

CLIENT ALERT

SEPTEMBER 29, 2026

Digital operational resilience and artificial intelligence: the European Systemic Risk Board and the ECB sound the alarm on frontier AI models

Cybersecurity and AI – European and Italian Banking and Financial Supervision

Within a few weeks of one another, the European Systemic Risk Board (“**ESRB**”) and the European Central Bank (“**ECB**”) sounded a coordinated alarm on the systemic cybersecurity risks posed by frontier artificial intelligence models. Shortly afterwards, the Bank of Italy, in a [communication to the market](#), called on the entities subject to its supervision to promptly strengthen their security safeguards in light of the same risks. More recently still, the three European Supervisory Authorities (“**ESAs**”), in a [joint risk assessment](#) published on 23 September 2026, confirmed ICT and cyber resilience and AI-driven threats as a shared supervisory priority.

This coordinated supervisory alarm has taken on particular significance in light of two concrete cases involving Italian entities which illustrate its practical relevance: a sophisticated AI-driven fraud against a major Italian private-banking institution, in which the company’s president was deceived by a forged WhatsApp message impersonating the CEO of the parent company (a major Italian banking group under ECB supervision) and by a telephone call in which the voice of a prominent lawyer was replicated using artificial intelligence, resulting in the loss of approximately EUR 36 million; and the theft of confidential data belonging to 680 customers of a well-known European fintech bank, obtained through a successful impersonation of an Italian Ministry of Interior office.

This alert sets out the content of the [ESRB’s warning](#) and of the [ECB’s letter](#) to significant institutions, before turning to the Bank of Italy’s communication and to the ESAs’ joint risk assessment, places all four in context in light of those cases, and identifies the operational steps that supervised entities should take in the coming months.

Concrete illustrations of the risks

Case 1 – The AI voice-cloning fraud against a private-banking institution

In February 2026, a major Italian private-banking institution fell victim to an international fraud scheme targeting its president. The attack was triggered by a forged WhatsApp message that appeared to come from the CEO of the parent banking group,

instructing the president to arrange a series of urgent wire transfers through the institution's treasury for a purported overseas acquisition opportunity¹.

To reinforce the deception, the fraudsters followed up with a telephone call in which a prominent lawyer – a managing partner of another leading international law firm in Italy – appeared to confirm the transaction. The lawyer, entirely unaware and uninvolved, had his voice replicated using artificial intelligence tools with such precision that the president, who knew him personally, believed the call to be authentic. Further emails, meticulously crafted to appear genuine communications from the law firm, provided the bank-account details for the transfers.

Acting on these instructions, the institution's chief financial officer executed transfers totalling approximately EUR 95 million, directed primarily to accounts in China and Hong Kong. The institution's internal security systems subsequently triggered an alert, and it was able to recover a significant portion of the funds. An investigation led by the competent Public Prosecutor's Office has secured additional recoveries, but at least EUR 36 million remain unaccounted for, having been rapidly routed through a chain of overseas accounts and converted into cryptocurrency.

Case 2 – The fintech data theft

In September 2026, a well-known European fintech company confirmed that it had fallen victim to an impersonation fraud, in which a group of hackers compromised, or at least spoofed, the address of a certified email account attributable to the Italian Ministry of Interior, using it to request and obtain confidential data relating to 680 customers².

The victims are believed to have been selected because they were suspected of holding crypto assets. One of the hackers reportedly subsequently demanded a \$3 million ransom not to disclose the stolen data, and one of the affected customers reportedly already received an individual ransom demand of \$50,000 for the deletion of his personal data.

The hacker collective also claimed to have stolen 147 gigabytes of confidential material belonging to Italian law enforcement agencies, including internal documents and communications between officers³.

¹ See Luigi Ferrarella. “Truffa Fideuram, il falso messaggio WhatsApp inviato all'ex presidente Molesini e la telefonata contraffatta con l'AI: spariti 36 milioni di euro”. Corriere della Sera, September 25, 2026.

² See, *inter alia*, Kalyeena Makortoff. “Revolut reportedly facing \$3m ransom demand after hackers steal hundreds of customers' data”. The Guardian, September 17, 2026.

³ See Roberto Cosentino e Paolo Ottolina. “Caso Revolut, l'hacker chiede riscatto di 3 milioni per i file rubati. «Ho 147 Giga di dati delle forze dell'ordine italiane»”. Corriere della Sera, September 16, 2026.

The ESRB warning: a systemic risk assessment

On June 25, 2026, the ESRB adopted a formal warning on the systemic cyber risks stemming from frontier artificial intelligence models (“**FAIMs**”), addressed to all ESRB members and, more broadly, to the authorities responsible for macro- and micro-prudential oversight of the EU financial system.

The ESRB notes that FAIMs are now capable of discovering vulnerabilities, generating working exploits and autonomously executing full-scale cyber-attacks at a speed, scale and level of accuracy far exceeding previous AI models – a development it describes as a paradigm shift and an inflection point in AI capability.

In the ESRB’s assessment, this weakens operational resilience across the financial sector along four dimensions:

1. the time available to patch complex systems without causing operational failure;
2. the capability of defenders to test, protect, detect and respond using FAIM-assisted tools;
3. the degree of concentration risk arising from dependency on a small number of AI and cloud providers; and
4. the capability of authorities to calibrate supervisory expectations, stress testing and preparedness measures to the pace of FAIM development.

The ESRB further identifies three sources of asymmetry that FAIMs amplify:

- between jurisdictions, given the geographic concentration of leading AI providers outside the EU;
- between attackers and defenders, since FAIMs lower the cost of mounting sophisticated attacks faster than defenders, who remain constrained by regulatory and operational requirements, can adapt; and
- between financial institutions themselves, depending on their resources and access to specialist expertise – with the weakest link in the chain capable of affecting the stability of the system as a whole.

The ESRB specifically calls on financial authorities, within their respective competences, to take these three sources of asymmetry into account, to consider cooperation arrangements and sectoral coordination alongside existing testing frameworks in order to reduce them, and to ensure that the boards of supervised financial institutions are fully committed to mitigating FAIM-driven cyber risks, with clear governance and accountability frameworks in place and timely responses adequately planned and resourced.

The ECB's call to action for significant institutions

On July 7, 2026, the Chair of the Supervisory Board of the ECB addressed a letter to the CEOs of significant institutions directly supervised by the ECB under the Single Supervisory Mechanism (“**Significant Institutions**”), calling on them to assess without delay the impact of the evolving AI-driven threat landscape and to develop a comprehensive action plan. The ECB stresses that this is a long-term shift in the threat landscape rather than a temporary phenomenon tied to any single tool, and that, while it does not introduce entirely new risks, it significantly amplifies the speed and scale at which such risks materialise. Responsibility for the response is placed squarely on banks’ management bodies, which are expected to revisit ICT investments, resource allocation and risk-tolerance frameworks, and to strengthen governance and control systems where necessary.

The ECB’s letter asks Significant Institutions to focus, in the short term, on three priority areas:

1. accelerating vulnerability and patch management at scale;
2. enhancing monitoring, detection and AI-enabled defensive capabilities; and
3. verifying that third-party risk management is fit for purpose, given the role of ICT service providers in critical supply chains, with priority given to internet-facing and externally exposed ICT assets, including third-party software and open-source components.

In addition, the ECB calls for structural measures over the medium term, namely reinforcing defence-in-depth and cyber hygiene, modernising legacy and unsupported infrastructure, and strengthening operational resilience through response, recovery and crisis-management arrangements and information-sharing arrangements.

Significant Institutions are required to prepare and submit their action plan to their Joint Supervisory Team (“JST”) by October 31, 2026. The JST will engage with the institution to discuss the plan and monitor its implementation, and the ECB will separately conduct a horizontal analysis across all submitted action plans to identify common trends and areas for improvement. As a countervailing measure, the ECB has extended the deadline for the annual IT Risk Questionnaire from September 2026 to February 2027, and will consider adjustments to other supervisory activities, such as on-site inspections or deep dives, on a case-by-case basis.

The Bank of Italy’s communication: strengthened safeguards against AI-driven threats

It is against this backdrop of increasingly sophisticated threats – already flagged at European level by the ESRB and the ECB, as described above – that on July 17, 2026 the Bank of Italy, within the framework of the requirements of the Digital Operational

Resilience Act (“**DORA Regulation**”)⁴, issued a communication calling on entities directly supervised by it (“**Supervised Entities**”) to promptly identify and implement the measures needed to strengthen their operational and cyber resilience.

Within the risk framework evidenced in the ESRB warning and complying with the ESRB’s invitation, the communication requires Supervised Entities to strengthen their safeguards across six operational areas:

1. Governance

Management and administrative bodies must review their risk appetite framework (“**RAF**”) to incorporate risks arising from frontier technologies, ensure a clear allocation of responsibilities for data security, set appropriate contractual requirements and selection criteria for external ICT service providers, and ensure that the administrative body includes members with adequate technological expertise, including in AI.

2. Cyber hygiene

Entities must integrate defence-in-depth principles and cyber hygiene practices into their corporate strategy – rigorous authentication and authorisation, granular access management, and continuous monitoring – together with network and operating environment segmentation strategies to limit the spread of any compromise.

3. ICT asset and attack-surface management

Entities need complete, up-to-date and reliable inventories of ICT assets, a criticality-based classification that takes into account direct internet exposure and reliance on cloud infrastructure, and the modernisation of legacy technologies that are no longer supported.

4. Vulnerability and patch management

Entities must rapidly identify vulnerabilities in their ICT systems – including, where appropriate, through AI-based scanning techniques – and prioritise remediation, starting with open-source software and systems directly accessible from outside the organisation.

5. Monitoring and defence

Monitoring and defence systems for applications, access and network traffic – including traffic to and from third-party ICT providers – must be strengthened, including through integration with AI-based tools to identify anomalies in real time, particularly with respect to critical ICT assets.

⁴ Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L 333, 27.12.2022).

6. Digital operational resilience testing

Digital operational resilience testing must be intensified, including structured crisis-management simulations based on realistic and progressively more complex scenarios, in line with Articles 24 and 25 of the DORA Regulation. Testing assumes an even more crucial role in assessing an entity's preparedness in a context where the likelihood of an ICT incident has increased.

The Bank of Italy requires a structured report – covering current risk exposure, adequacy of safeguards, gaps and priorities – **together with a work plan, to be first considered by the Board of Directors and by the Board of Statutory Auditors, and then transmitted to the Bank of Italy by December 31, 2026.**

Furthermore, the Bank of Italy expressly requires Supervised Entities to identify and notify a specific point of corporate accountability (for example, the second-level ICT risk control function), a formal designation requirement that does not appear in the ECB's letter.

It should be noted that following the above incidents, the Bank of Italy has been actively engaging with Supervised Entities, requesting information and carrying out targeted checks on the adequacy of existing safeguards against these specific types of threat. Other European supervisory authorities, including the Banque de France, the Swiss Financial Market Supervisory Authority (FINMA) and the Bank of England, are reported to be conducting similar inquiries, with a particular focus on the robustness of customer-verification protocols, the effectiveness of segregation-of-duties controls for high-value transactions, and on whether internal compliance controls were capable of detecting the sustained, anomalous flows of sensitive data and funds that characterised these attacks – inquiries that sit squarely within the systemic concerns already flagged by the ESRB⁵.

The ESAs' joint risk assessment: ICT dependencies, cyber risk and policy recommendations

On September 23, 2026, the three ESAs – the European Banking Authority, the European Insurance and Occupational Pensions Authority and the European Securities and Markets Authority – published a joint risk assessment which places the same set of concerns at the centre of the EU financial supervisory agenda, confirming the direction already taken by the ESRB, the ECB and the Bank of Italy.

On ICT and cybersecurity risk, the ESAs note that a high reliance on third-party ICT service providers (for example cloud service providers and software vendors) and on payment service providers amplifies operational risk, and that such providers are frequently domiciled outside the EU. According to the ESAs' risk assessment

⁵ See Fabrizio Gorla. "Caso Revolut, i controlli di Bankitalia dopo l'attacco". La Stampa, September 20, 2026.

questionnaire, banks regard ICT service-provider dependency as their single biggest challenge in this area (around 80% of respondents), with payment-solution dependencies ranked as the second most material risk (around 60%).

The ESAs further stress, drawing on 2026 DORA incident-reporting data, that system failures account for the majority of ICT incidents across EU financial sectors, with cyber risk and data security remaining the most significant drivers of operational risk, followed by fraud, and that the number of cyberattacks on financial institutions remains high. Looking ahead, the ESAs warn that rapid advances in artificial intelligence could substantially amplify vulnerabilities to cyberattacks, as frontier AI tools may be able to identify and exploit IT weaknesses at unprecedented speed, making it harder for market participants to respond in time.

On this basis, the ESAs set out in their Autumn 2026 Report the following two IT policy recommendations:

- continued monitoring of non-EU/EEA dependencies on technology service providers; and
- continued planning and preparation for the risks arising from the rapid development of AI and quantum computing.

The ESAs consider that the EU's regulatory framework – including the DORA Regulation and the AI Act – provides a solid foundation for managing cyber and AI-related risks, and call on financial entities to maintain strong operational resilience, cybersecurity controls and contingency planning, and to strengthen software quality and cybersecurity practices, including through the adoption of new practices such as AI-powered security testing.

Taken together with the ESRB warning, the ECB's letter and the Bank of Italy's communication described above, the ESAs' joint risk assessment confirms that ICT and cyber resilience, third-party and concentration risk, and AI-driven threats are now a shared and converging priority across European supervisory authorities, reinforcing the case for the prompt and coordinated action.

What you should do now

- Significant Institutions supervised directly by the ECB should treat the July 7, 2026 letter as requiring immediate board-level attention, given the October 31, 2026 deadline for submitting their action plan to the JST. Supervised Entities should, without delay, bring the communication to the attention of the Board of Directors and the Board of Statutory Auditors, and begin work on the required report, which must be submitted by December 31, 2026. In both cases, **the report or action plan requires a structured assessment across governance, cybersecurity, vendor management and crisis-response readiness**, and its conclusions will

define the entity's commitments, accountability framework and investment plan vis-à-vis the supervisory authority – making the quality and defensibility of its content a matter of direct legal significance.

- Existing verification and authentication procedures should be stress-tested against realistic threat scenarios, including social-engineering and impersonation attacks exploiting institutional communication channels, AI-generated voice cloning of corporate executives, and coordinated multi-channel deception schemes. In practice, this involves **mapping the full chain of authentication and authorisation steps in place for processing external requests, identifying gaps in the procedures for verifying the identity of counterparties and the legitimacy of incoming communications, assessing whether authorisation procedures for extraordinary or high-value transactions include adequate segregation of duties and independent verification steps, and assessing whether verification protocols are integrated across the compliance, IT-security and legal functions or operate in silos** – a gap that the Bank of Italy's governance requirements are intended to close.
- Where AI-based defence tools are in use or under consideration, **entities should carry out a structured gap analysis between the tool's operational design and the entity's broader AI strategy**, covering model-risk assessment, explainability requirements, and the adequacy of human-oversight mechanisms. More broadly, the two fraud cases illustrate that the compliance challenge facing financial entities is inherently multidisciplinary: the intersection of the DORA Regulation, the AI Act, data-protection legislation and corporate-governance requirements creates a layered regulatory framework in which operational, technological and legal dimensions are inseparable – and must be addressed as a coherent whole, with coordinated legal, regulatory and technical expertise, rather than in isolation.
- **Entities not directly subject to Bank of Italy supervision should not underestimate the practical relevance of the communication:** contractual obligations towards supervised counterparties, reputational exposure and the upcoming enforcement of the AI Act mean that the governance, vendor-management and training standards outlined by the Bank of Italy are rapidly becoming a market-wide benchmark. Entities that defer engagement risk both operational vulnerability and loss of competitiveness in a landscape where counterparties increasingly require demonstrated resilience capabilities as a condition of doing business⁶ – and where,

⁶ This is a relevant cross-sectoral issue that extends beyond the financial sector. In fact, entities operating in critical and highly critical sectors, as well as their suppliers across the supply chain, are subject to cybersecurity frameworks, including NIS II, and to guidelines issued by the international and national competent authorities.

as the two cases discussed in this alert show, the financial and reputational consequences of a successful attack can be severe and immediate.

- **The heightened focus on cybersecurity risk assessment is also relevant from a data protection perspective.** Article 32 GDPR requires controllers and processors to implement technical and organisational measures that ensure a level of security appropriate to the risk, based on an objective assessment of the likelihood and severity of the risk to data subjects' rights and freedoms. This requirement was recently addressed by the Irish Data Protection Commission in a decision against a retail bank, which found that the bank had infringed Articles 5(1)(f) and 32(1) GDPR by failing to implement technical safeguards against foreseeable human error and predictable fraud attacks on its contact centre, despite having identified the relevant risks in its own risk register, and imposed a fine of EUR 250,000.00 in this respect. **Entities should ensure that their risk assessments concretely translate into proportionate technical controls, rather than remaining at policy level⁷.**

About Curtis

Curtis, Mallet-Prevost, Colt & Mosle LLP is a leading international law firm. Headquartered in New York, Curtis has 19 offices in the United States, Latin America, Europe, the Middle East and Asia. Curtis represents a wide range of clients, including multinational corporations and financial institutions, governments and state-owned companies, money managers, sovereign wealth funds, family-owned businesses, individuals and entrepreneurs.

For more information about Curtis, please visit www.curtis.com.

Attorney advertising. The material contained in this Client Alert is only a general review of the subjects covered and does not constitute legal advice. No legal or business decision should be based on its contents.

Please feel free to contact any of the persons listed below if you have any questions on this important development:

⁷ See Data Protection Commission (Ireland), Decision in the matter of Permanent TSB plc trading as PTSB and PTSB Asset Finance, Case Reference IN-22-7-3, April 30, 2026.

**Giovanni Sagramoso**

Partner

gsagramoso@curtis.com

Milan: +39 02 7623 2028

**Gaia Morelli**

Partner

gmorelli@curtis.com

Rome: +39 06 6758 2269

**Maria Elena Sarvia**

Associate

msarvia@curtis.com

Milan: +39 02 7623 2054