

# **Approaches to combating online fraud**

The European FinTech Association (EFA) welcomes the opportunity to contribute to the European Commission's (Commission) action plan on online fraud.

We believe that to effectively prevent and mitigate online fraud, all players in the fraud chain must collaborate closely and establish practices to prevent fraud from originating from, or taking place through their services. Simultaneously, consumers should be provided with the necessary tools and information to recognise attempted fraud.

## **The rise of APP Fraud**

Traditionally, payment fraud involves unauthorised transactions or technical breaches, which are largely addressed under EU frameworks (PSD3/R, AML, etc.). However, As the Commission has observed, scams, i.e. Authorised Push Payment (APP), including impersonation fraud, has emerged as one of the most significant and rapidly expanding forms of cyber-enabled crime globally, including in the EU. These typologies exploit social engineering techniques to manipulate consumers into authorising payments or disclosing sensitive information. Generative AI represents a fundamental shift, enabling voice and identity impersonation as well as sophisticated automated fraud attacks that can bypass traditional diligence and investigation tools at scale. As a result, APP fraud now represents a major threat to consumer trust, financial stability, and the integrity of the EU payments landscape.

In most cases, consumers are first exposed to APP fraud through channels outside the remit of the financial sector. Evidence indicates that more than half of scams originate on non-payment platforms such as social media (e.g., Facebook, TikTok, Instagram), traditional telecommunications channels (e.g., spoofed phone calls, text messaging), or messaging applications (e.g., WhatsApp, Signal). By the time a payment is initiated through a payment service provider (PSP), the victim has already been deceived. Despite the spreadout nature of fraud liability in those cases, PSPs remain the only actors in the fraud chain currently expected to detect, prevent, and, where unsuccessful, reimburse fraudulent transactions – even though the root cause and early stages of these scams lie beyond their control. One sector alone cannot manage risk across the entire digital economy. The EFA firmly believes that tackling scams adequately requires distinct policies focused on upstream prevention and coordinated cross-sector, whole-of-government action.

## **Implementation of the Payment Services Regulation (PSR)**

The PSR will soon be adopted and will bring incremental improvements to fraud prevention and mitigation and the updated rules are a step towards the right direction. Therefore, it is vital that the new PSR framework is effectively implemented. However, in our view, more should be done to establish a comprehensive, systemwide framework addressing all fraud chain participants.

Regarding the implementation of the PSR, we emphasise a need for a swift establishment of the Commission's "Platform" (Art. 83b (1) of the draft agreement) is crucial to enable collaboration and

determine best practices on fraud prevention. On secondary liability between PSPs and ICT providers (art.58-59 and 59a of the draft agreement), we welcome co-legislators' efforts to hold other entities liable when it is found that their platforms harbour the origin of fraud. We also welcome the addition of a new Recital, calling for arrangements to facilitate data sharing between PSPs and ICT platforms, with the aim of "identifying fraudulent actors and fraudulent behaviour". These measures would ensure that PSPs are not held responsible for risks lying outside of their control, and allow for risk mitigation on a larger scale.

We also support the Commission's proposal to improve cross-border and international information sharing. However, if private sector stakeholders participate in these exchanges, the EFA stresses that administrative and compliance requirements should be minimized.

### **A whole-of-economy approach**

While the PSR will bring more collaboration between the fraud chair participants, we believe that to adequately prevent and mitigate new forms of fraud, including scams, the cross-sectoral approach must go beyond information sharing to establish clear accountability across the fraud chain. Each actor should mitigate risks within its sphere of control, supported by baseline sectoral anti-scam obligations (e.g. proactive and rapid takedown of scam content, SIM-swap protections, etc.) and aligned incentives (liability). Without this, interventions at the payment stage will remain reactive and insufficient. Existing frameworks, such as the Digital Services Act and the Payment Services Regulation do not fully address the entire scam lifecycle.

### **Cross-sector collaboration in fighting fraud**

Combating online fraud requires a unified, operational front across the entire ecosystem, linking all the relevant actors, such as financial institutions, online intermediaries, law enforcement, and Financial Intelligence Units (FIUs). Currently, the fragmentation of intelligence across disparate regulatory silos and jurisdictions hinders our collective response.

The EU's Action Plan should fill this important gap by prioritising the establishment of robust, legally certain frameworks for public-private information sharing. By institutionalizing the exchange of risk indicators and aligning fraud prevention with existing AML/CFT architectures, the EU can finally move from reactive mitigation to proactive disruption, intercepting criminal activity before harm is realized.

### **Online fraud and organised crime**

In recent years, online scams have become a part of organised crime, profiting and financing criminal organisations. Therefore, it is vital to also address fraud in this context, and we believe that the upcoming Action Plan should also address the role of law enforcement. As scams have become the remit of organised, transnational crime, a coordinated whole-of-government approach is required, supported by stronger law-enforcement capabilities, improved cross-border cooperation, and central EU-level coordination. Europol is uniquely positioned to act as this hub, and we should support strengthening its role through enhanced intelligence sharing, coordinated operations, and dedicated intelligence-led mechanisms focused on scams.

### **Supporting and empowering the EU citizens**

The EFA agrees with the Commission's suggestion to improve support for fraud victims. We however would emphasise that consumers must be equipped with the necessary information and tools to recognise scams.

While the players involved in the fraud chain must do their best to combat fraud, optimal results will be reached when fewer consumers fall victim to fraudulent practices in the first place. Often overlooked, this is a key link of the fraud-prevention chain, and one that is currently missing from the consultation document.

In addition, streamlining victim reporting will have a hugely beneficial impact on EU citizens. At the moment, this is a big gap across the EU, and EFA believes that it is crucial for information to be reportable once and then accessible in real-time by anyone who needs it in order to combat fraud effectively.