Business Fraud Alliance
Protecting Business. Preventing Fraud

Fraud Advisory Panel Response to Revised Fraud Strategy

FRAUD ADVISORY PANEL

BARCLAYS

Contents

Executive Summary

This policy paper has been drafted by the Fraud Advisory Panel (the Panel) in response to Lord Hanson's revised and expanded Fraud Strategy, part of the Government's plan for the public and business to be better protected from every aspect of the UK's growing fraud threat.

Introduction

Fraud is a rapidly evolving and increasingly sophisticated crime that exploits emerging technology to pose significant risk to economic stability, governance and public trust, with an estimated 70% of fraud now including an international element. Fraud and cybercrime make up 50% of all online crime in the UK.

As part of this response, the Fraud Advisory Panel working group has responded to six of the areas addressed by Lord Hanson:

- Data Sharing
- Technology
- Business and Growth
- Public Awareness
- Artificial Intelligence (AI)
- Criminal Justice System

Though each area has been reviewed independently, it is imperative to note that the increasing pace of change, the fraud threat, an effective and dynamic cross-sector international response, the importance of tackling fraud while promoting economic growth, and the vital role of clear communication to engage with the public in the conversation are crucial to a successful outcome.

Data Sharing

Data sharing, whilst subject to the controls of the Data Protection Act 2018 (DPA 2018) and provisions of the Data Access and Use Act (2025), remains a risk as criminals seek to obtain unauthorised access to held information, acts that serve as the precursor to certain frauds. To combat the threat organisations need to be able to protect themselves and their customers through the safe exchange of data.

In modern working environments, Data Sharing is an essential internal and external organisational process that allows resources to be shared through various means, facilitating cross-sector collaboration, efficiency and innovation. There is a requirement to balance interoperability with privacy and governance, removing obstacles to facilitate data and intelligence sharing between the public and private sector without being susceptible to misuse.

Improving the clarity of the law around data sharing and minimising legal barriers relating to civil liability could promote more open data sharing between organisations, following the examples of the Economic Crime and Corporate Transparency Act 2023 (ECCTA) and other fraud data-sharing initiatives. In particular, the implementation of a government-led framework would allow for early identification of fraudulent activity and potential criminality through indicators such as IP addresses, behavioral patterns, and other suspicious activities.

The Panel proposes the following:

- Leadership from government in providing a centralised data-sharing framework drawing together existing organisational bodies already involved in this space. This would allow for streamlined information and processes to be efficiently shared between professional, public, private and third sector bodies, and for simpler reporting processes and end-user requirements to assist with investigation and disclosure.

- Guidance and greater regulatory clarity on legislation around data-sharing (e.g., GDPR) and support from bodies like the ICO to remove concern about legislation misinterpretation that can prove an obstacle to positive data-sharing between sectors.

- Addressing bureaucratic concerns to stimulate the sharing of public body information with private organisations, streamlining communication flows and minimising red tape. Presently, the information flow is inefficient and slow due to lack of training and guidance. Removing unnecessary red tape where possible will help facilitate data-sharing and allow for a faster response to tackle and counter fraud issues.

- Removal of barriers to data-sharing to enhance capability and familiarisation of positive and effective data-sharing across all sectors.

- Adopting a 'common-sense' approach to information sharing, opening wider lines of communication through a clear legislative gateway, serving as the benchmark that establishes a centralised system where information can be shared widely between trusted partners.

- The banking industry plays a central role in the sharing of information, through the Business Fraud Alliance, Barclays can lead a working group bringing together the banking industry, promoting collaboration and a proactive approach to communication flows into and within the sector.

As with Anti-Money Laundering provisions there needs to be a clear process to legally share suspicions of fraud between parties and with law enforcement and the implementation of a top-down approach. Through an overarching framework body, for example a centralised system of approved contacts or an independent body, draft guidance and principles can draw together all parties to facilitate the sharing of information between users quickly and effectively.

Technology

Fraudsters have long exploited evolving technologies to target individuals and businesses, with traditional avenues like phishing and ransomware continuing to pose significant harm.

Some technological solutions, like telephone companies adding 'suspected scam' tags to suspicious numbers or banks operating robust 'think first' warnings before payment transfers, have had an impact in countering some fraud.

In consideration of addressing technological concerns, it is important to focus on what is realistic and achievable.

The Panel proposes the following recommendations:

- Incentivise big tech to accept shared responsibility through further regulatory measures and potentially expanding the Product Security and Telecommunications Infrastructure (PSTI). Government support should also assist in raising awareness of resources like FIRE System and Global Signalling Exchange as potential models for proactive collaboration.

- Encourage the implementation of a collaborative and centralised process to use technological advances to combat financial crime, supporting and guiding public and private stakeholders like tech companies, software providers and cyber security organisations.

- Consider the Fraud Advisory Panel review into the PSTI Act to tackle abuse of online remote access tools.

Business and Growth

It is a governmental priority to stimulate growth, removing regulatory barriers where possible. It is imperative to ensure that any review or amendment of regulatory policy or changes in law does not foreseeably increase the risk of fraud or prevent anti-fraud legislation being introduced.

Anti-fraud laws must be user friendly and not interpreted by businesses as a compliance cost but vital in preventing economic risk and harm. These must also be recognised by all parties as legitimate growth enablers, not growth inhibitors. An environment free from fraud, one that promotes good financial crime protection will encourage business and growth, through enhanced investor confidence whilst also avoiding the costs of investigations and other action that may occur as a result of limited financial controls.

It is vital the government encourages, supports and guides businesses to adopt a proactive approach to prevent fraud, rather than adopting a reactive and expensive response after fraud has already been committed. Training and investment in education is crucial in combatting this issue.

The Panel proposes the following:

- Invest in staff training and education to limit ongoing failures to identify and prevent fraud, including access to training material and resources. Incentivise businesses of all sizes to invest in counter-fraud training and upstream education by offsetting their costs against other areas of expense (e.g., tax, or through designing a standardised, freely available training package giving organisations a tool to present to insurers to reduce insurance costs).

- Introduce obligations within the annual return process to Companies House or through the Financial Services Council to develop mandatory standards that support businesses with counter fraud considerations, including risk assessments, response plans and clear signposting to available training and awareness resources.

- Review the Proceeds of Crime Act (POCA) and Asset Recovery Incentivisation Scheme (ARIS) confiscation process and redirect grants to support businesses with their training and counter fraud defences. This could be on a scale basis with smaller firms receiving bigger allocations based on income to create a sustainable and supportive cycle of fraud prevention.

Public Awareness

Public Awareness is critical in countering fraud. There have been various public awareness campaigns in the past from invested stakeholders like the government, individual businesses, the Fraud Advisory Panel and Cifas, but it is difficult to determine how effective these have been. It is necessary to produce a unified, coherent and targeted message that reaches every demographic to raise awareness of business fraud across the board.

A collaborative approach to embracing private and third sector expertise is vital to promote protective campaigns to raise awareness of resources and tools available to businesses to tackle fraud and economic crime. Early awareness of fraud prevention and countering societal norms of discouraging discussion of money is crucial in driving through a complete generational change in perception and resilience to financial crime.

The Panel proposes the following:

- Governmental support for long-running effective campaigning by organisations, bringing together the specialist skills and communications of each to work alongside Stop! Think Fraud, which is recognised as the government campaign tackling fraud. Further promotion of the following campaigns and organisations through platforms such as Stop! Think Fraud will assist with relevant communications tailored to each audience being delivered based on areas of expertise rather than a “one size fits all” approach:
  - The Fraud Advisory Panel (charity and business fraud)
  - Business Fraud Alliance (specific support for businesses)
  - Take Five (consumer fraud)
  - Get Safe Online (online safety)
  - Trading Standards (supporting vulnerable people)

- Adopting an early educational approach to countering fraud that can assist in generational change. By updating the school curriculum to include fraud awareness training from industry experts, future generations will be better equipped and more economically aware with the necessary tools to be resilient to financial criminal threats. A similar approach raising awareness at a younger age has proven successful in combatting other societal issues like smoking, drink driving and wearing seatbelts. Removing prohibitive red tape will also enable and encourage charities and the public sector deliver preventive education more widely and effectively.

- Raise awareness of ‘money muling’, the transferring of illegally obtained monies, a critical area requiring immediate attention by supporting targeted campaigns that focus on the issue and ensure communications are targeted appropriately.

Artificial Intelligence (AI)

Artificial Intelligence is a rapidly evolving and generative function that has introduced many new AI-driven financial, economic and cyber threats (e.g. deepfakes and synthetic identities).

It is imperative that AI systems are transparent, accountable and secure to prevent them being exploited for use in criminal offences, particularly if they currently do not possess an inbuilt ‘moral code’. This may require further legislation to regulate IT companies and adopting a future-proofing mindset due to the speed of AI development and the likelihood of an Artificial General Intelligence society.

Further criminalisation of the use of AI in criminal offences is unlikely to reduce its deployment by fraudsters. Focus should be on encouraging AI system developers to act with integrity and assist in preventing AI being used for malicious purposes.

The Panel proposes the following:

- Regulation of AI developers incentivising them to implement stronger controls that combat malicious use. A requirement to publish system vulnerabilities that serve as a guide for public (business) use that enhances awareness of potential criminal deployment of legitimate systems, enabling businesses to take appropriate steps to enhance system resilience and protection.
- Renewed focus on formal international agreements to tackle overseas threats as legal structures alone are insufficient. Platforms and ISPs must be considered to create anti-fraud tools that block use at source rather than relying on regulation alone to enforce. This approach may attract investment from business start-ups to develop tools for systems that tackle the problem at source, stimulating legitimate income against bad actors and criminal threats.

Criminal Justice System

The Criminal Justice System has been subject to financial constraints in recent years and requires considerable investment in digitisation, technology and process to support its functioning. There are areas where change can be implemented that does not necessitate unrealistic financial expectations on the CJS.

It is a concern that AI may render evidence unreliable and subject to challenge. There needs to be a focus on the use of IT in fraud investigations and trial. Changing the wider system is a complex long-term issue, but attention to enhancing efficiency where possible will generate results.

The Panel proposes the following:

- The government should consider streamlining the Disclosure process through further use of technological solutions including AI, which can be used to organise, filter and present relevant evidence. This can significantly accelerate the legal process, helping courts manage large volumes of data more effectively and ensure faster outcomes in fraud-related cases, all while maintaining independence and fairness.
- Consider out of court settlements and a review of the DPA process. Where criminal trials are not possible, guidelines and support around the use of civil recovery should be a consideration.
- Reform and rehabilitation programs for convicted offenders through educational support and consider potential employment opportunities through specific financial programs and support systems.
- Make sentencing a deterrent through robust and recognised penalties upon conviction, that recognise the harm fraud causes. Consider alternative tools like confiscation in a manner that emphasises criminal gains will not be retained. By increasing financial penalties, the attraction of economic crime will diminish. This should be applied internationally with a renewed diplomatic focus on cross-border agreements that share confiscations with co-operating countries.
- Increasing the maximum sentence for fraud offences and bringing bring it in line with the 14 years currently applicable to money laundering should also be considered.

Other Recommendations (Non-Exhaustive)

The following are a series of non-exhaustive potential recommendations the Panel propose should be considered and adopted:

- Harmonise international legal frameworks for cybercrime, including the expansion of the failure to prevent fraud offence.
- Support the creation of digital forensics units and cross-border task forces.
- Mandate robust data governance policies for inter-agency data sharing.
- International engagement: Collaborating cross-border with governments, regulators and organisations is crucial when tackling fraud and financial crime. When proceeds of crime are transferred to an international account the UK sector has limited jurisdiction to repatriate funds once finances reach the beneficiary account. Reaching mutual agreements internationally that enable the banking sector to identify, follow and recoup the proceeds of crime cross border is essential when tackling fraud to both support victims of crime and deter fraudulent activity.
- Ongoing review of the failure to prevent fraud threshold and its application to all businesses and sectors.