Industry Accord Against Online Scams & Fraud

2026

Introduction

This Accord addresses the growing problem of online scams and fraud, specifically deceptive schemes targeting individuals or organizations with the intent of taking money and/or personal information, which impacts billions of users across the globe.

As technology becomes increasingly integrated into everyday life, it has become a primary target for scammers seeking to exploit legitimate service providers to steal consumers' personal information and money. The most damaging of these actors, often operating on behalf of or as part of transnational criminal syndicates, leverage sophisticated techniques to defraud individuals and organizations. In the past year, consumers lost an estimated $442 billion to scammers, underscoring the devastating financial and societal impact of these crimes.

While the signatories commit to implementing robust measures to protect consumers and combat scams, this Accord recognizes that a safer online consumer experience is a shared responsibility requiring a collective response across the entire ecosystem, including key private sector institutions targeted by scammers and the public sector. Each sector has a role in this collective response, and we call on other industries to adopt similar commitments to protect consumers from scams and fraud.

This Accord seeks to set expectations for how signatories will work across online services to counter scammers, in line with their own policies and practices as relevant to the commitments in the Accord.

It also seeks to drive a united industry response alongside governments, law enforcement, NGOs, and others working to combat fraud and scams. The Accord recognizes that in order to deal with this political, societal, and safety issue that is largely driven by transnational organized crime, there is an important role for public authorities to play, alongside the efforts of the private sector. We, the signatories, will work with governments to support implementation of all applicable laws and to build law enforcement capacity and resources to pursue criminal organizations.

We sign this Accord as a voluntary set of principles and actions to advance four goals:

- **Prevention:**
  Developing and implementing proactive actions to prevent scams, including robust security features, AI-powered detection systems, and clear usage policies.
- **Cooperation and Collective Learning:**
  Increasing cooperation and lawful information sharing among industry and with law enforcement agencies to further (i) identify financial fraud, particularly when committed by transnational criminal organizations; (ii) protect consumers; and (iii) improve our joint understanding of scams, countermeasures, and evolving threats.
- **Resilience:**
  Supporting secure digital transformation and the deployment of defensive tools, such as AI-based and other enhanced technology solutions, and enabling swift and proportionate responses to adversarial shifts and scam incidents.
- **Public Awareness:**
  Engaging in shared efforts to educate the public about scams and digital literacy, and ways citizens can protect themselves from being manipulated or deceived by scammers.

By working together, signatories of this Accord commit to leveraging their expertise, skills, resources, and influence to combat online scams and protect consumers worldwide.

Commitments

The signatories commit to the following voluntary principles and actions:

Prevention

- **Deploying Technical and In-Product Solutions:**
  - Design and/or deploy processes and mechanisms to identify and address scam and fraud attempts, in line with companies' unique product and service policies and where actionable signals are present.
  - Implement product features to enhance user security.
- **Implement and Enforce Anti-Scam Usage Policies:** Design and enforce in a timely manner acceptable use policies and terms of use that prohibit scams and fraud across participating companies' platforms, products, and services.
- **Verification:** Service providers should promote risk-based, proportionate verification mechanisms that are designed to reduce scams and negative impacts to legitimate users.
- **Authorization and Authentication:** Financial payment services that initiate and execute financial transactions (such as wire transfers, instant payments, or financial asset purchases) should be subject to higher-friction authorization and authentication requirements than surfaces that facilitate communication or social interaction.

Cooperation and Collective Learning

- **Undertake collective efforts to share best practices and other information,** as permitted by applicable law related to scam trends, detection, and prevention through international forums like the Global Anti-Scam Alliance, the Tech Against Scams Coalition, and platforms like the Global Signal Exchange.
- **Explore pathways to share best-in-class mechanisms and processes** for detecting, preventing, and responding to scams.
- **Provide**, or adopt, process for law enforcement and trusted government partners to report suspected scam activity occurring on the companies' services

Resilience

- **Secure Digital Transformation** by developing and/or deploying secure technology across all sectors and adopting cybersecurity best practices such as modern and regularly-updated operating systems and hardware.

- **Provide swift responses** to adversarial shifts and incidents of scams and fraud. These should be proportionate to reduce the risk of unintended consequences.

- **Collaboration and Innovation:** Foster collaboration between industry, government, and civil society to develop and deploy defensive tools and increase resources available to address the shared threat.

- **Protection of User Privacy and Freedom of Expression:** Efforts to counter fraud and scams need to balance countering fraud while also protecting the fundamental right to speech and privacy.

Public Awareness (Education and Empowerment)

- **Engage in joint efforts to educate** the public about how to identify and protect themselves from scams. This includes targeted risk-based messaging when users may be exposed to additional risk.

- **Provide clear and accessible channels** for customers and users to report scams on companies' platforms, products, and services.

Addressing the political, economic and societal challenges presented by scams and fraud is a shared responsibility requiring collective and sustained action, including both the public sector and other industries impacted by the problem.

We suggest below specific actions that these sectors should take to combat scams, alongside and in coordination with the joint efforts of the signatories outlined in this Accord. This is not a challenge that any sector can solve in isolation. It requires a unified, cross-industry, and whole-of-society response to effectively combat the transnational organized criminal networks that are behind much of the scam activity. Therefore, we call upon governments, in partnership with the signatories, to take decisive actions to create a safer online environment for everyone, including:

- **Elevate Scam Prevention as a National Priority with Dedicated Resources:** We call upon governments to formally declare scam prevention a national priority. This declaration should be accompanied by explicit budgeting for anti-scam initiatives, including increased funding for law enforcement personnel, specialized tools (e.g., crypto tracing capabilities), and training for law enforcement. It should also be accompanied by coordinated diplomatic engagement, including criminally sanctioning/formally proscribing groups, networks and companies involved in scams and fraud, a step which in turn supports the efforts of private companies to counter these entities.

- **Modernize Government's Data Capabilities and Streamline Reporting:** Governments must urgently invest in modernizing their data collection and analysis capabilities for combating financial crimes, specifically improving existing databases.

- **Foster Cross-Border and Cross-Sector Information Sharing:** We emphasize the critical need for enhanced cooperation and lawful information sharing across industries and with law enforcement, both domestically and internationally. Governments should adopt and implement laws that facilitate the sharing of relevant, sensitive data for fraud detection and prevention, while safeguarding privacy and security.

- **Deconflict Laws and Provide Safe Harbors to Enable Action:** Policymakers must review and harmonize existing legal and regulatory frameworks, particularly at the intersection of consumer safety, privacy, anti-fraud laws, data protection, and competition rules, to eliminate ambiguities that hinder proactive anti-scam efforts. This clarity, coupled with "Good Samaritan" liability protections, is essential to shield companies acting in good faith to prevent or disrupt scams from undue civil or criminal liability or regulatory penalties.

Tackling online fraud and scams is a complex and ongoing challenge that necessitates a cross-industry response and collaboration with various stakeholder groups. Operating in silos will lead to missed synergies and gaps in the overall approach to tackling transnational organized criminals responsible for a significant portion of the scam problem. We welcome other sectors to join us by:

- **Scaling Bilateral Information Sharing:** Invest resources in improving the information sharing infrastructure, significantly expanding its capacity and reach, and reducing friction in its utilization by both the private sector and law enforcement.

- **Investing in Responsible AI and New Technologies:** Foster collaboration between industry, government, and civil society to develop and deploy defensive tools and increase resources available to address the shared threat. This includes supporting secure digital transformation by developing and/or deploying secure technology across all sectors and adopting cybersecurity best practices such as modern and regularly-updated operating systems and hardware, and leveraging AI to accelerate the detection of fraud and scams, thereby scaling approaches to combat abuse and harm on platforms.

Signatories:

Adobe

Google

OpenAI

LinkedIn

Match Group

Meta

amazon

Microsoft

LEVI STRAUSS & CO.