UK Member State Initiative

Operationalising a Global Public-Private Partnership on Fraud

The following Member States of the United Nations, **Australia**, **Canada, France, Italy, Japan, New Zealand, the Republic of Korea, Singapore, the United Kingdom of Great Britain and Northern Ireland, and the United States of America** and the following private sector organisations and industry bodies (hereby referred to as Organisations), **Meta, Google, Amazon, Match Group, Virgin Media O2 and International Banking Federation**, endeavour to advance the following principles and commitments for a Global Public-Private Partnership on fraud (also referred to as scams)[1], which sets out a practical framework to implement best practices for multi-sector and stakeholder collaboration on this shared transnational threat:

1) **Shared Responsibility:** Fraud prevention and response is a collective duty for a multitude of actors across sectors and borders. It is built on the spirit of collaboration and a shared sense of urgency, whilst leveraging the complementary strengths of public and private actors within clear legal and policy frameworks and contextualising responses to different contexts

    - All Participants recognise that tackling fraud is an urgent priority. All acknowledge the evolving nature of fraud, including the strong links to wider criminality such as human trafficking and affirm the importance of collective, coordinated efforts to stay ahead of emerging threats.
    - Organisations will work with relevant public authorities, agencies, and partners, to effectively prevent and combat fraud.
    - Member States will seek to strengthen or establish effective policies to enhance cooperation with the private sector and other entities outside the public sector to respond to emerging fraud threats and hold criminals accountable.
    - Member States will aim to pursue effective policies to combat fraud, to learn from one another, and to adapt approaches as necessary.
    - All Participants recognise the importance of an international multi-sector and stakeholder approach to tackling fraud and acknowledge the need to explore collaborative solutions.

[1] *The UNODC defines fraud as 'fraud that deliberately uses deception by any method or medium with the intent to make a wrongful financial or other material gain which causes detriment to another'.*

2) **Proactive and coordinated Prevention:** Preventing fraud before it occurs, through coordinated cross-sectoral action based on standardised definitions and methodologies, risk analysis, is the best disruption strategy and most effective and sustainable defence.

- Member States will seek to prioritise engagement with the private sector when developing policies to detect and prevent fraud, ensuring effective and appropriate mechanisms for collaboration.
- Organisations commit to putting in place reasonable and appropriate verification or Know Your Client (KYC) processes to prevent fraudsters from exploiting their services for scams and fraud.
- Organisations will, where possible, classify fraud, money muling and associated behaviours that enable fraud as non-compliant activities within their community standards, guidelines and/or terms of service/ conditions, ensuring these are supported by clear definitions.
- Organisations will strengthen or establish, maintain and update systems, processes and staff training to detect, prevent and act against attempted frauds knowingly occurring via their business models, while preserving records where appropriate and in accordance with applicable laws and regulations.
- Organisations commit to reducing the accessibility and reach of information systems and domains that demonstrate ineffectiveness at preventing abuse by those engaged in fraudulent activity, whilst ensuring that such actions do not affect legitimate digital infrastructure.

3) **Information sharing as Basis for Cooperation:** Timely, secure and lawful sharing of accurate and actionable data and information by all relevant actors, with due regard to data protection and privacy, is key to an effective fraud response.

- Member States will seek to minimise bureaucratic and/or restrictive barriers to information sharing, consistent with each jurisdiction's data protection laws and regulations, and leveraging existing agreements, providing clarity where required and possible.
- Organisations will proactively collaborate with stakeholders (that may include government, law enforcement, regulators and other industry partners) to share and act on information on fraud trends, signals and bad actors, domestically and internationally, in accordance with applicable laws and regulations.
- Organisations will strengthen or maintain existing reporting channels or explore establishing new mechanisms for law enforcement to enable quick and efficient two-way sharing of actionable information on fraudulent

activity, where appropriate and in accordance with applicable laws and regulations and the Organisation's Terms of Service.

- All Participants commit to horizon scanning, pooling shared knowledge and expertise on known threats, bad actors and new trends – including novel methodologies – and sharing this information with relevant public and private sector parties, as appropriate and as permitted by applicable laws and regulations.

4) **Victim Support:** Supporting victims of fraud is essential in order to rebuild trust and confidence and to learn from their experiences and facilitate their cooperation for an effective criminal justice response, enabling continuous improvement of preventive strategies, awareness efforts, and policy responses.

- Organisations will seek to have, or adopt, and maintain a simple, accessible and effective, and secure reporting function for users to report fraudulent contact, content and/or transactions.
- All Participants will endeavour to work with each other, and with victim support services, to deliver simple, tailored messaging and appropriate signposting, including providing timely guidance on next steps and safeguards.
- Organisations will seek to promptly review user or customer reports, taking reasonable steps to ensure the accuracy of their reviews, and where necessary take appropriate action including, but not limited to, the removal of content or the restriction of users or transactions.

5) **Education for the Public and Businesses:** Stronger and continuous public awareness, digital literacy and fraud prevention education are critical to reducing vulnerability and building widespread resilience against fraud.

- All Participants will endeavour to support the public in recognising, reporting, avoiding, and protecting themselves from fraud and associated harms.
- All Participants will aim to regularly promote public awareness campaigns and education initiatives to help individuals as well as public and private sector organisations recognise, avoid and report fraud.

6) **Innovation and Adaptability:** Leveraging collaborative innovation and emerging technologies is key to anticipating, preventing and disrupting evolving fraud schemes. This may include equipping stakeholders with the necessary skills and knowledge.

- All Participants will endeavour to develop and share, domestically and internationally, best practices to tackling of fraud with each other, including useful tools and expertise, whilst respecting trade secrets and confidentiality and in accordance with applicable laws and regulations.
- All Participants will endeavour to work together to develop and adopt new and novel technical solutions and ways of tackling fraud, domestically and internationally.
- Organisations where possible will invest in research and development of artificial intelligence and other emerging technologies to effectively and proactively counter fraud threats.
- Member States will encourage private sector innovation and initiatives to use artificial intelligence and other technologies to improve detection and action capabilities against fraud.

We, together, affirm our commitment to these Global Public-Private Partnership principles to tackle fraud, as a decisive step towards building a united and resilient global front against this growing threat.