**Electronic Money Association**
Crescent House
5 The Crescent
Surbiton, Surrey
KT6 4BN
United Kingdom
Telephone: +44 (0) 20 8399 2066
www.e-ma.org

By online submission

11 April 2025

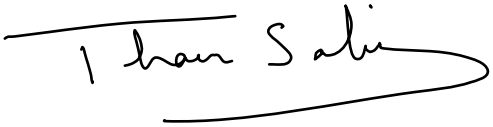
Dear Treasury Committee

**Re: EMA Submission – Treasury Committee Call for Evidence on Artificial Intelligence in Financial Services**

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 sincerely,



Dr Thaer Sabri
Chief Executive Officer
Electronic Money Association

## EMA response

**Q1. How is AI currently used in different sectors of financial services, and how is this likely to change over the next ten years?**

AI is increasingly being used across business operations within the UK financial services sector, including the e-money and payments sector, which the EMA represents. Its adoption has accelerated in particular due to innovations spurred by the COVID-19 pandemic. In financial services, AI represents an evolution of existing methodologies, as firms use it to improve their established rules-based models. However, AI systems still require human input and oversight, and fully automated decisions are not yet common. Across the EMA membership, over 64%[1] of firms have already deployed AI in their operations.

The most common AI use cases across members include:

- Fraud detection and transaction monitoring: AI can enhance transaction monitoring by identifying unusual patterns that indicate fraud. Machine learning models help differentiate legitimate transactions from fraudulent ones in real time, improving detection rates and reducing false positives. AI also supports financial crime compliance by streamlining customer onboarding and aiding Know Your Customer (KYC) and Anti-Money Laundering (AML) checks. AI can analyse customer data, flag suspicious activities, and strengthen due diligence processes.
- Customer service automation: AI chatbots and virtual assistants can improve user experience by handling queries and helping support staff to resolve disputes.
- Compliance and onboarding: AI helps Payment Service Providers ("PSPs") automate controls and reporting processes for regulations such as the Payment Services Directive[2], and for firms operating in Europe, the 6th AML Directive[3]. This reduces the risk of non-compliance penalties, helping to ensuring firms meet their obligations efficiently.
- Software development: AI is used internally by firms to support developers by helping to answer technical questions about application programming interfaces (APIs) and system documentation.

Within the payment sector generally, AI's capabilities also extend to cybersecurity, where it can find anomalies in patterns of access and monitor discussion on development forms to detect bad actors.

As AI evolves in the next 10 years, with faster computers and more expertise, we expect firms to increase their use of it.

However, we see a growing risk that criminals will also be using AI. Such misuse includes forging identity documents, attempting to bypass real-time authentication mechanisms, such as face-to-face sessions, and highly tailored phishing attempts.

[1] Data based on publicly available information published by EMA members.
[2] https://eur-lex.europa.eu/eli/dir/2015/2366/oj/eng
[3] https://eur-lex.europa.eu/eli/dir/2024/1640/oj/eng

PSPs may increasingly rely on AI to conduct behavioural analytics and real-time risk assessments of transactions, accounts, and merchants. As AI adoption grows, regulatory oversight will need to evolve to ensure fairness, transparency, and explainability in AI-driven decision-making.

In the longer term, AI adoption will likely impact the financial services workforce in terms of skill requirements, job displacement, and reskilling needs. Firms will need to support employees to develop new skills, particularly those related to data analysis, AI, and the ability to work alongside advanced AI-based automation.

**Q2. Are financial services adopting AI at a faster rate than other sectors in the economy?**

The third survey on AI and Machine Learning ("ML") in financial services, BoE and FCA report: Artificial intelligence in UK financial services**,** indicates that 75% of respondents within the financial services sector are already using AI, with another 10% planning to do so in the next three years. This provides an indication of the current level of adoption within financial services.

The "AI Opportunities Action Plan recommendations" (January 2025) focus on ramping up AI adoption across the UK with a view to boosting economic growth, implying a general need for increased adoption across all sectors.

AI adoption offers significant opportunities for the payments industry, particularly in tackling fraud risks, meeting regulatory requirements, and addressing evolving customer expectations. The rapid integration of AI in financial services is evident in fraud prevention. AI-driven models can detect account takeovers, synthetic identities, and money laundering attempts in real time, enhancing security and reducing financial crime.

Regulatory uncertainty or cost implications could slow adoption within financial services. It is difficult to draft regulation that manages to keep up with fast-evolving technology and related risks. However, it is essential that regulators feel they have a well-defined remit and the power to issue firms with clear guidance on the use of AI. The UK approach, with responsibility allocated across the existing remits of several regulators, was an expedient way to establish a framework, but it is unclear that this is the best solution in the long term.

**Q3. To what extent can AI improve productivity in financial services?**

AI-powered identity verification tools and risk scoring can streamline onboarding processes, reducing delays and costs associated with manual checks.

In transaction processing, AI can reduce reliance on manual review for fraud detection and can continuously learn fraud patterns, thereby improving detection rates. AI-driven risk scoring also speeds up transaction processing and payment approval, reducing transaction delays for customers.

AI is also being used to streamline both front and back office functions. In customer service, for example, AI-powered chatbots can handle common or routine queries without the need for human intervention. This allows support staff to focus on more complex or sensitive issues, improving both efficiency and customer experience. In the back office, AI helps automate manual processes such as data entry, document management, and the preparation of regulatory reports, freeing up teams to concentrate on higher-value, strategic tasks.

The use of AI can increase efficiency through more responsive pricing and more accurate decision-making. AI's ability to analyse and process large volumes of data enables it to quickly identify patterns and insights that might be difficult or time-consuming for humans to discern. However, while AI brings productivity gains, it also presents challenges such as regulatory complexity, the need for continuous model training and human oversight, and the risk of algorithmic biases.

While AI may offer productivity improvements, firms will need to consider how customers perceive efficiencies compared to concerns about, for example, depersonalised interactions which may alienate vulnerable consumers who prefer human support.

**Q4. What are the risks to financial stability arising from AI, and how can they be mitigated?**

There is growing evidence of AI being misused to bypass KYC/CDD checks, enabling criminals to create synthetic identities, manipulate video verification processes, and bypass security measures using deepfake technology.

AI models often operate as 'black boxes', making it difficult for customers to challenge decisions and for regulators to scrutinise AI-driven processes. If left unchecked, AI could contribute to systemic risks. AI trained on biased data can make unfair decisions, such as denying services to certain groups of people. Criminals are leveraging generative AI to create high-quality forged documents, deepfake videos, and synthetic identities to open fraudulent accounts. The Joint Money Laundering Intelligence Taskforce (JMLIT) published an Amber Alert (0752-NECC) covering the use of AI to bypass customer due diligence (CDD) checks - according to which, AI-powered fraud attempts on KYC/CDD checks have risen significantly since 2022[4].

AI models can be proprietary and are often provided as a remotely hosted service. This presents a number of risks.

Before deploying AI tools, firms must carry out appropriate due diligence on their providers—particularly around the provenance and quality of training data. This can be difficult in practice, as AI developers are not always forthcoming about where their data has come from or how broad its scope is. This lack of transparency can be especially challenging for smaller firms, who often lack the bargaining power to secure greater clarity or adapt contractual terms.

Moreover, firms may use AI models in ways not originally intended or tested by the developer, increasing the risk of unpredictable or unsuitable outcomes. As firms remain responsible for the outputs or decisions AI systems make on their behalf, it's essential they carry out their own testing to confirm that any models perform as expected, and align with their operational and regulatory standards.

Firms must ensure that AI services are secure and will maintain the confidentiality of any personal data they process or transmit. This obligation applies not only to structured personal data but also to less

[4] This Amber Alert has been shared with the JMLIT+ membership and is not publicly available.

obvious Personally Identifiable Information (PII), such as passwords or names and addresses, revealed during customer service interactions.

The reliance on third-party providers for AI services can represent a concentration risk. Potential operational failures or cyberattacks targeting critical AI providers could represent a systemic risk, with outages impacting multiple firms in the sector. Contracts with AI providers should include clear service-level agreements. They should also establish communication protocols for incidents, enabling firms to fulfil their incident reporting obligations to regulators. Firms must identify their critical dependencies on AI services. They need to consider both their short-term business continuity plans and their long-term strategies for migrating to other providers in case of market failures.

Mitigation strategies could include the following:

- Regulators should require transparency and explainability in AI-driven decisions, so consumers can understand if they are impacted by an AI decision, and what recourse they have to seek to understand or challenge decisions.
- Firms should combine AI with human oversight.
- Financial institutions, law enforcement, and regulators should collaborate to share intelligence on emerging AI threats.
- AI systems should undergo regular audits to identify biases, vulnerabilities, and potential financial stability risks.
- Deep trading algorithms will need extensive training, testing in multi-agent sandbox environments, and constrained by tightly monitored risk and stop-loss limits. Managers will need to constantly monitor for unusual behaviour.
- International regulators, market participants, and AI safety experts should work together to ensure the safety of future algorithms.

**Q5. What are the benefits and risks to consumers arising from AI, particularly for vulnerable consumers?**

The use of AI in financial services presents both potential benefits and risks for consumers, with vulnerable individuals particularly susceptible to the downsides. In particular, AI systems are often hard to understand (the 'black box problem'), making it difficult for consumers to understand and challenge potentially incorrect outcomes.

We need to consider how to educate consumers, especially vulnerable groups, about AI risks like targeted phishing or deepfake scams.

Benefits:

- AI-powered fraud detection could help protect consumers from unauthorised transactions and financial scams.
- Customers may receive faster and more personalised services through AI chatbots and digital assistants to enhance customer support, reducing wait times and improving accessibility.
- By analysing large volumes of data, AI could identify customer characteristics and preferences, enabling firms to offer services tailored to individual needs.

Risks:

- Criminals can exploit AI-generated deepfakes and voice synthesis to impersonate trusted individuals, and deceive vulnerable customers into making fraudulent transactions. Educating consumers about AI-enabled fraud may help them recognise and avoid scams.
- AI models may store and exchange significant amounts of personal data, increasing risks of data breaches.
- Bias in the underlying data used to train AI models can result in biased or discriminatory decisions, financial exclusion, and reduced trust.
- AI's detailed knowledge of customers could be used to take advantage of their weaknesses.

**Q6. How can Government and financial regulators strike the right balance between seizing the opportunities of AI and protecting consumers while mitigating threats to financial stability?**

A collaborative approach between regulators, financial institutions, and law enforcement is essential to harness AI's potential while safeguarding financial stability and consumer protection. Efforts should focus on the following areas:

- Developing proportionate AI regulation tailored to financial services, including payment services and e-money, ensuring AI innovation is not stifled while maintaining strong consumer protections.
- Firms using AI for fraud detection should have documented decision-making processes, including outlining how the performance of the AI is monitored and how any shortcomings are corrected.
- Regulators should foster collaboration between fintechs, PSPs, and law enforcement agencies to develop best practices for AI governance.
- The rise of AI-powered fraud necessitates investment in law enforcement's ability to detect, investigate, and prosecute AI-enabled financial crime.
- Regulators could introduce regulatory sandboxes or incentives for PSPs developing AI-driven compliance tools that enhance fraud detection and risk mitigation.
- There is a need for international collaboration to establish harmonized standards for AI governance. This is important for mitigating cross-border risks associated with AI adoption.

AI presents both opportunities and risks for non-bank PSPs and the wider financial services industry. While AI enhances fraud detection, compliance automation, and customer experience, it also introduces new vulnerabilities, particularly in KYC/CDD processes.

## Members of the EMA, as of April 2025

Airbnb Inc
Aircash
Airwallex (UK) Limited
Amazon
Ambr
American Express
Banked
Benjamin Finance Ltd.
Bitstamp
Blackhawk Network EMEA Limited
Boku Inc
Booking Holdings Financial Services International Limited
BVNK
Cardaq Ltd
CashFlows
Circle
Coinbase
Contis
Crypto.com
Currenxie Technologies Limited
Curve UK LTD
Decta Limited
Deel
eBay Sarl
ECOMMPAY Limited
Em@ney Plc
emerchantpay Group Ltd
EPG Financial Services Limited
eToro Money
Etsy Ireland UC
Euronet Worldwide Inc
Facebook Payments International Ltd
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
Nuvei Financial Services Ltd
OFX
OKG Payment Services Ltd
OKTO
OpenPayd
Owl Payments Europe Limited
Own.Solutions
Papaya Global / Azimo
Park Card Services Limited
Payhawk Financial Services Limited
Paymentsense Limited
Paynt
Payoneer Europe Limited
PayPal
Paysafe Group
Paysend EU DAC
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 Payments SA
Weavr Limited
WEX Europe UK Limited
Wise
WorldFirst
Worldpay