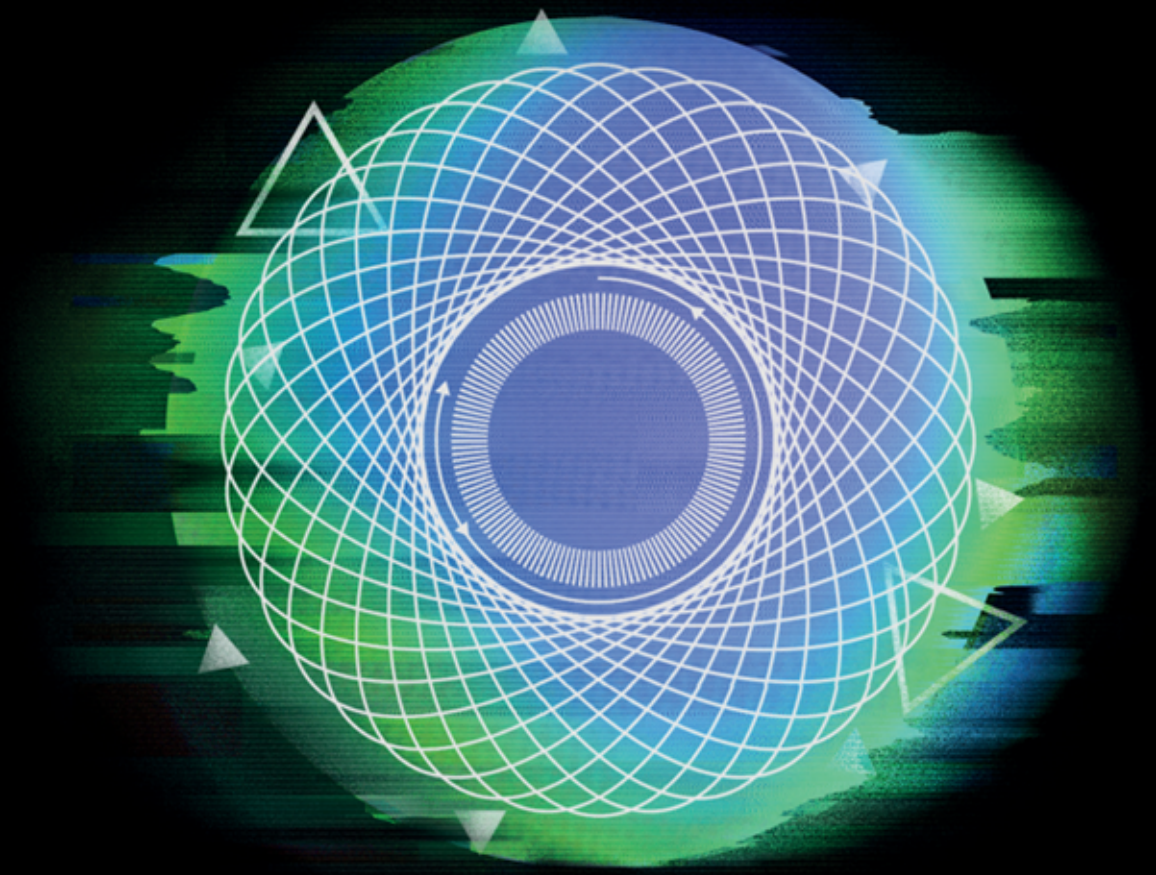
Deloitte.



Tackling Fraud in a Borderless World

Towards a Global Response

March 2026

Introduction

Fraud is no longer a peripheral threat – it is a systemic risk to economies and societies worldwide, and a national security challenge for every country. As digital transformation accelerates, so too does the scale and sophistication of fraud, outpacing the ability of current frameworks to detect, prevent, and disrupt it. Globally, fraud poses significant threats to consumers' financial, emotional, and physical security.

In the UK, fraud now accounts for 45% of all crime – the largest crime type – and the UK Government estimates that fraud cost the UK economy at least £14.4 billion in 2023–2024.[1] Other sources, such as Cifas, suggest the broader economic impact of fraud and error may be significantly higher, with estimates reaching up to £219 billion annually. For context, this exceeds the entirety of the NHS budget for 2024/25 (£205bn)[2] and represents an average cost of £3,200 per person. It is a global pandemic, with the Global Anti-Scam Alliance (GASA) reporting that seven in ten adults have encountered a scam in the last 12 months, with 13% encountering a scam at least once a day.[3]

Despite these alarming figures, the global response remains fragmented and underpowered. Investigations are few, prosecutions rare, and recovery of criminal proceeds minimal.

This paper explores why current approaches fall short and proposes a more ambitious, coordinated response to this growing crisis.

[1] CP 1523 – Fraud Strategy 2026-2029 Disrupting crime, supporting economic resilience and delivering justice, page 4

[2] The King's Fund 'The NHS budget and how it has changed', 16 December 2025

[3] Global Anti-Scam Alliance (GASA) 'Global State of Scams – 2025 Report', page 45

The scale and complexity of the threat

Fraud is a uniquely complex and borderless crime. The rapid shift to online services, instant payments, and the increasing use of artificial intelligence have dramatically expanded the attack surface for criminals. The threat is:

CROSS-BORDER:

Criminals exploit jurisdictional gaps and regulatory arbitrage, where based on recent reports from the National Crime Agency (NCA), the Home Office, and leading fraud prevention services, it is estimated that over two-thirds of UK fraud cases now involve an international element.

CROSS-SECTOR:

Fraudsters move seamlessly between all sectors including financial institutions, social media, telecoms, and the public sector. In the UK, for example, fraud and error affecting the public sector is estimated to cost the taxpayer up to £81bn per annum.[4]

TECHNOLOGY-DRIVEN:

Advances in technology, particularly generative AI tools such as deepfakes, large language models, and voice cloning, are being rapidly adopted by organised crime groups. These tools increase the sophistication, credibility, and volume of attacks, making them harder to detect and prevent.

CROSS-PAYMENT RAILS:

New payment methods and platforms are exploited as quickly as they emerge, with criminals adapting to innovations faster than the protective response can keep pace.

Across both public and private sectors, collaboration remains insufficient, and fraud levels continue to rise despite significant investment and effort. This is despite all the resource, time and effort that is being deployed to combat it. Existing anti-fraud infrastructure is not utilised to maximum effect and, given the furious pace of technological development, regulatory frameworks rapidly become misaligned with the realities of modern digital fraud.

[4] An Overview of the impact of fraud and error for the new Parliament (2023-24), page 6

Why are we failing to reduce fraud?

Despite increasing awareness and investment, fraud has continued to rise globally. Several persistent barriers undermine efforts to reduce its impact:

Chasing not preventing	83% of frauds start online or on telecoms platforms.[5] Once money is moving through the banking system it is too late; our focus must pivot to prevention. This means all stakeholders in the fraud value chain will have to take greater accountability, doing more to address vulnerabilities on their platforms to ensure they play a full part in stopping the fraud threat at source.
Siloed Approaches	Information sharing remains limited within and between sectors and jurisdictions. The UK Fraud Strategy identifies a fragmented data landscape as a major challenge, noting that partners across the public and private sectors lack a clear, shared, and real-time picture of the fraud threat, delaying collective disruption.[6]
Privacy at all costs	Privacy and data protection laws, while essential, can inadvertently hinder effective prevention and detection. Whilst this is changing (for example, the UK's Data (Use and Access) Act 2025 which establishes fraud prevention as a lawful basis for sharing data)[7] uncertainties remain causing corporates to hesitate over data sharing and we must ask ourselves if we have got the balance between privacy and protection set correctly.
Resource Constraints	Law enforcement investment is not commensurate with the scale of the threat.
Not using the tools we have	Sharing data is critical but challenging. There are points in our ecosystem (such as faster payments networks), where data already sits in aggregation. These capabilities are not fully exploited to prevent and detect fraud at scale and must be (as we argued here).[8]
Consumer Demand for Frictionless Services	The appetite for speed and ease drives instant payment adoption, significantly heightening fraud vulnerability where robust controls are not also present.
Pace	Criminals move at the pace of payments. The ecosystem works at the pace of legislation. This enables them to move huge quantities of money at pace across borders and between institutions with relative impunity. Criminals will always move faster than institutions, but we must do what we can to close the gap.

[5] Over £600 million stolen by fraudsters in first half of 2025 | Insights | UK Finance

[6] CP 1523 – Fraud Strategy 2026-2029 Disrupting crime, supporting economic resilience and delivering justice, page 14

[7] CP 1523 – Fraud Strategy 2026-2029 Disrupting crime, supporting economic resilience and delivering justice, page 16

[8] Leveraging the payments architecture in the fight against economic crime | Deloitte UK

What we can do – tactical options

The tide is turning, and governments are increasingly seeking to do more. For example, the UK Government's Fraud Strategy 2026–2029, launched in March 2026 and backed by over £250 million of investment, marks the most significant national commitment to tackling fraud in a generation. The UK Fraud Strategy sets out a comprehensive framework for disruption, resilience, and justice, but recognises that the response must be global – especially as digital platforms (social media, dating, e-commerce) are now central to both the problem and the solution.

In this vein there are promising tactical interventions already in play, many of which could be scaled or replicated internationally. Recent research by Future of Financial Intelligence Sharing (FFIS) has profiled a range of collaborative platforms, detailing capabilities such as consortium analytics, joint investigations, warning functions, tracing, and combined transaction monitoring. Increasingly, these platforms use privacy-enhancing technologies, like federated learning and homomorphic encryption, to enable secure data sharing without exposing sensitive information. This opens up a range of new options which can be deployed:

COLLABORATIVE TYPOLOGY DEVELOPMENT:

Jointly developing and sharing typologies of economic crime threats.

ENHANCED MESSAGING:

Bilateral and multiparty communication platforms for real-time intelligence sharing.

CONSORTIUM ANALYTICS:

Multi-party platforms that aggregate intelligence and deliver risk scores, revealing threats invisible to any single participant.

JOINT INVESTIGATIONS:

Both single-sector and public-private collaborative investigations.

WARNING AND TRACING FUNCTIONS:

Adverse incident databases and rapid alert chains to track money flows across networks.

COMBINED TRANSACTION MONITORING:

Partnership-based monitoring to detect suspicious patterns.

KYC DATA COMPARISONS:

Cross-entity verification to identify inconsistencies and prevent identity fraud.

The following are examples of effective current practices:

The Cifas National Fraud Database in the UK is a leading example of a collaborative platform that enables banks and other organisations to share intelligence on known fraudsters, saving members an estimated £2.1bn in 2024.[9]

In the US, Section 314(b) of the USA PATRIOT Act provides a legal basis for information sharing between financial institutions to detect and prevent money laundering and fraud.[10]

The FedNow Scam Classifier Model in the US and the pan-European fraud taxonomy developed by EBA Clearing are examples of efforts to standardise fraud typologies and improve data interoperability.[11]

Additionally, the UK is set to launch the Online Crime Centre (OCC), with £31 million of investment, to be a public-private data-sharing hub led by the Home Office and National Crime Agency. Bringing together law enforcement, the intelligence community, and key private sector partners, the OCC will enable rapid analysis and sharing of data to disrupt online fraud and high-volume cybercrime. This collaborative model aims to inform proactive interventions, strengthen platform defences, and could serve as a blueprint for international replication.

[9] Fraud Prevention | Identity Fraud | Protective Registration | Cifas

[10] Section 314(b) Fact Sheet

[11] FedNow, 2024; EBA Clearing

Raising our ambition: Systemic levers for change

To make a real impact, we must think bigger and act collectively. Key levers include:

International Collaboration	Enhanced cross-border partnerships, potentially culminating in a global Public-Private Partnership (PPP) to tackle fraud.
Sector Bridging	Expanding PPPs to include social media, telecoms, and other critical enablers.
Investment in What Works	Scaling up proven interventions such as counter fraud intelligence hubs.
Global Taxonomy and Standards	Developing a universal fraud taxonomy and international data standards to enable interoperability.
Legal Powers and Clarity	Leveraging existing legal frameworks (e.g. GDPR legitimate interest), utilising imminent opportunities (e.g. AMLR Article 75), and creating new legislation where needed. As an example, Payment Services Directive 3 will introduce stricter protections for victims of impersonation fraud, where platform companies will be liable to compensate banks and payment firms who have reimbursed defrauded customers, if the platform was informed of the fraudulent content on their platform and failed to remove it. Similarly, policymakers are increasingly focussing on how online services can be misused to facilitate fraudulent activity, and starting to introduce regulation aimed at combatting this.[12] We must ensure we use these new powers to best effect.
Outcome-based Regulation	Ensuring fraud regulatory focus includes consideration of each sector and institutions' contribution to and participation in activities that not only ensure compliance but also lead directly to measurable crime prevention.
Narrative Shift	Rebalancing the privacy vs. protection debate to ensure the right to safety is not overshadowed.
AI as a Force for Good	Connecting data responsibly to harness AI for proactive fraud prevention.
Enforcement Investment	Aligning law enforcement and regulatory resources with the scale of the threat.
Infrastructure Optimisation	Using payment architectures and standards (e.g., ISO20022) for centralised analysis and rapid response.

[12] Deloitte Digital Regulatory Outlook 2026

Towards a global response: A ‘FATF for fraud’

The challenges of policy, law, data, incentives, and outcomes demand a more coordinated approach. The anti-money laundering community has built an architecture – anchored by the Financial Action Task Force (“FATF”) that, while imperfect, provides a foundation for global cooperation. For example, every country has a Financial Intelligence Unit to report to, and mechanisms exist for information exchange domestically and cross-border.

It is time to learn from the FATF experience and apply the best of its model to fraud. A successful outcome for the global community would be a commitment to establish a ‘FATF for fraud’ – a body to set standards, measure effectiveness, and drive coordinated action against this global threat. To turn this into reality we need to be discussing:

- Which tactical options are most effective in your context?
- What barriers exist to greater collaboration, and how can they be overcome?
- How can we build momentum for a global, coordinated response to fraud?

Conclusion

Fraud is a global crisis, but it is also an opportunity for innovation and collaboration. By building consensus, investing in what works, and adopting a truly global approach, we can begin to turn the tide. Let us seize the opportunity to create a safer, more resilient financial system for all.

Contacts

Chris Bostock

Partner, Forensic & Financial Crime

cbostock@deloitte.co.uk

+44 20 7007 4355

Amber Andrade

Partner, Forensic & Financial Crime

amandrade@deloitte.co.uk

+44 20 7007 3169

Deloitte.