widely recognised as a significant and evolving threat, but that awareness, preparedness and confidence vary across roles and organisations. Fraud specialists tend to view the issue as complex, resource-intensive and shaped by rapidly changing methods, while non-specialist staff often show broad awareness but identify a need for clearer language, more practical guidance and stronger communication.

3.56 The surveys also point to several consistent priorities. Businesses appear to value strong organisational culture, regular and relevant training, clear reporting mechanisms, practical examples and better access to timely support. There is also a strong sense that current arrangements for external reporting and follow-up do not always meet business needs, and that better information sharing, clearer terminology and stronger coordination would improve prevention and response.

3.57 These findings should be interpreted cautiously given the limited sample sizes involved. Nevertheless, they offer important insight into the lived experience of fraud within organisations and highlight areas where support initiatives may be most beneficial. In particular, they suggest that support for businesses affected by fraud is likely to be most effective where it combines practical prevention advice, clear communication, accessible reporting pathways and responsive post-incident assistance.

Section 4. Summary and implications for the Business Fraud Alliance initiative

Key findings

4.1 This report has examined fraud against businesses from three connected angles: the wider evidence on the scale and nature of the threat, the practical perspectives of businesses and specialists, and the implications of those findings for the design of a business fraud initiative. Taken together, these strands point to a clear overall conclusion. Fraud is now a

routine feature of the business risk environment rather than a marginal or exceptional issue. It affects organisations of different sizes and sectors, is increasingly enabled by digital systems and social engineering, and can impose significant operational, financial and organisational strain even where direct losses are limited. At the same time, the support landscape available to businesses remains uneven, fragmented and often difficult to navigate, particularly for smaller firms and for organisations outside sectors with mature fraud prevention infrastructures.

4.2 The central finding is that the current state of business fraud is characterised by normalisation, complexity and uneven resilience. Fraud is no longer experienced as a rare event. National and international evidence suggests that a substantial proportion of businesses encounter fraud, while the primary research undertaken for this study shows that many organisations view it as an established and evolving operational reality. Businesses are not facing a single, stable category of threat. Instead, they are dealing with a broad mix of internal fraud, external deception, cyber-enabled offending, impersonation, payment diversion, supplier fraud, identity misuse and increasingly sophisticated AI-enabled attacks. These frauds do not sit neatly in separate boxes. They frequently overlap, moving across finance, cyber security, procurement, communications and leadership functions, and exploiting the spaces between them.

4.3 This matters because the impact of fraud on businesses is wider than direct financial loss alone. Across both the literature and the business and expert perspectives, fraud emerges as a resilience issue as much as a financial crime issue. The consequences described include operational downtime, diverted staff time, reputational damage, legal and administrative burdens, reduced morale, weakened trust in systems and pressure on leadership teams. For some organisations, especially SMEs, even a modest fraud loss may have a disproportionate effect where margins are tight, internal capacity is limited and recovery support is hard to access. This broadens the rationale for support. Businesses do not only need help to prevent fraud; they also need support to absorb, respond to and recover from it.

4.4 A second major finding is that business capability to deal with fraud is highly uneven. Larger organisations, and businesses in sectors such as financial services and insurance, are more likely to benefit from specialist staff, established controls, intelligence-sharing arrangements and stronger external networks. By contrast, many SMEs and businesses in less organised sectors appear to rely on a narrower set of internal resources, more limited expertise and less access to structured support. The research with businesses reinforces this point. Fraud specialists often described their organisations as reasonably confident in their controls, but that confidence was qualified by concerns about resource constraints, the pace of threat evolution and the difficulty of keeping the wider workforce engaged and informed. Among non-specialists, awareness was often

present but inconsistent, with gaps in training, policy awareness and understanding of emerging legal and fraud issues. The overall picture is therefore not one of absence of effort, but of patchy readiness.

4.5 That unevenness is also evident in the way businesses experience support. One of the clearest themes in the research is the contrast between internal arrangements and external pathways. Within organisations, many respondents said they knew how to report concerns and felt able to do so, although this too was not universal. Outside the organisation, however, views were much less positive. Businesses described a landscape in which reporting routes, support services, enforcement bodies, intelligence organisations and advisers all exist, but where the overall system can feel confusing, slow and poorly connected. For businesses that have experienced fraud, the issue is not simply whether some support exists somewhere; it is whether that support is visible, accessible, timely and practically useful at the point of need. The evidence gathered here suggests that this is often not the case.

Implications for the initiative

4.6 Collectively, these findings have clear implications for the design and focus of a business fraud support initiative. They suggest that fraud represents not only a law enforcement challenge, but also a systemic operational risk for organisations across the UK economy, requiring a response that is embedded in business practice as well as policy frameworks.

4.7 First, the scale and prevalence of fraud affecting businesses means that any initiative should treat fraud as a routine organisational risk rather than an exceptional event. Businesses therefore require support that strengthens their ability to prevent, detect and respond to fraud as part of core risk management, rather than relying solely on external enforcement.

4.8 Second, the nature of fraud affecting businesses is evolving rapidly, driven by digitalisation and technological change. Online platforms,
digital communications and the growing use of artificial intelligence are enabling fraud to be conducted at greater scale, speed and sophistication. This creates an ongoing requirement for businesses to access timely intelligence, practical guidance and up-to-date support in order to respond effectively to emerging threats.

4.9 Third, while fraud risks and organisational capabilities vary across the business population, exposure to fraud is widespread. This implies that support should not be narrowly targeted at a single segment but designed to be accessible and relevant across organisations with differing levels of capability, sectoral exposure and access to specialist expertise.

4.10 Fourth, although the UK has developed an extensive policy and institutional framework to address fraud, the updated fraud strategy places greater

responsibility on organisations to prevent fraud within their systems and services. However, this increased expectation is not fully matched by equivalent, coordinated support mechanisms for businesses experiencing fraud.

4.11 From a business perspective, the current landscape therefore remains difficult to navigate. While numerous organisations contribute to prevention, intelligence sharing and enforcement, there is limited evidence of a clear, end-to-end support pathway following a fraud incident. In practice, businesses may face challenges in identifying appropriate points of contact, navigating reporting and response processes, and accessing practical guidance on containment, recovery and future prevention.

4.12 Overall, these implications suggest a clear role for an initiative designed to bridge the gap between policy expectations and practical support for businesses. In particular, a business-focused fraud support initiative should prioritise providing a clear entry point for support, simplifying navigation of the existing landscape, offering practical operational guidance on response and recovery, facilitating coordination between relevant actors, and supporting organisations in translating prevention expectations into effective practice.

Drawing up the recommendations

4.13 There is a key reason why the recommendations in this report take the shape they do. They do not begin from the assumption that there is little activity or policy attention directed at fraud affecting businesses. The UK Government's latest fraud strategy explicitly recognises that businesses are significant victims of fraud, noting that around one in four UK businesses with employees experience fraud each year. Alongside this, the strategy outlines a range of system-level responses, including reforms to Companies House, enhanced cyber resilience support, expanded awareness campaigns and new corporate accountability measures such as the FTPF offence.

4.14 Building on this policy context, the recommendations in this report focus more directly on the practical support needs of businesses. They address the operational challenges organisations face in understanding fraud risks, strengthening internal resilience, navigating reporting pathways and accessing meaningful support following an incident.

4.15 The shorter-term recommendations are shaped by what appears most immediately missing from the current landscape: clarity, accessibility and practical help. The evidence suggests that many businesses need simpler and more consistent fraud language, clearer internal communications materials, more visible leadership ownership of fraud risk and more usable guidance on specific high-risk scenarios such as payment

diversion, executive impersonation and AI-enabled deception. The recommendation to develop reusable briefing materials, terminology guides, webinars, AI-focused alerts and practical communications packs arises directly from the finding that awareness is present but uneven, and that businesses respond best to information that is plain, rolerelevant and easy to apply.

4.16 The emphasis on simplified minimum standards and SME-facing toolkits follows from the report's finding that smaller businesses face the sharpest capability gap. For many of these organisations, the barrier is not lack of concern but lack of capacity, time and specialist knowledge. Recommendations on basic controls, fraud risk assessment, accessible reporting routes, insider risk management and third-party fraud safeguards are therefore designed to translate a complex threat picture into manageable and proportionate steps. They reflect the reality that many businesses need help with foundational resilience before they can engage with more advanced approaches.

4.17 Similarly, the recommendations on reporting, incident response and recovery stem directly from the evidence that businesses often find external support fragmented and unsatisfactory after fraud has occurred. Guidance on how and when to report, what to do in the first 72 hours, where to seek different forms of help and how to think about recovery options responds to a recurring finding in the research: businesses want practical navigation and realistic support, not just exhortations to report. The proposal for a support directory and clearer referral pathways reflects the strong sense that the current landscape is difficult to understand from the user's perspective.

4.18 The longer-term recommendations reflect a related but distinct need to build a more durable business fraud support infrastructure. The report shows that fraud is not static and that one-off awareness activity will not be sufficient. Emerging threats, especially AI-enabled impersonation and blended cyber-fraud techniques, mean that organisations will require regular updates, stronger governance, improved detection capability and more mature internal cultures over time. The recommendations therefore extend beyond awareness materials to include modular training, professional development, fraud maturity tools, scenario exercises and more developed guidance for boards and senior leaders.

4.19 The longer-term focus on sector engagement and coordination also follows directly from the evidence. Support ecosystems are more developed in some sectors than others, leaving gaps elsewhere. Recommendations on mapping sector networks, developing sectorspecific materials and encouraging sector-based resilience structures are intended to reduce these inequalities while recognising that businesses experience fraud in sector-specific ways.

4.20 Finally, the recommendation to strengthen coordination across the wider fraud ecosystem responds to one of the most consistent cross-cutting findings in the report: fragmentation remains a significant practical barrier. Stronger public–private coordination, improved information sharing, clearer interpretation of data-sharing rules and more consistent signposting would help address the cross-boundary nature of fraud as experienced by businesses.

4.21 Overall, the recommendations should be understood as a staged response to the current state of business fraud. In the shorter term, the priority is to make the landscape more understandable and usable through clearer materials, minimum standards and practical response guidance. In the longer term, the priority is to build stronger and more consistent organisational capability through training, diagnostics, sector engagement and improved coordination.

4.22 Viewed in this way, the role of the initiative is not to add another layer of activity to an already crowded field, but to make the existing landscape more coherent, accessible and effective for businesses, particularly those least well served by current arrangements.

Section 5. Recommendations

1. Improve fraud awareness and understanding

Shorter-term actions

- **Promote clear organisational accountability for fraud risk management**
  Encourage organisations to establish clear ownership of fraud risk at senior leadership level, including defined governance arrangements, designated responsible roles and appropriate reporting to boards or relevant committees. Guidance should emphasise the importance of integrating fraud risk oversight into existing governance and risk management structures.

- **Develop reusable internal fraud briefing materials**
  Develop concise, reusable briefing materials that organisations can use internally to explain fraud risks, legal obligations, warning signs and reporting expectations to non-specialist staff. These should be suitable for inductions, team briefings and refresher use.

- **Create a standard fraud terminology guide**
  Create and publish a fraud terminology guide in plain English clearly distinguishing commonly confused concepts such as fraud, scams, cyberenabled fraud, corruption and non-financial fraud.

- **Develop practical fraud awareness videos for businesses** Create short practical awareness recorded briefings aimed at business

audiences highlighting emerging fraud risks and immediate actions organisations can take.

- **Produce briefing materials on AI-enabled fraud risks**
  Produce concise materials explaining how generative AI, deepfakes and synthetic identities may be used in fraud attempts and what immediate controls organisations should consider.

- **Promote the treatment of fraud as a business resilience risk** Provide clear guidance encouraging organisations to treat fraud as a business resilience issue, recognising impacts such as operational disruption, reputational damage, staff pressure and recovery effort alongside financial loss, and to consider the role of fraud insurance as part of their overall risk management approach.

Longer-term actions

- **Develop baseline fraud awareness training for all staff** Develop modular training using short e-learning modules, videos or interactive content (including ‘escape room’ type scenarios) focused on real-world scenarios, emerging fraud risks and clear reporting routes.

Develop professional development resources for fraud personnel
Create enhanced learning resources addressing emerging risks such as cyber-enabled fraud, AI-enabled deception, investigation governance and detection techniques.

- **Provide guidance on effective fraud communication within organisations**
  Develop guidance explaining how organisations can embed fraud awareness into onboarding, determine appropriate reminder frequencies and tailor messaging for different audiences.

- **Provide board and senior leadership briefing resources on fraud risk**
  Develop materials to help leadership teams understand fraud threats, governance expectations and their role in overseeing fraud risk management, including clarifying the responsibilities of boards and relevant committees (such as risk or audit committees) in providing effective oversight.

- **Provide regular business fraud threat updates and typology briefings**
  Develop periodic briefings summarising emerging fraud patterns, common attack methods and evolving risks affecting businesses. These updates should highlight practical prevention measures and be accessible to organisations without specialist fraud expertise.

2. Bolster prevention and internal controls

Shorter-term actions

- **Publish guidance on the Failure to Prevent Fraud offence**.
  Provide clear, practical guidance on the FTPF offence under the ECTA for organisations to which it applies, explaining what reasonable procedures may look like in practice and how they can be evidenced, while encouraging organisations not currently in scope to adopt similar good practice principles.

- **Provide ready-to-use internal fraud communications packs** Develop communication packs including templates, intranet text, posters, stickers, digital graphics and short briefing materials to help organisations improve the visibility of fraud policies, reporting routes and whistleblowing arrangements.

- **Provide simplified minimum fraud prevention standards for smaller organisations**
  Develop a concise set of minimum fraud prevention practices aimed at micro and small organisations, focusing on a small number of essential controls such as payment verification, basic supplier checks, separation of duties/financial responsibilities and clear reporting routes.

•

• **Develop a basic fraud resilience toolkit for SMEs**
  Create a practical toolkit focused on simple, affordable and high-impact measures such as payment verification procedures, supplier due diligence checks, clear escalation routes and minimum internal controls, alongside guidance on the use of modern tools such as transaction monitoring, anomaly detection, data analytics and secure digital reporting channels.

• **Publish guidance for handling high-risk financial requests**
  Provide practical guidance covering urgent payment requests, bank detail changes or instructions appearing to come from senior executives, recognising the growing risk of AI-enabled impersonation and deepfake fraud.

• **Encourage organisations to review internal fraud reporting arrangements**
  Encourage organisations to review whether internal reporting routes are genuinely accessible and trusted in practice, ensuring staff can raise concerns easily and without unnecessary barriers, including obstacles linked to hierarchy or seniority.

• **Provide practical guidance on conducting organisational fraud risk assessments**
  Develop clear, practical guidance helping organisations identify and assess their exposure to fraud risks across key areas such as payments, procurement, third-party relationships, customer interactions and digital channels. The guidance should explain how organisations can prioritise risks, document assessments and link findings to proportionate prevention and control measures.

• **Provide guidance on managing insider fraud risks**
  Develop practical guidance helping organisations understand and manage risks arising from insider fraud, including conflicts of interest, abuse of access privileges, procurement manipulation and collusion with external parties. Guidance should highlight preventative measures such as segregation of duties, monitoring of high-risk activities and strong governance over privileged access.

• **Provide guidance on managing fraud risks in third-party relationships**
  Develop practical guidance to help organisations assess and manage fraud risks linked to suppliers, agents and partners, including verification controls, payment safeguards, proportionate due diligence and appropriate contractual protections.

Longer-term actions

- **Support organisations in strengthening fraud detection capabilities**
  Provide guidance on good practice in using data analytics and continuous monitoring to detect and prevent fraud, alongside improving coordination between fraud, cyber, audit and risk functions.

  Develop fraud resilience diagnostic tools and self-assessment frameworks
  Develop practical tools to help organisations assess the maturity of their approach to fraud risk, including levels of staff awareness, training coverage, reporting arrangements, governance and overall organisational resilience, and to identify areas where further improvement may be needed.

- **Develop tiered fraud guidance for organisations of different sizes**
  Develop guidance and support offers tailored to micro, small, medium and large organisations recognising differences in capability, resources and governance structures, in consultation with any other relevant support organisations.

3. Enhance fraud response and recovery

Shorter-term actions

- **Improve clarity and confidence around reporting business fraud**
  Develop clear guidance explaining how and when businesses should report fraud incidents, including the roles of national reporting bodies, law enforcement, financial institutions and regulators. The guidance should help organisations understand reporting pathways, the benefits of reporting and how information provided may contribute to disruption and prevention efforts.

- **Develop practical guidance on responding to fraud incidents** Produce clear guidance outlining the immediate steps organisations should take following a fraud incident, including actions in the first 72 hours, preserving evidence, contacting banks or payment providers, considering legal and insurance issues, reporting incidents and preventing further loss.

- **Create a directory of fraud support and reporting organisations**
  Develop a simple, clear and accessible guide showing where businesses can seek help for different types of fraud-related support, distinguishing between reporting bodies, law enforcement, intelligence-sharing organisations, cyber support services, professional advisers and victim support organisations (the table in Appendix B can be used to further this).

- **Provide guidance on financial recovery following fraud incidents**
  Develop practical guidance explaining the options available to organisations seeking to recover losses following fraud, including engaging with banks and payment providers, freezing or tracing funds, considering

- civil recovery options and making use of insurance or legal remedies where appropriate.

Longer-term actions

- **Develop template fraud incident response and recovery plans** Develop practical templates including checklists covering containment, communications, evidence preservation, external reporting and organisational recovery.

- **Provide templates for post-incident fraud reviews** Provide guidance and templates to help organisations identify root causes, control weaknesses and lessons learned following fraud incidents.

- **Develop fraud scenario exercises and tabletop materials** Create practical exercises covering emerging risks such as AI-enabled impersonation, cyber-enabled fraud and social engineering attacks. This could include virtual or in-person 'escape room'-type scenarios.

4. Expand sector engagement and capability

Longer-term actions

Develop sector-specific fraud guidance and case studies for underrepresented sectors

Identify under-represented sectors not traditionally included in fraud policy discussions or consultations and develop role-specific case examples and practical guidance illustrating how fraud risks arise across operational, finance, customer-facing, IT and leadership roles.

- **Map existing sector support networks and engagement channels** Identify sector-based business networks, professional forums and intelligence-sharing groups that could support improved fraud awareness and resilience. Use this mapping to identify sectors with limited engagement and opportunities to introduce fraud prevention, informationsharing and support through existing networks.

5. Strengthen coordination and the wider fraud ecosystem

Actions involving wider collaboration

- **Support improved cross-sector sharing of fraud intelligence and lessons learned**
  Encourage and facilitate the sharing of fraud typologies, control failures and emerging risks across sectors, building on existing information-sharing networks and initiatives where possible.

- **Provide guidance on lawful and confident fraud information sharing**
  Develop or signpost to practical guidance addressing common misunderstandings around data protection, confidentiality and cross-sector collaboration.

  Establish a structured fraud support referral and signposting model
  Develop a model helping businesses navigate the fraud support landscape by linking organisations to appropriate reporting bodies, advisers and sector networks.

- **Work with partners to improve consistency in fraud terminology and messaging**
  Work with regulators, government and industry partners to improve consistency in fraud terminology and messaging across campaigns, guidance and regulatory communications.

- **Encourage the development of sector-based fraud resilience networks**
  Promote collaborative fraud prevention structures, particularly in sectors where such networks are less mature.

- **Strengthen public–private coordination on business fraud** Promote improved coordination between reporting bodies, law enforcement, regulators and support organisations to reduce fragmentation in the fraud response landscape.

- **Develop a stronger evidence base on business fraud**
  Support periodic measurement of business fraud experiences, reporting behaviours and recovery outcomes to inform future policy and support initiatives.

•

Appendix A – Top ten frauds against businesses

Insider fraud

Fraud may also be committed by employees or other individuals with legitimate access to organisational systems. This includes not only opportunistic internal misconduct, but also cases where employees are coerced or blackmailed into facilitating fraud, as well as instances where individuals are deliberately placed within organisations to enable fraudulent activity. Insider fraud can involve the theft of company funds, manipulation of financial records, misuse of company resources or the disclosure of confidential information. According to the ACFE's Report to the Nations, occupational fraud frequently involves employees exploiting internal knowledge of organisational processes and control systems. Insider-enabled fraud can be particularly difficult to detect, especially where perpetrators understand internal governance structures and control weaknesses.

Payment diversion/ invoice fraud

Payment diversion fraud, sometimes referred to as invoice fraud or mandate fraud, involves criminals impersonating suppliers or company executives in order to redirect legitimate payments to fraudulent bank accounts. In many cases fraudsters monitor or imitate email communications between businesses and their suppliers before requesting that payment details be amended. The increasing reliance on digital communications in commercial transactions has contributed to the growth of this fraud type. Fraudsters are often able to gather information about businesses through publicly available sources, enabling them to craft highly convincing fraudulent requests.

Business email compromise

Business email compromise (BEC) is a closely related form of fraud in which criminals gain access to, or convincingly impersonate, corporate email accounts in order to request fraudulent payments or sensitive information. These attacks often rely on social engineering techniques designed to exploit organisational hierarchies or urgency in financial decision-making. For example, fraudsters may impersonate senior executives and request urgent payments or confidential financial information from employees responsible for financial transactions. Industry studies consistently identify business email compromise as one of the most significant fraud risks facing organisations due to the widespread reliance on electronic communication for financial transactions.

AI-enabled and deepfake fraud

AI-enabled fraud refers to the use of artificial intelligence technologies to facilitate or enhance fraudulent activity. This includes the generation of highly convincing text, audio and visual content designed to impersonate real

individuals or automate large-scale fraud campaigns. One emerging risk is the use of deepfake technology to replicate the voice or likeness of senior executives or trusted contacts. This can be used to support payment diversion fraud or to bypass internal verification processes, particularly where

organisations rely on voice or video communication. Industry reporting indicates that these techniques are becoming more accessible and more difficult to detect, increasing the risk that businesses may be exposed to highly sophisticated impersonation attacks that exploit trust in digital communications.

Cyber-enabled fraud

Many fraud schemes affecting businesses are now facilitated by cybercrime techniques. These include phishing campaigns, malware attacks, credential theft and unauthorised access to organisational systems or financial accounts. The digitalisation of business operations has expanded the opportunities for fraudsters to exploit vulnerabilities in corporate systems. Remote working, cloud-based services and online financial platforms have increased the potential attack surface for organisations. Research suggests that cyberenabled fraud is becoming increasingly sophisticated, with criminals often combining technical attacks with social engineering techniques in order to bypass organisational security controls.

Data and intellectual property theft

Data and intellectual property theft involves the unauthorised access, extraction or misuse of sensitive business information, including customer data, financial records, trade secrets and proprietary technology. This type of fraud may be carried out by external attackers or by insiders with legitimate access to systems. In some cases, stolen data is used directly for financial gain, while in others it may be sold, used to facilitate further fraud or exploited for competitive advantage. The increasing value of data and the growing interconnectivity of business systems have made organisations more vulnerable to such activity, particularly where data governance and access controls are not sufficiently robust.

Identity and business impersonation fraud

Identity fraud involving businesses occurs when criminals impersonate legitimate companies, directors or employees in order to obtain goods, services or credit. This may involve the creation of fraudulent companies, the misuse of legitimate business identities or the use of stolen personal information. Data from fraud prevention organisations indicates that identity fraud remains the most prevalent type of fraud recorded within the UK. Cifas reported almost 250,000 cases of identity fraud in 2024, representing the majority of cases recorded by its members. The increasing availability of compromised personal and organisational data has contributed to the growth of identity-based fraud schemes, allowing criminals to create convincing fraudulent identities or impersonate legitimate organisations.

Account takeover fraud

Account takeover fraud occurs where criminals gain unauthorised access to business bank accounts or financial systems, typically through the use of stolen credentials, phishing attacks or malware. Once access has been obtained, fraudsters may initiate unauthorised payments, alter account details or use the compromised account to facilitate further fraudulent activity. In some cases,

access may be maintained over a period of time in order to avoid detection. The increasing use of online banking and digital financial platforms has contributed to the growth of this fraud type, particularly where authentication controls are weak or where compromised credentials are reused across systems.

Procurement and supplier fraud

Procurement fraud involves the manipulation of purchasing processes in order to divert organisational funds. Examples include the creation of fictitious suppliers, submission of inflated invoices or collusion between employees and external suppliers. Research from the ACFE identifies procurement and billing schemes as among the most common forms of occupational fraud affecting organisations. These schemes often exploit weaknesses in procurement oversight and internal financial controls.

Goods and services fraud

Goods and services fraud involves the acquisition of goods or services without payment, or with no intention of paying. This may include the use of false identities, fraudulent payment details or the exploitation of credit arrangements. Businesses may be targeted through online ordering systems, trade credit arrangements or supply chains, particularly where verification processes are limited or where transactions are conducted remotely. Research suggests that this type of fraud is often underreported, but can result in significant financial losses, particularly for small and medium-sized enterprises that may have fewer resources to absorb such impacts.

Appendix B – Business fraud supporting organisations

Organisation	Who	Area	Details	Type	Contact and further information
Anti-Fraud Forum	All	Int'l	Insolvency and asset recovery	Networking, education and best practice	https://www.insol-europe.org/antifraudforum-introduction-and-members
British Chambers of Commerce (BCC)	All	UK national & local chambers	Coordinate intelligence sharing, produce guidance.	Guidance, support, and advocacy	https://www.britishchambers.org.uk/
British Retail Consortium (BRC)	Retail sector	National	Represents retailers; fraud & crime insights	Policy, guidance and advocacy	https://brc.org.uk/
Businesses Against Scams (BAS)	All	National	Part of Friends Against Scams but for businesses. Set up by Trading Stds.	Network, support and education	https://www.friendsagainstscams.org.uk/businesses-against-scams
Business Crime Reduction Partnerships (BCRPs)	All	Local	Business-led crime reduction initiatives for members.	Intelligence sharing and enforcement	https://nbcc.police.uk/partnerships/business-crime-reduction-partnerships-bcrp
Cifas	All	National	Fraud prevention database and intelligence	Data sharing, education, research and awareness	https://www.cifas.org.uk/

City of London Police (CoLP)	All	National	National policing lead for fraud	Enforcement, guidance, research and awareness	https://www.cityoflondon.police.uk/
Crimestoppers	All	National	Individuals and businesses can report crimes which will be passed onto law enforcement	Reporting, advice and campaigns	https://crimestoppers-uk.org/

Organisation	Who	Area	Details	Type	Contact and further information
Cyber Aware	All	National	Public awareness campaign on cyber fraud	Advice and tools	https://www.ncsc.gov.uk/cyberaware/home
Cyber Resilience Partnerships	SMEs / other organ's	Regional	Support businesses with cyber resilience	Advice, intelligence, support and training	https://www.gov.uk/government/collections/cyber-resilience
Eastern Fraud Forum	All	Regional	Fraud awareness, collaboration and networking	Networking and events	https://www.easternfraudforum.co.uk/
Federation of Small Businesses (FSB)	SMEs	National	Membership with business support including fraud guidance.	Support, advice and campaigns	https://www.fsb.org.uk/
Fraud Advisory Panel	All	Int'l	Champions best practice in the prevention, detection, and deterrence of fraud	Education, collaboration and research	https://www.fraudadvisorypanel.org/
Fraud Prevention Network (FPN)	Fin'l	National	Fraud prevention credit professionals network	Networking and events	https://o2clab.com/forums/
Get Safe Online	All	National	Online safety and fraud prevention	Advice, tools and alerts	https://www.getsafeonline.org/

Global Anti Scam Alliance (GASA)	All	Int'l	Global collaboration against scams	Advice, advocacy and events	https://gasa.org/
Institute of Chartered Accountants in England and Wales (ICAEW)	All	National	Guidance on financial fraud for members	Training, advice and support	https://www.icaew.com/
Isle of Wight Against Scams Partnership (IWASP)	All	Regional	Scam awareness	Awareness and support	https://www.iow.gov.uk/article/1955/IWASP-Isle-of-Wight-Against-ScamsPartnership

Organisation	Who	Area	Details	Type	Contact and further information
Joint Money Laundering Intelligence Task Force (JMLIT)	Fin' l sector	National	Intelligence sharing between banks & law enforcement	Intelligence	https://www.nationalcrimeagency.gov.uk/what-we-do/national-economic-crimecentre
London Fraud Forum	All	Regional	Fraud awareness, collaboration and networking	Networking and events	https://www.londonfraudforum.co.uk/
Midlands Fraud Forum	All	Regional	Fraud awareness, collaboration and networking	Networking and events	https://www.midlandsfraudforum.co.uk/

National Association of Business Crime Partnerships (NABCP)	Retail	National	bringing together local crime partnerships to reduce crime affecting commercial areas	Representation, support, intelligence and advice	https://www.nabcp.com/
National Vehicle Crime Intelligence Service (NaVCIS)	Motor and fin'l sectors	National	Helps identify fraud or vehicle-related criminal activity	Data and analytics	https://navcis.police.uk/
National Business Crime Centre (NBCC)	All	National	Police-led business crime support	Guidance, intelligence, coordination	https://nbcc.police.uk/
National Crime Agency (NCA)	All	National	Serious and organised crime including fraud	Enforcement, intelligence, campaigns	https://www.nationalcrimeagency.gov.uk/
National Cyber Security Centre (NCSC)	All	National	Cyber security guidance	Advice, alerts, toolkits and guidance	https://www.ncsc.gov.uk/
National Economic Crime Centre (NECC)	All	National	Coordinates economic crime response	Intelligence, strategy and national priorities	https://www.nationalcrimeagency.gov.uk/what-we-do/national-economic-crimecentre
National Hunter	Fin' l sector	National	Application fraud detection systems for members	Data sharing	https://nhunter.co.uk/

Organisation	Who	Area	Details	Type	Contact and further information
Norfolk Against Scams Partnership (NASP)	All	Regional	Scam awareness for businesses	Support and campaigns	https://www.norfolk.gov.uk/

North East Cyber Resilience Centre	SMEs	Regional	Cyber support	Support, education, cyber services	https://www.nebrcentre.co.uk/
North West Fraud Forum	All	Regional	Fraud awareness, collaboration and networking	Networking and events	https://www.northwestfraudforum.co.uk/
Northern Ireland Fraud Forum	All	Regional	Fraud awareness, collaboration and networking	Networking and events	https://www.nifraudforum.co.uk/
Online Fraud Steering Group (OFSG)	All	National	Coordinates industry and government efforts to tackle online fraud and improve prevention efforts	Awareness, education and advocacy	https://www.techuk.org/
Report Fraud	All	National	National reporting service for fraud and cybercrime	Reporting, guidance and intelligence sharing	https://www.reportfraud.police.uk/
ROCUs	All	Regional	Tackle organised crime and fraud affecting businesses, particularly where it complex or spans borders.	Enforcement, disruption, intelligence and support.	https://www.rocu.police.uk/
Scottish Scams Strategic Partnership	All	Regional	National scams strategy	Coordination, prevention, enforcement	https://www.gov.scot/groups/scottishscams-strategic-partnership/
South West Fraud Forum (SWFF)	All	Regional	Fraud awareness, collaboration and networking	Networking and events	https://swff.org.uk/

Organisation	Who	Area	Details	Type	Contact and further information

South West London Fraud Partnership (SWLFP)	All	Regional	Shared service undertaking fraud investigation work for SW London Boroughs	Intelligence sharing, support and networking	https://swlfp.org.uk/
Telecommunications UK Fraud Forum (TUFF)	Telecom sector	National	SAFO. Members can share intelligence and experience of communication abuse	Intelligence sharing, support and events	https://www.tuff.co.uk/
Trading Standards	All	National & local	Consumer protection including frauds and scams	Enforcement and advice	https://www.nationaltradingstandards.uk/
UK Finance	Fin'l sector	National	Banking & finance fraud prevention for members	Guidance, education, intelligence and events	https://www.ukfinance.org.uk/
UK Identity Fraud Advisory (UKIFA)	All	National	Helps businesses to identify fake identity documents.	Guidance	https://www.ukifa.co.uk/
Wales Fraud Forum	All	Regional	Fraud awareness, collaboration and networking	Networking and events	https://fraudforum.wales/

* Note that this table is not exhaustive and some organisations that support organisations with business fraud may not be listed.

Appendix C – Fraud personnel survey results[36]

Background

Q1. Which sectors does your organisation primarily work in?

Sector	Number of respondents	Percentage
Financial services	10	18%
Risk management and security	5	9%
Government / public administration / other services	5	9%
Accounting	4	7%
Charity	4	7%
Investigations and intelligence	4	7%
Legal	3	5%
Education	3	5%
Consultancy	3	5%
Retail	2	4%
Other sectors (individual responses)	12	22%
Total	**55**	**100%**

Q2. What is the approximate total number of employees in your business?

Organisation size	Number of respondents	Percentage
Under 50 employees	6	11%
50–249 employees	12	22%
250–999 employees	14	25%
1,000+ employees	23	42%
Total	**55**	**100%**

Q3. What is the level of your role in your organisation?

Role level	Number of respondents	Percentage
Director / Executive	32	58%
Manager	11	20%

[36] All free-text responses are recorded as they appeared in the survey.

Supervisor	2	7%

Role level	Number of respondents	Percentage
Officer	6	11%
Other	4	4%
Total	**55**	**100%**

Q4. Where is your business primarily based?

Location	Number of respondents	Percentage
England	42	76%
Scotland	0	-
Wales	0	-
Northern Ireland	2	4%
Outside the UK	11	20%
Total	**55**	**100%**

Experience of fraud and other crime incidents

Q5. Has your business experienced any of the following types of crime in the past three years? (n=17)

(Respondents could select more than one option)

Type of crime experienced	Number of respondents
Internal Fraud	21
External Fraud	19
Cyber-enabled fraud / cybercrime	17
Identity Theft	8
Other crime types	4
No crime experienced	4

Free text responses:

- *An attempt was made to take our organisations identity to launch a telephone based fraud, the telecoms providers noticed the fraudulent application and refused.*
- *Internal fraud – A manager collected clients' payments and did not remit them. External fraud – A sacked employee forged company contracts and invoices and billed persons not contracted by the company.*
- *Theft of petty cash and fake / false inventories*

- *External Fraud - abuse of position, fraud by deception against a not-forprofit organisation, one of our clients. External Fraud - romance / dating fraud committed against one of our clients Will & PoA fraud committed against one of our clients Theft of IP by a former business partner, abuse of position.*
- *Many examples of fraud on the public purse, ranging from theft from VAT false accounting to false income tax reclaiming to under declaring direct txes to laundering of criminal proceeds*
- *External fraud - the main types relate to grants and can be divided into either falsifying information to apply for a grant they are not eligible for or obtaining a grant legitimately then spending vouchers/cash on inappropriate items. Cyber-enabled fraud - we receive phishing and other related emails frequently. Our internal training makes staff aware so it is infrequent that someone has clicked on one of these, the internal culture is such that they reported it immediately and action was taken before any loss was experienced.*
- *Our fully integrated IT system was destabilised by an unknown third party seeking payment of a substantial ransom. We reacted quickly and were able to transfer all information from back up files to the Cloud. In total our systems were down for five days.*
- *These are the primary frauds experienced either personally, within my immediate family and via our clients*
- *Expenses overstatement. Failure to bank retail takings. Theft of stock and subsequent sale on Vinted. Theft of cash based assistance.*
- *Internal, theft of property and equipment other theft of materials, parking permit fraud*
- *Vendor email compromise resulting in funds transfer to a fraudsters account which was fully recovered with a quick response from the Irish Garda*
- *Internal fraud - expenses fraud External fraud - AI deepfakes of staff contacting customers Cyber-enabled fraud - business email compromise fraud*
- *I know that this has happened however I am not senior enough to know the details*
- *Fraudsters were impersonating bank employees and contacting our clients. Fraudsters were impersonating clients (hacking their emails) and contacting bank*

Q6. Approximately how much financial loss did your business incur as a result of these incidents in the last three years?

financial loss	Number of respondents	Percentage Estimated
No financial loss	16	43%
Under £10,000	8	22%
£10,000–£49,999	0	-

£50,000–£249,999	0	-
Over £250,000	6	16%
Prefer not to say	7	19%
financial loss respondents Total	**Number of 37**	**Percentage Estimated 100%**

Q7. How did the incident(s) affect your business operations? (n=20)

(Respondents could select more than one option)

Operational impact	Number of respondents
Reputational impact	12
Reduced staff morale	8
Temporary shutdown / disruption	4
Incurred legal costs	4
Loss of clients	4
Increase in insurance premium	3
Other	4
No significant impact	5

Prevention and Preparedness

Q8. How confident are you in your business's ability to prevent fraud?

Confidence level	Number of respondents	Percentage
Very confident	12	39%
Somewhat confident	14	45%
Neither confident nor unconfident	4	13%
Not very confident	1	3%
Not at all confident	0	-
Total	**31**	**100%**

Q9. What do you think are the biggest barriers to effective fraud prevention or detection in your business? (n=29)

(Respondents could select up to three options)

Barriers	Number of respondents
Complexity of threats	18
Lack of resources / budget	17
Lack of awareness / expertise	13
Barriers	**Number of respondents**
Low prioritisation by leadership	6
Regulatory uncertainty	3
Lack of external support	1
Other	3
Total	

Q10. Adequacy of measures for preventing and detecting fraud in organisation

Measures	1 Not at all adequate	2 Somewhat adequate	3 Moderately adequate	4 Very adequate	5 Completely adequate
Anit-fraud culture set from the top (n=28)	-	-	9	8	11
Fraud training and awareness for staff (n=28)	-	2	7	11	8
Anti-fraud policies and procedures (n=28)	-	2	8	10	8
Use of anti-fraud software and tools (n=28)	3	4	9	5	7

Free text responses:

- *Must get cameras*
- *IT security run mock phishing emails regular training annual fraud awareness course for the business Bringing in ECCTA*
- *We have moved our accounts system to the Cloud*
- *Business has pivoted from consulting work to events and hospitality. Experiencing changes in fraud risk as a result.*
- *The huge scale of fraud on the public purse makes complete prevention unachievable. They do reasonably well on prevention and detection and enforcement etc.*
- *Org too small to participate in, for example, data sharing via Cifas, DD via credit bureaux. Costs are prohibitive for SMEs*
- *Being a sole director makes things arguably simpler!*
- *I train/teach/coach/mentor/ and assess counter fraud students, therefore my systems have to be above and beyond the threats out there.*

Q11. Adequacy of measures for preventing and detecting fraud in organisation

Measures	1 Not at all adequate	2 Somewhat adequate	3 Moderately adequate	4 Very adequate	5 Completely adequate
Internal audit or risk assessments (n=25)	1	2	7	9	6
Proactive data analysis to identify potential frauds (n=25)	4	2	9	9	1
Internal fraud reporting mechanisms (such as whistleblowing lines etc.) (n=25)	1	4	8	8	4
External consultancy or expert support when required (n=24)	1	3	7	7	7
Pre-employment and contractor vetting (n=26)	1	3	5	9	8
Insurance against fraud incidents (n=25)	3	2	10	7	3
Publicity of successful fraud action or prosecutions (n=24)	1	2	8	4	3

Free text responses:

- *Penultimate measure response is due to the size of my company and the cost / benefit analysis undertaken to cover risks assessed as under adequate control through my own design and processes. Last measure response is owed to the fact that there have not been any fraud actions or prosecutions taken with respect to my business activity. Disclaimer - the firm is very new and time will tell!*
- *We have not used external consultancy or support*
- *No fraud incidents requiring Publicity*

Q12. How effective do you believe data and information sharing is between organisations for fraud prevention and detection in the business community?

Effectiveness	Number of respondents	Percentage
Very effective	7	29%
Somewhat effective	8	33%
Neither effective nor ineffective	4	17%

Not very effective	3	13%
Not at all effective	2	8%
Total	**24**	**100%**

Q13. How effective do you believe data and information sharing between the public and private sectors is for fraud prevention?

Effectiveness	Number of respondents	Percentage
Very effective	7	29%
Somewhat effective	3	13%
Neither effective nor ineffective	6	25%
Not very effective	6	25%
Not at all effective	2	8%
Total	**24**	**100%**

Free text responses:

- *Without private /public collaboration with regards to data sharing we are making life very difficult for ourselves and missing vital frauds not to mention opportunities to undertake proactive fraud risk assignments*
- *Communication, people must take responsibility for their actions.*
- *Name and shame and the executives don't want to be in the spot light relevance and what can be gained by sharing?*
- *Lack of awareness and inadequate training.*
- *Clarity around legislation, what can and can't be done and a lack of central leadership guiding organisations into what is possible*
- *Companies fear to disclose fraud perpetrated against them for fear of losing customer trust. Companies fear to involve law enforcement agents, citing legal challenges.*
- *As ever, certain entities do not understand the legal basis for data sharing to detect and prevent fraud. Greater education is required.*
- *Confidentiality maybe? Reputation worries?*
- *Companies are reluctant to disclose relevant information.*
- *Incorrect perception and barriers relating to data protection and support from relevant regulators. Needless barriers within sectors and across sectors Needless barriers for sharing data across borders*
- *Privacy / confidentiality / self-interest and a general lack of awareness and TRUST to share appropriate information with appropriate bodies and individuals. A cadre of vetted and trusted individuals from each organisation could be formed for such intel-sharing purposes.*
- *An unwillingness to admit to being a victim of fraud due to associated reputation issues.*
- *Legal and privacy coupled with misunderstanding*

- *lack of training, understanding, money, priority from above, systems outdated, and the general acceptance to commit fraud by anyone - taking the lead from managers, government, etc.*

Support and Response

Q14. Have you ever sought any external help after a fraud incident (such as from the police, Action Fraud, expert consultants etc.)?

Response	Number of respondents	Percentage
Yes	16	73%
No	4	18%
Not applicable	2	9%
Not sure	0	-
Total	**22**	**100%**

Q15. If yes, who did you approach for support? (n=22)

(Respondents could select more than one option)

Support	Number of respondents
Action Fraud	9
Local police	7
Legal adviser	6
Specialist police unit	5
External consultant	5
Industry body / trade association	2
Accountant	0
Other	1
No help sought	6

Free text: Usefulness of any support received:

- *Local policing non-existent AF very good*
- *Very good*

- *It was easy to report to the police, but it took a long time for the police follow up. A lot of bureaucracy. Rated 5/10.*
- *Action fraud / NFIB remains a black hole and a one way street. Not viable for SMEs to join Cifas.*
- *Have internal experts usually*
- *The help was effective in pursuing a prosecution and recovery against a high-value fraud individual.*
- *Used IT consultant to help secure all files.*
- *Legal via Tenet, always our go to for support. Action Fraud remains a black hole.*
- *Action Fraud have been consistently unhelpful even when supplied with repeated reports regarding the same individual including police reports no action has been taken.*
- *not particularly effective. police are disinterested in following up crime reports*
- *Not helpful.*
- *Just to make a point – Action Fraud – is known commonly as 'non-action fraud' and a complete waste of time*

Free text: Challenges faced in accessing help or justice after a fraud incident

- *Lack of awareness or know how on identity fraud this is where collaboration between third sector also needs to be explored as Action Fraud and policing needs to signpost business and citizens to UKIFA.co.uk on how to repair their ID and how/who to report providing a real chance to make a difference to victims of ID fraud albeit funding would help too*
- *i suppose amount of paper work and resources needed and the time taken to get to courts etc*
- *Major problem was downtime.*
- *Costs for legal assistance*
- *Only time pressure in restoring all systems in the cloud. • Inaction Fraud / NFIB Not fit for purpose*
- *Lack of expertise.*
- *One department in government that takes over from - cabinet office, home office, etc. and is on the same level of power as HMRC/DWP/police*

Needs and Gaps

Q16. Support, or resources which would be the most helpful to better protect your business from fraud (n=21)

(Respondents could select more than one option)

Support	Number of respondents

Improved response from law enforcement	13
Practical guidance or toolkits for tackling fraud	10
Fraud awareness campaigns	9
Sector-specific information for tackling fraud	9
Tailored fraud training for staff	8
Easier access to expert advice	4
Better insurance products	3
Other	2

Free text: Experience of any support received:

- *Majority suffer poor experience from AF not personally and always promote AF*
- *We have no cameras, and police don't come out.*
- *having regular training keeps the knowledge awareness, having workshops may be to get it to life to view , having expert's advice is great but at what costs?*
- *All staff should have sufficient background knowledge.*
- *Government prioritisation to tackle the threat and a co-ordinated response that shares information from cases to prevent recurrence cross-sector will assist, more focus on prevention rather than reaction.*
- *Rarely does fraud get taken seriously by local law enforcement*
- *A lot of fraud info is generalist, focussing on common themes that any individual or organisations may experience. Some more practical advice that is sector-specific would be more useful for training staff*
- *Personal insurance against fraud? Does such a thing exist? It's taken for granted that we have home and personal possessions insurance, what about fraud?*
- *All are considered relevant and could be contained under the umbrella of the concept outlined in 'other' above.*
- *The first four are pointless and a waste of money - change is required to the behaviour of everyone first - fraud is too easy in the UK*

Free text: Gaps in current fraud prevention efforts

- *More proactive cross sector exercises with meaning and using live data and not generally public sector biased as NFI is at present*
- *Better policing.*
- *to get the fraudsters sooner , punishments to be a deterrent*
- *Lack of awareness of threat*
- *as above*
- *More intel sharing, data sharing, meet ups. Cross sector collaboration could be better.*
- *Not gaps particularly but the nature of the organisation means that more resources would always help prevention*

- *Cross sector data sharing need improving. Cross border info sharing should be a priority. The fraudsters do not respect geographic or political borders, giving them a distinct advantage.*
- *Government enforcement and policy is too divided - SFO / NCA / local police / FCA / ICO etc and SFO / CPS for prosecutions. There could also a a more effective central intelligence agency that has excellent contacts with the banking industry so that temporary money freezing order can be implemented on trust and professionalism alongside all necessary checks and measures (e.g. HK's Joint Financial Intelligence Unit - police and customs working closely together).*
- *More response and follow up by management and the board.*
- *Yes, punishment - sanctions - should be much harsher*

Language and Terminology

Q17. Have you ever found fraud or fraud-related terminology confusing or inconsistent across different sources (such as government, insurers, regulators)?

Response	Number of respondents	Percentage
Yes	7	32%
No	9	41%
Not applicable	2	9%
Not sure	4	18%
Total	**22**	**100%**

Free text: Types of fraud-related terminology that is confusing or inconsistent across different sources

- *Victims continually being described as “fallen for fraud” as an example Victims need to be treated as victims of crime not fraud cyber etc then they will Be treated accordingly as opposed to at present whereby they receive very little support Also stop using the word scam whereby fraud has occurred as it undermines the importance and the victims*
- *No help from anyone.*
- *As an organisation working within risk management, we have learnt the jargon that comes with counter fraud. We acknowledge it is confusing for regular businesses. Esp. due to different sectors / communities having their own set of jargon (AML, Infosec, Cybersec, payments compliance etc etc)*
- *Each sector has their own set of terms, own language. This is a problem.*
- *I teach it - so, it is the language I use*

Q18. To what extent is it important that fraud-related terminology and definitions are conveyed clearly and consistently across all campaigns, policies and guidance?

Importance	Number of respondents	Percentage
Very important	16	73%
Quite important	6	27%
Neither important nor unimportant	0	-
Not very important	0	-
Not important at all	0	-
Total	**22**	**100%**

Free text responses:

- *Prevents people From Reporting as made to feel silly, nothing happens and support is non existent*
- *but bear in mind what industry you are working in for its weighting*
- *There should be a unified response to provide a clear message to those not working within the sector as well as those within, fraud is a cross sector problem and should be addressed as such – supporting all not just subject matter experts*
- *There is a need for some kind of reference / Wiki type site to allow the different communities to describe their TLAs (Three Letter Acronyms)*
- *I believe there is a clear need for some kind of fraud terminology wiki site*
- *Certainty is always encouraged when dealing with legal issues as complicated as fraud cases are, so that everyone speaks the same language and understands the threats, issues and solutions.*
- *If someone does not understand what fraud has been committed, getting any response from enforcement is negligible*

Q19. Who in your organisation would benefit from clearer, simpler explanations of fraud? (N=22)

(Respondents could select more than one option)

Support	Number of respondents
Board members	5
Senior leadership	13
Operational staff	11
Finance team	6
IT team	6
All staff	9
No staff	1

Q20. What would help improve the understanding of fraud risks across your organisation? (n=21)

(Respondents could select more than one option)

Type	Number of respondents
Sector-specific examples	14
Examples or case studies in plain English	12
A glossary of key fraud terms	9
Simpler language in official guidance	9
Interactive or visual materials (e.g. videos or infographics)	9
Other	3

Future Threats and Preparedness

Q21. How concerned are you about the risks associated with the following frauds in the future?

Type	1 Not at all concerned	2 A little concerned	3 Neutral	4 Quite concerned	5 Very concerned
Fraud involving phishing and social engineering (n=23)	-	2	-	13	8
Business email compromise (n=23)	1	3	5	10	4
Insider threats (n=23)	4	3	8	6	2
Identity fraud (n=23)	1	3	6	6	7
Supply chain fraud (n=23)	1	5	5	8	4
Crypto-related fraud (n=23)	7	6	3	3	4
Fraud involving Cloud storage (or similar) (n=23)	1	1	10	6	5
Fraud involving QR codes (n=23)	4	5	7	2	4
Fraud involving deep fakes or that which is AI-enabled (n=22)	3	1	3	8	7

Free text: Other frauds not listed in survey

- *Hijackings of vehicles*
- *unknown as they are ahead of the game - sharing knowledge to protect personal belongings will be good too . car theft , door locks, alarms etc - just to make it wider and that it can happen at home or start from home?*
- *AI misinformation, misdirection, misrepresentation*
- *The above list just about covers it - recent cases indicate that social engineering and AI (and the confluence between the two) could be an additional independent threat to be considered - 'Social AI-enhanced engineering' for example.*
- *The general level of fraud on a daily basis*

Q22. How prepared to you think your organisation is to tackle the risks associated with evolving or new fraud tactics in the future? (n=23)

Extent	Number of respondents	Percentage
Very prepared	2	65%
Somewhat prepared	15	26%
Neither prepared nor unprepared	6	9%
Not very prepared	0	-
Not prepared at all	0	-
Total	**22**	**100%**

Free text: Specific steps taken

- *Take all steps, promises is all I get.*
- *would like to think very prepared ! cyber threat we are prepared and working hard on this supplier chain / invoices - can happen? doing phishing email simulations with staff MFA Password changes and longer ones etc*
- *Staff Training.*
- *Member of specific fraud forums. Delivery of awareness campaigns.*
- *Key staff are aware of the various frequent types of fraud*
- *Learning about AI and organising specific events covering the intersection between AI, cyber security, and fraud*
- *2FA, off-web encrypted data back-up, regular change of passwords, safe fireproofed storage of relevant devices and data, verification of all information where deemed necessary. P2P contact whenever in doubt.*
- *Best software, up to date software, bin everything not from someone I contacted*

Free text: Further support or resources that would help prepare for future fraud risks

- *More security officers and cameras.*
- *Possibly additional software packages.*
- *ongoing training that is engaging and not simply delivered as mandatory • More time / staff to assess new and evolving risks*
- *Notification of new types of fraud.*
- *Financial support to grow awareness and facilitate sharing of best practice*
- *Engagement in a FAP-created think-tank that anticipates possible new threat areas.*

Q23. Would you say that your organisations has a good culture towards tackling fraud?

Response	Number of respondents	Percentage
Yes	19	82%
No	2	9%
Not sure	2	9%
Total	**23**	**100%**

Free text: Actions businesses should take to strengthen their counter-fraud culture among new staff

- *start from the top and talk openly and frequently be alert at all times Regular training and mandatory for new staff Limit social media actions for new staff (i.e. advertising that they are at a new place etc) or remove certain permissions until they pass probation -as fraudsters can start from there*
- *Investigate employment history and seek strong references.*
- *training and awareness, open and clear communication and cross sector engagement*
- *Pre-screening of staff, appropriate training during onboarding. Mandatory annual refresher training.*
- *One individual should be nominated to head up fraud prevention.*
- *Induction training, ensure it is not a tick box exercise.*
- *Appointment of a fraud intelligence officer in each organisation would spearhead the strengthening of counter-fraud (why not anti-fraud?) culture.*
- *More frequent updates and training*
- *Would not take on new staff*

Appendix D – Non-fraud personnel survey results[37]

BACKGROUND

Q1. Which sectors does your organisation primarily work in?

Sector	Number of respondents	Percentage
Accounting	6	12%
Agriculture	0	0%
Banking	3	6%
Charity	1	2%
Construction	2	4%
Consultancy	4	8%
Education	4	8%
Energy	0	0%
Financial Services	0	0%
Government / Public Officer / Other	2	4%
Health / Care	2	4%
Hotel & Catering / Hospitality	0	0%
ICT	0	0%
Investigation & Intelligence	1	2%
Legal	2	4%
Leisure & the Night Time Economy	1	2%
Manufacturing	0	0%
Mining / Quarrying / Utilities	0	0%
Motor Trades	2	4%
Pharmaceutical	1	2%
Post & Telecommunications	1	2%
Production	1	2%
Property	1	2%
Retail	2	4%
Risk Management and Security	5	10%
Training	1	2%
Transport / Logistics	1	2%
Wholesale	0	0%
Other (please specify)	9	17%
Total	**52**	**100%**

[37] All free-text responses are recorded as they appeared in the survey.

Q2. What is the approximate total number of employees in your business?

Organisation size	Number of respondents	Percentage
Under 10 employees	10	20%
10–49 employees	5	10%
50–249 employees	7	14%
250+ employees	26	52%
Not sure **Total**	2	4%
	50	**100%**

Q3. What is the nature of the department that you work for in your organisation?

Department type	Number of respondents	Percentage
Finance (not dealing with fraud)	16	33%
Operations / Service delivery	4	8%
Customer Services	4	8%
Legal	2	4%
Internal Audit	2	4%
Risk / Compliance	2	4%
IT / Digital	1	2%
Small business no depts	5	10%
Other	13	27%
Total	**49**	**100%**

Q4. Where is your business primarily based?

Location	Number of respondents	Percentage
England	30	61%
Scotland	2	4%
Wales	0	-
Northern Ireland	0	-
Outside the UK	17	35%
Total	**49**	**100%**

GENERAL AWARENESS

Q5. How confident are you in identifying suspicious or potentially fraudulent behaviour in your role?

Confidence level	Number of respondents	Percentage
Very confident	18	38%
Fairly confident	28	58%
Not very confident	0	-
Not very confident at all	1	2%
Not sure	1	2%
Total	**42**	**100%**

Q6. Does your organisation mandate that each member of staff receives training or guidance about fraud?

Response	Number of respondents	Percentage
Yes	31	66%
No	13	28%
Not sure	3	6%
Total	**47**	**100%**

Q7. Which of the following best describes the training and guidance you have received on recognising or reporting fraud?

Statement	Number of respondents	Percentage
When first started work	1	2%
In the past 12 months	32	32%
Over 12 months ago	5	5%
Never received any	9	9%
Not sure	0	-
Total	**47**	**100%**

Free-text responses: types of training received

- *Training on common cyber risks such as phishing emails etc*

- *Ongoing conduct and compliance awareness training.*
- *Fraud Awareness and Reporting Procedures*
- *Fraud Awareness and Reporting Procedures*
- *As a board member of a credit union I receive annual training on fraud in the workplace*
- *I am reading Blackstone's Counter Fraud Professionals Handbook and Fraud The Counter Fraud Practioner's Handbook by Alan Doig.*
- *I read information from various agencies about counter fraud and also cyber security*
- *As an academic I have the opportunity to attend a variety of fraud events annually to keep abreast of the evolving nature of this crime. I designed a compulsory fraud course for my University staff which must be attended by all staff every two years.*
- *Online awareness - short 5 mins*
- *Basic anti-fraud course*
- *CPD courses, using AI*

Q8. How easy is it to find information about your organisation's fraud policy and reporting procedures?

Ease of access	Number of respondents	Percentage
Very easy	12	26%
Somewhat easy	19	40%
Difficult	6	13%
Not aware we had any	10	21%
Total	**47**	**100%**

Q9. Do you know how to report a suspected fraud within your organisation?

Response	Number of respondents	Percentage
Yes	40	89%
No	5	11%
Total	**45**	**100%**

COMMUNICATION AND CULTURE

Q10. How clearly does your organisation communicate its stance on fraud and unethical behaviour?

How clearly?	Number of respondents	Percentage
Very clearly	24	55%
Somewhat clearly	13	30%
Not very clearly	5	11%
They do not communicate	2	4%
Total	**44**	**100%**

Q11. How often have you been encouraged and reminded to speak up about any concerns (fraud-related) or otherwise?

Frequency	Number of respondents	Percentage
Regularly	17	39%
Occasionally	14	32%
Rarely	6	13%
Never	7	16%
Total	**44**	**100%**

Q12. If you had a concern about a potential issue, how comfortable would you feel about reporting it?

Level of comfort	Number of respondents	Percentage
Very comfortable	28	65%
Somewhat comfortable	10	23%
Not very comfortable	3	7%
Not at all comfortable	2	5%
Total	**43**	**100%**

LANGUAGE AND TERMINOLOGY

Q13. Have you ever found fraud or fraud-related terminology confusing or inconsistent across different sources?

Response	Number of respondents	Percentage
Yes	18	43%
No	16	38%
Not sure	8	19%
Total	**42**	**100%**

Free-text responses provided by respondents included:

- *There are a lot of abbreviations that are used. Briefings are often incredibly long without an executive summary.*
- *Fraudulent emails from look-alike email addresses. Telephone scams.*
- *Assessment scores.*
- *Some view corruption as a form of fraud or vice versa, while others treat it as a separate scam altogether and consistently refer to such acts as fraud.*
- *In a court case, the person accused of fraud stated under oath that they did not realise their actions constituted fraud. If that is accepted, there is no hope of preventing fraud.*
- *Definitions vary considerably. Overlap with cybercrime.*
- *Sometimes if there is a non-financial fraud it is not clearly understood. It can be difficult to get to a point where a fraud is "proven".*
- *Not sure.*
- *I am bemused by the level of obfuscation and concealment in this area. Financial professionals routinely ignore the laws with unclean hands.*
- *The words fraud and scam are used interchangeably. Also behaviour is sometimes dismissed as naughty, a joke or a trick on the organisation.*

Q14. To what extent is it important that fraud-related terminology and definitions are conveyed clearly and consistently?

Importance level	Number of respondents	Percentage
Very important	32	78%
Quite important	5	13%
Neither	2	5%
Not very important	1	2%
Not important at all	1	2%
Total	**42**	**100%**

Free-text responses:

- *It helps if everyone speaks the same fraud language, especially where there is collaboration across industry and government.*

- *Social engineering is complex. Risk professionals need to explain clearly what fraud activities are, what the impact is and how to stop them.*
- *For enlightenment.*
- *Clear, understandable language communicates more easily and avoids people getting bogged down and giving up.*
- *Either fraud is unacceptable or it is not. Authorities and judges need to be consistent. Jurisdictions must be clear that it is not acceptable.*
- *I don't feel wording is important or relevant. Fraud policies should only cover what's needed in order to prosecute.*
- *A common language across organisations and businesses would improve shared understanding and experience relating to fraud.*
- *I work in local government so the term fraud isn't used. Not sure if it is under a different name.*
- *Unclear definitions create opportunities for non-compliance.*
- *Transparency and simplicity will maximise the effectiveness of policies.*
- *To help reporting routes both as an individual and an organisation.*
- *Terminology should be clear and simple for all ages to understand. Fraud can happen to anyone.*
- *The UK is operating in a vacuum of non-enforcement and disregard for regulatory compliance.*
- *Some people don't realise that certain activities are fraudulent.*
- *Inconsistent terminology makes it more difficult to compare policies and practices.*
- *If it isn't simple to identify and understand, it becomes confused with other issues and policies.*
- *To minimise confusion.*

Q15. Who in your organisation do you think would benefit from clearer, simpler explanations of fraud? (n=42)

(Respondents could select more than one option)

Support	Number of respondents
Board members	5
Senior leadership	6
Operational staff	13
Finance team	9
IT team	4
All staff	35
No staff	3

Q16. What would help your understanding of fraud risks across your organisation? (n=42)

(Respondents could select more than one option)

Type	Number of respondents
Regular alerts and updates on emerging frauds	33
Examples or case studies in plain English	23
Interactive or visual materials (e.g. videos or infographics)	23
Simpler language in official guidance	21
A glossary of key fraud terms	20
Role-specific guidance	20
Sector-specific examples	19

Free-text responses:

- *More regular reminders about common issues and information about emerging types.*
- *A whole approach, risk types are dealt with in isolation. In reality they are cross border always.*
- *Developing policies related to fraudulent cases and consequences and communicating to every staff by training and certification.*
- *Have annual training*
- *More interactive training*
- *Simplify the reporting system and communicate that clearly to staff.*
- *Guidance for new starters in an onboarding guide and regular refreshers for existing staff.*
- *Not much for the size we are*
- *Needs to be more re impersonation ID fraud with advent of AI*
- *Provide tangible examples whenever fraud is spotted.*
- *Educate them all in the types of fraud that outsiders may attempt to perpetrate*
- *Set up a policy or review into this*
- *Improve whistleblowing procedures and protections*
- *Have a dedicated phone line or email address. Currently reports should be made to the CFO which can be quite daunting for some staff*
- *Educate the wider business to fraud, so then can be alert when engaging with new suppliers, more background checks on new / onetime suppliers.*
- *Yes, example case study video story telling*
- *Everything possible is being done by us..... BUT simply ignored and disregarded - we have a case that can be shown as a confidential example and it is an absolute shocker*
- *Have a bigger and more joined up team for security, covering not just fraud but all other security related matters • Report on examples that are of current event.*
- *It is done exceptionally well. Nothing further.*

RECENT LEGAL UPDATES

Q17. Have you heard of the Economic Crime and Corporate Transparency Act?

Response	Number of respondents	Percentage
No	20	48%
Yes and understand how it applies	16	38%
Yes but do not understand how it applies	6	14%
Total	**42**	**100%**

Q18. Are you aware that organisations can be held criminally liable under the Failure to Prevent Fraud offence?

Response	Number of respondents	Percentage
Yes	25	61%
No	16	39%
Total	**41**	**100%**

Q19. Do you think that your organisation has communicated these new legal requirements effectively?

Number of Response	respondents	Percentage
Wasn't aware of the requirements	12	30%
Yes	6	15%
Somewhat	6	15%
No	11	27%
Do not affect our company	6	15%
Total	**41**	**100%**

About Perpetuity Research

Perpetuity Research is a leading research company specialising in economic crime, security and wider crime issues, with strong expertise in both quantitative and qualitative methods. We have extensive experience in

evaluating what works and what does not in preventing, detecting and responding to threats such as fraud, money laundering, bribery, corruption, cybercrime and other forms of criminal activity. Our work helps clients understand behaviours, risk drivers, perceptions and levels of awareness across individuals and organisations, while identifying emerging trends across the crime and security landscape.

Our mission, committed to making a difference, is reflected in our focus on delivering practical, evidence based insights that strengthen decision making, enhance compliance and security frameworks, and support effective policy development. We translate complex data into clear, actionable intelligence that enables organisations to manage risk, improve resilience and respond confidently to evolving threats.

We work closely with a wide range of clients including businesses, national and local governments, regulators, law enforcement bodies, industry associations, international organisations, charities and foundations. By combining rigorous research with sector specific expertise, we aim not only to meet expectations but to exceed them, as reflected in the long standing partnerships we have built over many years.

About the author

Doctor Janice Goldstraw-White

Janice is a criminologist and the editor of our monthly *Security and Risk Thought Leadership* newsletter and has been affiliated with Perpetuity since 2010. She has specialised expertise in the study of crime, governance, audit, risk management and security, supported by more than two decades of prior experience as an accountant.

Her research focuses on economic crime, fraudster behaviour and the role of women in fraud, and she has examined these areas extensively in both the UK and Australia. She has a particular interest in fraudster behaviour and the narratives individuals use to explain and justify their actions. She has conducted over fifty interviews with incarcerated white collar offenders and has considerable experience undertaking qualitative research within custodial settings.

Janice's methodological expertise is grounded in qualitative approaches, including literature and policy reviews, institutional and procedural mapping, interviews and focus group facilitation. She also has a strong working knowledge of quantitative methods and data analysis.

She has led and contributed to a wide range of research projects, including work on fraud in local government, the case for mandatory fraud reporting in the UK, digital evidence challenges, fraud management in the Middle East,

responses to fraud victimisation, NFT related fraud, and cross sector collaboration and data sharing to tackle economic crime.

Her research also extends beyond economic crime into broader security and crime issues, including organised crime in the private rental sector, the disproportionate impact of COVID 19 on security personnel, data centre security, the integration of artificial intelligence into security practices, and the development of sector specific key performance indicators. She has also recently contributed to research examining how the value of security can be effectively demonstrated to stakeholders.

Janice has authored and co-authored multiple peer reviewed publications and book chapters, most recently on female perpetrators of fraud. Her book, White Collar Crime Accounts of Offending Behaviour, was published in October 2011.

Perpetuity Research & Consultancy International Ltd

11a High Street
Tunbridge Wells TN1
1UL
United Kingdom
Tel: +44 (0)1892 538690

Email: prci@perpetuityresearch.com

Website: https://www.perpetuityresearch.com