A Global Framework for Tackling Fraud and Scams: **Practical Suggestions for Collective Action**

FINAL:MARCH 2026

Introduction: The Scale and Urgency of the Challenge

Fraud and scams have reached epidemic proportions globally, costing economies hundreds of billions of dollars annually, eroding public trust in digital and financial systems. According to the Global Anti-Scam Alliance (GASA), in 2024 scams cost consumers over US$500bn worldwide – a figure that continues to rise as criminals exploit digital platforms, cross-border transactions, and institutional silos[1].

In the UK alone, fraud is estimated to cost £219bn per year, more than the entire health budget,[2] with 4.2 million incidents reported in 2025 – a 31% increase from the previous year.[3] Fraud is no longer a niche issue; it is a systemic threat. It undermines economic stability, public services, and societal cohesion. Transnational Organised Crime Groups (TOCs) operate with impunity, leveraging the anonymity of digital platforms, the speed of cross-border payments, and the fragmentation of national responses.

Yet, despite its scale, fraud often remains under-prioritised, under-resourced, and poorly coordinated – both within and between countries.

This multi-stakeholder recommendation sets out a global policy framework for action, focusing on three critical pillars:

1.Political Leadership and System Governance

The need for Governments to elevate fraud as a national and international priority, providing clear accountability, resources, and strategic direction. This must be at national and international levels to help set standards and hold nations to account.

2.Data Sharing

Breaking down silos between sectors (financial services, telecoms, technology, law enforcement) to enable real-time data and intelligence sharing and the collective disruption of fraud networks, at national levels and across borders globally.

3.Enabling Conditions for Collaboration and Success

Legal, technical, and cultural shifts required to facilitate trust, proportionality, and speed in the response to fraud sand scams, by enabling collaboration particularly for the sharing of data, while protecting privacy and civil liberties.

1. Research | Global Anti Scam Alliance (GASA)
2. Annual Fraud Indicator | Crowe UK
3. Crime in England and Wales - Office for National Statistics

1. Political leadership and System Governance

Political Leadership: Fraud as a National and International Priority

The Problem: Fragmented Responses

Fraud thrives in environments where responsibility is diffuse, accountability is weak, and collaboration is optional. Historically, governments and law enforcement have treated fraud as a secondary issue, not a 'serious crime' like drug trafficking or people smuggling, delegating it too often to underfunded law enforcement units or relying on voluntary industry initiatives. The result has typically been a patchwork of disjointed efforts that criminals easily exploit.

Key failures include:

- Lack of central accountability: No single government department or minister is typically responsible for coordinating anti-fraud efforts across financial services, telecoms, technology, and law enforcement.
- Misaligned responses: Private sector actors (banks, tech platforms, telecoms) have been slow to realise and find strategic responses to the rapid rise and extent of fraud and scams in recent years, leading to gaps in detection and inconsistent enforcement.
- An imbalance between safety and ease of use for consumers: Creating vulnerabilities that are exploited by criminals. The goal is an easy and safe customer journey.
- Underinvestment in enforcement: Despite fraud often ranking as the number one reported crime in many jurisdictions, policing resources remain woefully inadequate, with fraud investigations often deprioritised in favour of other crimes (e.g., fraud accounting for 44% of all crime in the UK, but only 1% of policing resource).

A New Model: System Leadership by Policymakers

To reverse this trend, Governments must treat fraud as a Tier 1 threat – on par with terrorism, cyber warfare, and organised crime. This requires:

A. Designating a Senior Ministerial Lead

Every country should appoint a Fraud Minister (or equivalent) with cross-departmental authority to:

- Set national fraud reduction targets and report annually to parliament on progress.
- Coordinate between relevant agencies, particularly financial regulators, authorities in charge of telecom and digital matters, and law enforcement.
- Ensure consistent funding and resourcing for fraud prevention, disruption, and victim support.
- Lead international engagement to shape a common response internationally.

B. Establishing Clear National Strategies

Governments must publish time-bound, measurable fraud strategies that:

- Define roles and responsibilities for public bodies and agencies.
- Establish clear objectives for fraud detection, reporting, and victim support, together with industry.
- Are the subject of regular public 'Transparency Reports' on efforts made.

C. International Alignment on Standards and Enforcement

Fraud is a transnational crime, yet responses remain largely national. Governments working with industry must:

- Back and encourage international initiatives that help prevent fraud.
- Develop best practices and meaningful public and private collaboration across key jurisdictions to help break down the current patchwork of national responses and conflicting approaches.

To enable greater enforcement and determined action against TOCs, Governments should:

- Harmonise legal definitions of fraud and scams to enable cross-border investigations, including where needed to confirm its serious criminal nature
- Establish international task forces (for instance under INTERPOL, the UNODC or Financial Action Taskforce (FATF) to coordinate disruption of global fraud networks.
- Streamline/create mutual recognition frameworks for evidence sharing and asset recovery.
- Clarify the intersection between consumer protection and anti-fraud laws with other legislation such as data protection and competition rules, to ensure that actions narrowly taken to combat scams are unambiguously possible under the law, with oversight internationally through an appropriately empowered body (eg FATF or UNODC).

Case Study: The UK's 2025 Fraud Strategy

The UK Government's Fraud Strategy has set a global benchmark for driving a coherent and collaborative national approach to tackling fraud. Key elements requested by industry and civil society and delivered in the new strategy include:

- Legislating to extend fraud prevention duties to all online advertising intermediaries (not just those covered by the Online Safety Act).
- Mandating real-time data sharing between banks, telecoms, and tech platforms.
- Committing to sustainable funding for fraud policing and victim support.

D. Delivering Change: The Role of National Anti-Scam Centres

National Anti-Scam Centres (NASCs) – such as those in Australia, Singapore, and Taiwan – demonstrate how centralised, multi-disciplinary coordination can transform fraud responses. Their success lies in:

- Breaking down silos: Bringing together banks, telecoms, tech platforms, and law enforcement as well as all relevant government agencies and regulators under one roof or coordinating structure.
- Real-time intelligence sharing: Enabling the rapid disruption of scams (e.g., freezing accounts, taking down fraudulent websites).
- Public-private fusion cells: Targeting high-harm scams with time-bound task forces.

2. Data Sharing and Collaboration

Data Sharing: The Backbone of Fraud Prevention

The Problem: Siloed Data, Slow Responses

Fraudsters operate at network speed; defenders move at bureaucratic speed. The biggest obstacle to effective fraud prevention is the lack of real-time, cross-sector data sharing. Currently, the various key relevant impacted industries – telecom, tech, banks – often have visibility on only a small part of a scam's 'kill chain' and may be limited in how much intelligence they do or can share with other private actors or law enforcement. This fragmentation allows criminals to exploit gaps undetected.

The Solution: Outcome-Driven Data Sharing

To disrupt fraud networks, Governments must encourage and facilitate secure, proportional data sharing between key sectors, focusing on prevention and enforcement. This requires:

A. Legal and Regulatory Enablers

Clarifying "safe harbours" for data sharing both nationally and globally: Many organisations fear legal repercussions (e.g., data protections violations) when sharing fraud-related data. Governments must:

- Work through the UNODC, to establish a global safe harbour by creating an International Fraud Data Standard (IFDS) built around globally recognised standard terms and a certification system. This would form the basis of a trust framework, the connective tissue to enable banks, Payment Service Providers, platforms, telecoms, and crypto providers to take action with confidence.
- Issue clear guidance on what constitutes lawful data sharing for fraud prevention, including in relation to proportionality and measurement.
- Establish explicit exemptions for sharing data with trusted anti-fraud bodies (e.g., national fraud databases) as well as other relevant industry actors and intermediaries.

B. Technical Infrastructure for Secure Sharing

- National fraud data platforms: Governments should back existing, established and secure, interoperable databases where these do not exist, to allow for flows of critical data. These could enable, among others:
    - Financial institutions to share payment fraud patterns and identified compromised financial assets such as bank accounts and suspect transactions.
    - Telecoms providers to contribute SMS/call spoofing data and compromised telecom assets such as SIM cards exploited by scammers.
    - Tech platforms to report or receive reports of fraudulent ads, profiles, and domains.
- Standardised APIs and protocols: To ensure data can be shared in real time without manual intervention.

3. Enabling Conditions for Collaboration and Success

How Governments Can Enable Collaboration

(i) Aligning Incentives

- Convene key sectors to exchange best practices and establish common approaches and shared objectives, including on success criteria and the measurement of impact.
- Regulatory incentives:
    - Offer reduced compliance burdens for firms that participate in data-sharing schemes.
    - Liability protections: Shield organisations from legal risks, including when taking action against scams and sharing data and intelligence in good faith. Governments can incentivise companies to take preventive action through the adoption of 'Good Samaritan' liability protections, which shield intermediaries from liability for their proactive efforts against scams.
- Public recognition: Highlight best practices in annual reports to encourage participation.

(ii) Building Trust Through Governance

- Multi-stakeholder coordination: Bring together industry, law enforcement, and civil society to ensure transparency and implement practical collaborations.
- Independent audits: Verify that data is used proportionately and protected securely.

(iii) Trusted Intermediaries to Facilitate Collaboration

- Anti-fraud hubs: For example, Cifas in the UK, ScamShield in Singapore, Global Signal Exchange at international level can act as neutral conveners, aggregating and analysing data while protecting commercial sensitivities.
- Public-private fusion cells: Acting on shared data, time-bound taskforces (e.g., Australia's National Anti-Scam Centre) can target high-harm scams like investment fraud or romance scams.

The Global Nature of Fraud: A Unified Front Against Fraud

Fraud does not respect borders. Criminals exploit:

- Cross-border payments (e.g., money mules moving funds between jurisdictions).
- International telecoms networks (e.g., SIM-swap fraud originating in one country, targeting victims in another, with no caller identification).
- The global reach of technology (e.g., fraudulent content hosted on servers in one country, seen by users worldwide).

Yet, international cooperation remains ad hoc. To change this, Governments must:

i. Establish a Global Anti-Fraud Framework

- Common definitions: Agree on standardised terminology for fraud types (e.g., 'investment scams', 'phishing').
- Mutual legal assistance: Streamline cross-border evidence sharing and investigations.
- Joint disruption operations: Enable real-time coordination between national anti-fraud centres and other relevant actors, across borders, to disrupt scam operations such as freezing accounts, blocking malicious domains, and recovering funds.

ii. Leverage Existing Institutions

- INTERPOL's Global Financial Crime Task Force: Expand its mandate to include fraud intelligence sharing and investigations.
- FATF-Style Body for Fraud: Create an international standard-setting body (e.g., modelled on the Financial Action Task Force) to monitor compliance and hold to account those jurisdictions who are slow to adopt the framework.

iii. Support for Low-Capacity Countries

- Support training for nations with limited anti-fraud infrastructure and capacity.
- Regional hubs (e.g., in Africa, Southeast Asia) to pool resources and share intelligence.
- Ensure that low-capacity jurisdictions receive appropriate support to build effective fraud and scam prevention infrastructure in line with global standards.

Develop and Deploy Technical Solutions

Invest in responsible AI and policies that encourage technological innovation:

- Ensure that legislative frameworks allow for anti-fraud innovation, to leverage the potential of emerging technologies like AI to better prevent, detect, and respond to scams and fraud, and develop the tools necessary to counter the misuse of synthetic media such as deepfakes.
- Encourage the development and implementation of technical solutions to prevent, detect, and act against scams and fraud across the public and private sectors, including in-product user warnings and 'safety by design' principles.

Educating and Protecting People, Consumers, and Victims

Equipping people with information about scams remains a crucial element of fighting scams and fraud. Victim support is a societal requirement. Governments and relevant community actors should:

- Conduct public awareness campaigns: Particularly for vulnerable groups and extend to all types of organisations including small and medium-sized businesses.
- Provide clear and accessible reporting channels for citizens: Governments should make reporting to official channels clear and accessible for victims and witnesses of fraud and scams. Private actors should also have clear reporting channels for reports of suspicious activity exploiting their products and services.
- Provide appropriate victim support: Such as referrals to counselling, financial advice, and legal aid.

4. Conclusion: A Call to Action

Fraud is not an inevitability – it is a solvable problem, but only if Governments, industries, and civil society act together, urgently, and at scale.

The steps outlined in this suggested framework provide a blueprint for change:

- Elevate fraud to a Tier 1 threat with ministerial leadership and national strategies.
- Facilitate real-time, cross-sector data and intelligence sharing with legal protections and technical infrastructure, particular through the creation of internationally recognised standard
- Streamline the law and align incentives to encourage collaboration and action.
- Strengthen international cooperation through standardised frameworks and joint operations.
- Invest in National Anti-Scam Centres as instruments for coordination.

The cost of inaction is too high. Every day of delay means more victims, more losses, and more erosion of trust in our digital and financial systems.

The time for collective, decisive action is now.

This guide has been developed with input from a informal multi-stakeholder working group involving experts from organisations across the banking, telecom and technology industries and the public sector.

The contributing experts and organisations include: Konrad Shek - Advertising Association; Dr. Simon Miller - Cifas; Erica Stanford - CMS; Garry Lilburn - Cyber Defence Alliance; Jean-Jacques Sahel - Google; Marco Doeland - Dutch Banking Association (Nederlandse Vereniging van Banken); Carolina Caeiro and Emily Taylor - Oxford Information Labs; PayPal; Helen Fairfax-Wall and Adil Munim - Stop Scams UK; Colleagues at Teamviewer, Nick Sharp and Marc Knotts - UK National Crime Agency.

FINAL:MARCH 2026