

EN

E-001920/2025

Answer given by Executive Vice-President Virkkunen
on behalf of the European Commission
(24.7.2025)

The Commission recognises the serious threat of digital fraud and AI-enabled fraud¹, including investment scams using deepfakes. To tackle these threats, the European Union has put in place a robust regulatory framework.

The Digital Services Act² offers a range of tools to address digital fraud and misleading practices, such as financial scams and deepfakes. These include the obligations for providers of online platforms to put in place notice and action mechanisms and measures to tackle repeated offenders³, enhanced due diligence obligations for providers of very large online platforms (VLOPs) and very large online search engines⁴ (VLOSEs)⁵ as well as other duties⁶.

The AI Act⁷ addresses this phenomenon through two mechanisms: prohibited practices and transparency obligations. The AI Act prohibits AI systems that employ subliminal or deceptive techniques to distort human behaviour, particularly when this leads to significant harm⁸. This prohibition includes AI systems designed for investment scam using deepfakes. Moreover, the AI Act establishes transparency obligations for synthetically generated or edited content, including deepfakes, requiring that providers mark AI-generated outputs in a machine-readable way⁹.

¹ From the recent initiatives, see the ProtectEU Strategy, which announced the intention to ‘strengthen our ability to combat online fraud – which is causing very significant financial harm – the Commission will support prevention measures and more effective law enforcement action and will work with Member States and stakeholders to support and protect victims, including by assisting in recovering their funds. These efforts will be formalised in an Action Plan on Online Fraud. See: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on ProtectEU: a European Internal Security Strategy, COM/2025/148 final.

² Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act, DSA).

³ Article 16 and Article 23 DSA.

⁴ Online platforms and online search engines with a number of average monthly active recipients in the EU equal to or higher than 45 million and which are designated as VLOPs or VLOSEs under Art. 33(4) DSA.

⁵ Such as the obligation to compile and make publicly available advertising repositories (Article 39 DSA).

⁶ Providers of VLOPs and VLOSEs are also required to diligently identify, assess and analyse the systemic risks stemming from design, functioning and use made of their services and related systems (including algorithmic systems) (Art. 34 DSA) and to put in place reasonable, effective and proportionate mitigation measures, tailored to the identified risks (Art. 35 DSA). Such systemic risks include the dissemination of illegal content and any actual or foreseeable negative effects for fundamental rights to inter alia a high-level of consumer protection, and may therefore include the creation and spread of scams and deep fakes on VLOPs and VLOSEs. Mitigating such risks may include adapting their content moderation policies and reinforcing their internal process for the detection of systemic risks. The Commission has opened formal proceedings for suspected infringements relating to some of these issues. See <https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses#ecl-inpage-metaplatforms>.

⁷ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).

⁸ Article 5(1)(a) of the AI Act.

⁹ In particular, under Article 50, providers of AI systems, including general-purpose AI systems, generating synthetic content, are required to ensure that the outputs of the AI system are marked in a machine-readable format and detectable as artificially generated or manipulated.

On public awareness, several existing initiatives already contribute to raising awareness of online safety¹⁰ and cyber risks¹¹, including scams¹². In the area of financial services, the Commission is currently updating retail investor protection rules¹³, addressing new forms of payment fraud as part of its proposal to revise rules on payment services¹⁴, and aims to promote financial awareness and literacy in its upcoming communication on a Financial Literacy Strategy, which is due for adoption in the third quarter of 2025¹⁵.

¹⁰ See e.g. JRC website: https://joint-research-centre.ec.europa.eu/scientific-tools-and-databases-0/happy-onlife-play-learn-about-online-safety_en; European Youth Portal: https://youth.europa.eu/get-involved/your-rights-and-inclusion/be-safe-online_en. With regard to protection of minors, the Commission is currently working on Guidelines – see <https://digital-strategy.ec.europa.eu/en/news/commission-publishes-draft-guidelines-protection-minors-online-under-digital-services-act>.

¹¹ See e.g. ENISA website: <https://www.enisa.europa.eu/audience/citizens>; Cybersecurity Month initiative: <https://digital-strategy.ec.europa.eu/en/news/launch-european-cybersecurity-month-focus-addressing-social-engineering>.

¹² The Commission will publish an EU financial literacy strategy in the autumn to empower citizens and raise awareness, including on potential financial risks.

¹³ The legislative proposals are a Retail Investment Strategy, adopted in 2023 and under negotiation, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0279>.

¹⁴ The legislative proposals were adopted in 2023 and are under negotiation. https://finance.ec.europa.eu/publications/financial-data-access-and-payments-package_en.

¹⁵ Communication on a Savings and Investments Union (2024), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025DC0124>.