Electronic Money Association
67 Square Marie-Louise
Brussels 1000
Belgium
www.e-ma.org

DG HOME
European Commission
Rue de la Loi 200 / Wetstraat 200,
1049 Bruxelles/Brussel,
Belgium

13 February 2026

Dear Sir/Madam

Re: EMA Response to Call for Evidence Consultation: Fighting Online Fraud - Action Plan

The EMA is the EU trade body representing electronic money issuers and alternative payment service providers. Our members include leading payments and e-commerce businesses worldwide, providing online payments, card-based products, electronic vouchers, and mobile payment instruments. Most members operate across the EU, most frequently on a cross-border basis. A list of current EMA members is provided at the end of this document.

I would be grateful for your consideration of our comments and proposals.

Yours faithfully,

Dr Thaer Sabri
Chief Executive Officer
Electronic Money Association

We welcome the Commission's initiative to reinforce the framework for preventing and addressing fraud through a dedicated Action Plan. As the Call for Evidence notes, online fraud has reached unprecedented levels and exploits advances in automation and AI.

We would be grateful for your consideration of our comments and proposals regarding the following key topics:

1. Involvement of all actors involved in the payment chain

The Call for Evidence highlights the need for a "whole-of-society" approach involving public and private sectors to build collective resilience.

We propose that the Action Plan formalises the involvement of the payments sector in the "cooperation mechanisms" mentioned. As PSPs are predominantly the first actor in detecting the "money mule" networks and fraudulent crypto-asset transfers mentioned in the initiative, their active involvement in the design of preventative measures is essential. Given the Action Plan's emphasis on detecting, tracing and disrupting fraud proceeds channelled through crypto-asset transfers, the expertise provided by PSP would be particularly valuable in strengthening the EU's cross-border 'follow-the-money' capabilities.

Cooperation mechanisms must also involve other actors, such as social media platforms, hosting service providers, and telecom providers. These entities are essential because they frequently serve as the initial "point of entry" for the fraudulent activity, and possess valuable data and knowledge that can aid in the fight against online fraud. Every stakeholder in the scam lifecycle—including entry-point actors not directly involved in the payment chain—must mitigate risks within their sphere of control. This requires clear sectoral mandates and incentives aligned to ensure compliance. Ultimately, defeating fraud requires a holistic approach that addresses the entire scam lifecycle.

It is essential to maintain and assure consistency of treatment of fraud typologies at EU level. Therefore, we suggest that the Commission establishes a permanent dialogue structure with the electronic money and payments industry to ensure that the "action plan against online fraud" remains responsive to the rapidly evolving "crime as a service" tools used by fraudsters. We understand that the Payment Service Regulation (PSR) may create a platform that would have this objective.

2. Data Sharing

We note that the Call for Evidence identifies the lack of information sharing between the private sector and public authorities as a specific problem (Problem 7), which hinders the identification and prosecution of fraudsters.

We strongly support the objective to strengthen coordination through the sharing of relevant information. However, current legal frameworks often create barriers to effective collaboration: Payment Service Providers (PSPs) operating cross-border often face difficulties when attempting to collaborate to mitigate the impact on fraud victims.

We recommend that the Action Plan prioritizes a harmonised EU legal framework that explicitly permits and encourages the sharing of fraud data and typologies between PSPs, and between PSPs and law enforcement, without conflicting with data protection (GDPR) or banking secrecy laws. We note that the Payment Service Regulation (PSR) currently being negotiated may include provisions that support data sharing.

- *Encouraging industry practice*: In many Member States, it is good industry practice for PSPs to notify each other of transactions flagged as fraudulent to facilitate the freezing and return of funds. The Action Plan should ensure this practice is legally supported across all Member States to prevent "safe havens" for fraudsters due to fragmented national laws.
- *Real-time monitoring*: To support the detection of fraud using real-time transaction monitoring, PSPs require access to broader data sets regarding emerging fraud typologies. We would also support the publication of fraud data collected by public entities as soon as possible, to allow PSPs to monitor and mitigate emerging fraud threats.

3. Communication between the anti-fraud actors

Effective communication is critical in the "follow-the-money" response. This applies both to communication between authorities and the private sector, and communication between PSPs.

We note that the current lack of coordination and collaboration between stakeholders is a major barrier (Problem 6).

- *Cross-border communication*: We support measures that streamline the communication channels between Financial Intelligence Units (FIUs) and PSPs across borders. Currently, the speed at which funds move —particularly via instant payments and crypto-assets— outpaces the speed of formal communication requests between national authorities.
- *Operational communication*: We recommend that the Action Plan includes guidelines for the rapid communication of "fraud flags" between sending and receiving PSPs. Cross-border cooperation is essential to disrupt scam proceeds. A harmonised standard for communicating fraud suspicions would allow for faster freezing and recovery of assets.

4. Payment Service Users awareness & education

We agree with the assessment that a lack of awareness about the nature and forms of online fraud makes it difficult for victims to avoid crime (Problem 3).

We propose that awareness-raising campaigns should not be the sole responsibility of PSPs but should be a European coordinated effort involving the platforms where the fraud originates (e.g., social media, telecom providers, and DNS service providers).

- *Harmonised messaging:* To provide consumers with a consistent experience, EU-wide guidelines on fraud awareness would be beneficial.
- *Victim Support*: We welcome the focus on enhancing victim support. Awareness campaigns must clearly signpost how and where to report fraud to ensure victims do not suffer from additional stress from the reporting process.

5. Role of Law Enforcement

Because modern scams are the domain of organised, transnational crime, and do not care about borders, the EU must adopt a coordinated, whole-of-government approach.

This strategy requires bolstered law enforcement, seamless cross-border cooperation, and centralised EU-level oversight. Europol is uniquely positioned to serve as this central hub; the EMA believes that the EU should further empower it through enhanced intelligence sharing, joint operations, and dedicated, intelligence-led mechanisms specifically targeting scams.

Members of the EMA, as of February 2026

Airbnb Inc
Aircash
Airwallex (UK) Limited
Amazon
American Express
Banked
Benjamin Finance Ltd.
Bitstamp
Blackhawk Network EMEA Limited
Boku Inc
Booking Holdings Financial Services International Limited
BVNK
Bytedance Payments
Cardaq Ltd
CashFlows
Circle
Coinbase
Crypto.com
Currenxie Technologies Limited
Decta Limited
Deel
eBay Sarl
ECOMMPAY Limited
emerchantpay Group Ltd
EML Payments
EPG Financial Services Limited
eToro Money
Etsy Ireland UC
Euronet Worldwide Inc
Finance Incorporated Limited
Financial House Limited
FinXP
First Rate Exchange Services
Fiserv
Flywire
Gemini
Globepay Limited
GoCardless Ltd
Google Payment Ltd
IDT Financial Services Limited
iFAST Global Bank Limited
Imagor SA
Ixaris Systems Ltd
J. P. Morgan Mobility Payments Solutions S. A.
Kraken
Lightspark Group, Inc.
Modulr Finance B.V.
MONAVATE
MONETLEY LTD
Moneyhub Financial Technology Ltd
Moorwand Ltd
MuchBetter
myPOS Payments Ltd
Navro Group Limited
Newrails, UAB
Nuvei Financial Services Ltd
OFX
OKX
OpenPayd
Owl Payments Europe Limited
Own.Solutions
Papaya Global / Azimo
Park Card Services Limited
Payhawk Financial Services Limited
Paymentsense Limited
Payoneer Europe Limited
PayPal
Paysafe Group
Paysend EU DAC
Peratera UK Ltd
Plaid B.V.
Pleo Financial Services A/S
PPS
Push Labs Limited
Remitly
Revolut
Ripple
Satispay Europe S.A.
Securiclick Limited
Segpay
Soldo Financial Services Ireland DAC
Square
Stripe
SumUp Limited
Syspay Ltd
TransactPay
TransferGo Ltd
TransferMate Global Payments
TrueLayer Limited
Uber BV
Unzer Luxembourg SA
VallettaPay
Vitesse PSP Ltd
VIVA WALLET.COM LTD
Weavr Limited
WEX Europe UK Limited
Wise
WorldFirst
Worldpay