Ms Maria Julve
Head of Non-Financial Risk,
European Central Bank,
60640 Frankfurt am Main
Germany

26 May 2026

Frontier AI

Dear Ms Julve,

Cc Mr Francisco Garcia, Head of Section

I am writing following the virtual roundtable with AFME on the 12th May, where we appreciated your and colleagues' openness and the offer of continued dialogue on the important topic of Frontier AI.

Firstly, we strongly welcome your offer to consider short term regulatory relief to industry, in order to facilitate resource prioritisation towards urgent remediation work. It is an encouraging recognition of the seriousness of the challenge facing the sector and the importance of prioritising risk management over business-as-usual compliance activity.

In particular, we would encourage the ECB to:

- **Delay any relevant upcoming on-site inspections (OSIs);**
- **Delay any upcoming DORA TLPT (threat led penetration test) exercises;**
- **Cancel the June 2026 ITRQ (IT Risk Questionnaire).**

Such high-intensity supervisory interventions compete directly for specialist time and attention. Making these changes to supervisory plans would immediately release specialist cyber and technology team capacity to focus on Frontier AI remediation, with limited impact to regulatory objectives.

In addition, we would request your assistance in educating ECB joint supervisory teams (JSTs) as to the need for appropriate discretion to waive certain expectations which may no longer be fit for purpose. The new cyber risk environment may necessitate changes to the way firms manage risk requiring commensurate flexibility from supervisors, in particular:

- Firms may need to adjust risk parameters (including service downtime) in order to make appropriate technology changes (patching) to protect the firm.
- Supervisors should allow for this to enable firms to take the steps they believe are right to protect themselves and clients.

This change of approach should though be communicated to firms through direct supervisory channels rather than public communications as the latter could inadvertently undermine confidence in the financial system.

Related to this, given vulnerability disclosures contain firms' most sensitive data, supervisory requests for information should be limited and focused on aggregate information to avoid exposing individual firms and the wider sector to additional risk. Equally, some supervisors regularly request firms to confirm awareness of particular vulnerabilities. In the future, higher severity vulnerabilities may be a more regular occurrence and therefore the cost to firms and authorities of making and answering such

requests will be higher. New ways of achieving comfort regarding firms' awareness need to be considered.

Finally, we encourage your team to apply pressure on the owners of critical infrastructure to accelerate cybersecurity preparedness in line with expectations for the sector. This infrastructure underpins the financial sector operationally, and in the case of regulators, is the store of significant amounts of highly sensitive supervisory information. Breaches in such systems could disrupt market functioning, undermine trust and create cybersecurity risk for firms. We would encourage:

- Providing industry with greater assurance that the ECB's own platforms and infrastructure are safeguarded with the latest cybersecurity preparedness.

- Employing ECB supervisory reach to material third parties, especially FMIs and CTPPs to drive systemic uplift and a coordinated sector response to the cybersecurity risks posed by Frontier AI.

- Promoting cross-sector engagement to address key dependencies within industry, in part by amplifying, with government partners, the importance of remediation within other critical infrastructure sectors such as energy, telecommunications, water and transport. Regulators could leverage existing connections with other sectoral regulators to raise awareness, share best practices and encourage action.

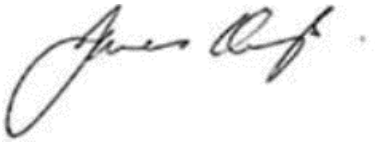
For your awareness, I wanted to share that AFME is also reaching out to relevant policymakers to discuss the requirements in the Digital Operational Resilience Act (DORA) and the Cyber Resilience Act relating to vulnerability reporting, including to the public. In light of the altered cybersecurity risk for the sector, these may need adjusted, to ensure public confidence in the EU financial system is not degraded.

- At a minimum, firms must be allowed to patch the vulnerability before any disclosing any information about the vulnerability, even to a regulator or CSIRT.

- Obligations under the CRA to notify all customers and clients alongside regulatory notification should be reversed. The security consequences for disclosure are no longer neutral and these requirements do not reflect the current threat environment. The CRA also envisaged disclosure to be a rare occurrence. In the future, more firms may see active exploitation of vulnerabilities. Exploitation does not necessarily mean the firm has experienced any operational disruption or data theft. Providing frequent notices to the public could erode confidence in the financial system.

In making the above requests to policymakers, we are highlighting that these frameworks were designed for a different threat baseline. Applying them without modification in the current environment risks converting transparency obligations into attack surfaces.

With thanks again for meeting with AFME and members earlier this month, we look forward to hearing from you on the above priorities and would be happy to discuss further. Any questions, please do not hesitate to let us know.



James Kemp
Managing Director
GFMA - Global FX Division,
AFME - Technology & Operations and CCA Divisions