Association for Financial Markets in Europe

Position Paper

EU Cyber Resilience Act: Level 2

March 2025

Executive Summary

The Association for Financial Markets in Europe (AFME) supports the EU institutions' focus on robust cybersecurity across the EU market, and supports DG-CNECTs intention to improve cybersecurity across the EU market and wishes to ensure the effective integration of the CRA with existing financial regulation. Following publication of the Cyber Resilience Act within the EU Official Journal in October 2024, we look forward to continuing our engagement with policymakers as this Regulation proceeds towards implementation. At this stage we are highly conscious that several of the incoming Level 2 instruments will be instrumental in whether and how the incoming obligations can effectively and efficiently bolster the EU's approach to cyber risk.

In summary we are flagging as our top priorities that:

1. ***The application of the Cyber Resilience Act should take account of existing risk management obligations. Manufacturers should be advised to exclude by default all 'products' where these fall within scope of sectoral legislation. This reflects the rationale of the European Supervisory Authorities in their recent decision not to construe regulated services as ICT services for the purposes of DORA: it prevents operational duplication where there would no benefit in terms of risk management.***

2. ***We call for a proportionate and risk-based approach to determining whether a product modification would render a distributor the manufacturer for the purposes of this Regulation. The practice of 'white-labelling' is a critical avenue by which market participants can embed digitalisation in their offering.***

3. ***The financial sector is subject to a harmonized incident reporting regime as one of the primary intentions of DORA. The CRA should not introduce a further regime and allow for all incident reporting to be facilitated via the existing DORA regime. We support the proposal for vulnerability notifications to be delayed where onward disclosure could exacerbate cyber related risks. It is critical that policymakers do not inadvertently assist malicious actors through the sharing of information which could be misused.***

4. ***We support the speedy resolution of certain guidance, Implementing Acts and Delegated Acts that are critical to the effective compliance of the CRA by the deadline. This includes Article 14 reporting obligations, Article 26 scope guidance and Article 27 common specifications to comply with the Essential Cybersecurity Requirements. Any delays to further guidance will disrupt compliance programs and apply significant pressure to in-scope organizations.***

5. ***The Members would welcome further clarification from DG-CNECT concerning the enforcement of the CRA for the financial sector. The financial sector is a regulated sector with pre-existing enforcement and supervisory practices. The enforcement powers of alternative Member State surveillance authorities directly interact with the powers of financial regulators.***

6. ***We welcome the proposal to leverage the European cybersecurity certifications schemes via the presumption of conformity. Yet these schemes are at risk of being captured by wider political discussions, including on geopolitical risk. ENISA should be empowered to remove any requirement for a cybersecurity certificate where there is a risk to market resilience.***

7. ***The inclusion of the CE Marking and product-specific support requirements within the CRA do not relate to financial products but the applications and software that deliver those products. The haphazard application of consumer legislation, which has never been applied to financial services, serves only to confuse consumers and does not appropriately reflect the intangible nature of products provided by the financial sector.***

AFME remains on hand to discuss in detail this position paper, or any of advocacy on this important file. Please do not hesitate to contact the team via marcus.corry@afme.eu

1. ***The application of the Cyber Resilience Act should take account of existing risk management obligations. Manufacturers should be advised to exclude by default all 'products' where these fall within scope of sectoral legislation. This reflects the rationale of the European Supervisory Authorities in their recent decision not to construe regulated services as ICT services for the purposes of DORA: it prevents operational duplication where there would no benefit in terms of risk management.***

- We once again welcome the decision of the EU to commission guidance for manufacturers on the scope of the Regulation under Article 26, in particular with regards to existing Union harmonisation legislation. The growing prevalence of cyber threats has led to a plethora of initiatives in this space across the EU institutions, by policymakers, supervisors and cyber agencies. Without concerted effort, it is likely that the various approaches may inadvertently conflict or fail to synchronise. AFME also stresses that given the level of demand on cybersecurity resources, any operational uplift should be justified through a tangible benefit in terms of risk management and wider cyber resilience.

- We agree that there is likely to be greatest overlap in scope with regards to remote data processing solutions and open-source software but also all controls and risk management applications across a firm's IT infrastructure. All of this will be captured within the financial services sector under the requirements of DORA. This overlap would significantly undermine a complimentary product-entity versus entity-level approach by DGs CNECT and FISMA respectively. Please see our previous position paper for further examples of how this overlap is likely to emerge.

- We strongly urge the Commission to clarify that where a product, under the Cyber Resilience Act, is found to be within scope of existing risk management legislation, whether as a product or by virtue of a different terminology, manufacturers should prioritise the existing obligations in line with the Commission's wider goals on ensuring a harmonised regulatory framework. AFME recommends this is achieved by advising manufacturers to exclude (in with Article 2(5) of the Cyber Resilience Act) all products which are within scope of the sectoral legislation, unless the Commission has explicitly determined the sectoral rules do *not* offer the same or a higher level of protection. This should reflect and build upon the clarification provided in the 2023 FAQ on the CRA, which acknowledged that software as part of a service should not be covered by the CRA.

- We also urge, building on the alignment of the Cyber Resilience Act with the AI Act, that the Commission to actively pursue opportunities for future harmonisation. As part of the ongoing implementation of the EU's DORA, the ECB has published a feasibility study on an incident reporting hub. Should this hub proceed, the Commission should review how information held by the hub could be shared with non-financial authorities, to avoid manufacturers having to issue duplicate reports.

2. ***We call for a proportionate and risk-based approach to determining whether a product modification would render a distributor the manufacturer for the purposes of this Regulation. The practice of 'white-labelling' is a critical avenue by which market participants can embed digitalisation in their offering.***

- The practice of white-labelling is a long established way in which market participants, who are themselves not technology providers, can leverage and incorporate the benefits of digitalisation within their own product and service offerings. Typically this will see participants make significant, yet overall cosmetic modifications to a product, which will not negate the safeguards of the original manufacturer.

- In developing the *concept of substantial modification* as part of the incoming Guidance under Article 26, we would urge the Commission to take a proportionate and risk-based approach, which does not capture changes which are undertaken with the primary purpose of assimilating a product into the business' operations. This would ensure that the listed obligations associated with manufacturers are fully leveraged and utilised, as reflects the fact they will continue to be accurate and applicable:
    - Conduct and document a cybersecurity risk assessment for products
    - Handle vulnerabilities effectively and maintaining a coordinated vulnerability disclosure policy
    - Affix the CE marking and draw up an EU declaration of conformity for compliant products (an obligation which does sync with the nature of financial services products: see point 7 for further detail)
    - Provide technical documentation and keep it available
    - Include information and instructions for users.

- Instead we would propose that the following should act as factors for consideration:
    - That the modification of the product constitutes a material change in the risk of the product that was not considered or foreseen in the initial risk assessment of the product by the distributor or manufacturer.
    - The purpose, original performance or type of the product has changed outside of the description of the product assessed in the risk assessment by the distributor or manufacturer.
    - The modifications have not been made by the consumers themselves or on their behalf for their own use.

- All factors included above are reflected within previous EU product-related rules that introduce the concept of substantial modification for manufacturers. The financial sector is concerned that the Cyber Resilience Act is applying regulatory concepts that do not apply to the financial sector and are appropriate for consumer or digital policies-only (financial services are out-of-scope of the Product Liability Directive and the Regulation on General Product Safety). The financial sector is subject to product-specific regulation that is appropriate for specific financial products or intangible services. Consumer protection and the unique aspects of financial services are regulated via separate, product-specific regulation proposed by financial regulatory authorities. The Cyber Resilience Act is applying consumer and digital legislation to the financial sector for the first time which is causing significant interpretation difficulties and uncertainty.

- The Cyber Resilience Act adds a further concept to substantial modification that is not considered in previous EU legislation. The criteria that 'substantial modification' occurs when the distributor "affects the compliance of the product with digital elements with the essential cybersecurity requirements set out in Part I of Annex I" represents a materially lower threshold than former Regulations where the products purpose, type and performance is modified. The ECRs constitute many aspects of the product with digital elements that could be altered without the risk assessment of the manufacturer being amended. The financial sector encourages the guidance to align with former regulation and predicate substantial modification on a material change being exhibited to the form of product or the risk assessment provided by the manufacturer.

3. ***The financial sector is subject to a harmonized incident reporting regime as one of the primary intentions of DORA. The CRA should not introduce a further regime and allow for all incident reporting to be facilitated via the existing DORA regime. We support the proposal for vulnerability notifications to be delayed where onward disclosure could exacerbate cyber related risks. It is critical that policymakers do not inadvertently assist malicious actors through the sharing of information which could be misused.***

- A stated intention of DORA was to introduce a harmonized incident reporting regime for financial services. The European Commission stated that this intention was to ensure that reporting was "streamlined, so overlapping and duplicative requirements would be deleted and compliance costs and burdens be alleviated.[1]" The CRA has immediately introduced a new regime for the sector before the compliance deadline of DORA has been reached. DG-CNECT should allow for all financial sector reporting to be undertaken via DORA reporting channels. DORA allows for relevant incidents to be shared be competent authorities, including CSIRTSs, and therefore remains in compliance with the intention of the CRA. This aligns with all private-sector advocacy in relation to NIS2 reporting.

- The incoming obligations on vulnerability notifications reflects the growing level of incident reporting which is in effect in many sectors and industries, for example under DORA in the case of financial services. In principle, these information exchanges can assist authorities as they triage incidents, evaluate the potential knock-on impact and consider where to support contingency measures, provided the level and volume of information sought does not exceed the capabilities of the authorities. It is however inevitable that these notifications can and will be targeted by malicious actors. AFME has been stressing the importance of authorities' own cybersecurity controls, to ensure their databases do not in future become a golden source of information for malicious actors, for example as with the proposed EU DORA Incident Reporting Hub, which could in future store information on significant cyber threats.

- A risk to the reporting of actively exploited vulnerabilities before sufficient patches or remediation has occurred is that malicious actors could intercept information and exacerbate the disruption faced by the financial entity. Members request that any information provided within this reporting, or when being required to be publicly disseminated, remain high-level and organisations have the flexibility to not report when there remains a threat to that individual organisation.

- We welcome the decision at Level 1 to permit manufacturers to request a delay to the onward sharing of the notification by virtue of Article 16(2). We would recommend that in drafting the upcoming delegated act, policymakers use as their overriding gauge whether there is any tangible or actionable outcome which is being sought from the receiving authorities. It is crucial that the

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020SC0198

exchange of vulnerability notifications (and corresponding incident reports) do not become a source of generic data analysis, which will add little value to vulnerability management, and instead present malicious actors with a further interface target.

4. ***We support the speedy resolution of certain guidance, Implementing Acts and Delegated Acts that are critical to the effective compliance of the CRA by the deadline. This includes Article 14 reporting obligations, Article 26 scope guidance and Article 27 common specifications to comply with the essential cybersecurity requirements. Any delays to further guidance will disrupt compliance programs and apply significant pressure to in-scope organizations.***

    - All Article 14-related Acts refer to the incident reporting requirements that will be implemented within the shorter 21-month timeline. These are therefore more critical than those Acts with the longer timeline. AFME encourages that standardization of formats and data fields be expedited to ensure that in-scope organizations are able to begin compliance programs effectively and allow sufficient time for incident management teams to reflect the additional rules. Data fields are intrinsic to the information gathering, report processing and automation compliance response to incident reporting regulations and compliance cannot begin before these are finalized, therefore resulting in a materially shorter timeline than proposed within the legislation.

    - Article 26 includes guidance relating to how the CRA will complement existing sectoral regulation and interpretation regarding 'remote data processing services'. All guidance is critical to the depth and breadth of compliance programs that the financial sector will need to adopt to comply with the CRA. The *de facto* timeline of the CRA is predicated on the finalization of the guidance included in Article 26. Members support the speedy resolution of this guidance to ensure compliance programs can begin effectively.

    - Article 27 requires European standardisation organisations to draft harmonised standards for the essential cybersecurity requirements included in Annex I. Annex I represents the wholesale requirements for any product with digital elements that are not considered important or critical and therefore constitute crucial elements for compliance.

5. ***Members would welcome further clarification from DG-CNECT concerning the enforcement of the CRA for the financial sector. The financial sector is a regulated sector with pre-existing enforcement and supervisory practices. The enforcement powers of alternative Member State surveillance authorities directly interact with the powers of financial regulators.***

    - The CRA provides Member State market surveillance authorities with powers to ensure organizations comply. The financial sector is regulated by designated financial regulators, at a Member State or EU level, and are subject to supervision to ensure continued compliance. Members are unclear how the CRA market surveillance authorities will interact with their regulatory authorities and how enforcement will take place.

    - The CRA, for instance, allows for a market surveillance authority to withdraw a product with digital elements from the market should the product not be in compliance with the CRA. This could hypothetically remove a systemic financial product from a specific jurisdiction without the interaction of the competent financial regulator or the European Central Bank. For certain members of AFME who are globally systemic, a removal of a product could constitute a financial stability risk for European and global financial markets.

- Further clarity is therefore required regarding the interaction of the CRA with existing enforcement of financial regulation in the EU, including its implications for third country sourced products. The CRA adds further complexity to the regulatory landscape within the EU and fragments existing enforcement of cybersecurity and resilience regulation for the financial sector.

- Similarly, we urge the authorities to be mindful of the potential unintended consequences to market resilience and stability which could result from an order to restrict or withdraw any product as part of a corrective measure. Article 56 makes provision for a reasonable period for withdrawal, commensurate with the nature of the risk, but we would stress that with many products which are critical for a bank's digital offering, an orderly and secure substitution would require at least 12-18 months in a worst case scenario, for example the withdrawal of all products from a major Cloud Service Provider (CSP).

6. ***We welcome the proposal to leverage the European cybersecurity certifications schemes via the presumption of conformity. Yet these schemes are at risk of being captured by wider political discussions, including on geopolitical risk. ENISA should be empowered to remove any requirement for a cybersecurity certificate where there is a risk to market resilience.***

    - The development of the European cybersecurity certification schemes, under the Cybersecurity Act 2019, has been a welcome opportunity to advance coherent and transparent controls across the EU market. Cyber threats are one of the major risks facing financial services and one which is likely to grow, with the EU schemes helping to drive standards on safeguards, in part by ensuring that users of products have greater assurance as to the steps being taken to protect clients and their data.

    - The proposal to embed these schemes within the application of the Cyber Resilience Act is further welcomed by AFME. It contributes to a joined up, coherent policy landscape, which can facilitate greater harmonisation of the obligations being pursued by various EU institutions. We support the presumption of conformity under Article 27 where a relevant certificate has been obtained by the manufacturer.

    - There is however an ongoing risk that in future the cybersecurity certificates may be hijacked by political developments, and potentially even used as a tool for geopolitical negotiations. In light of the narrow, opaque nature of the implementing acts by which the schemes were enacted, the repercussions of such a scenario were not fully explored, giving rise to the risk of unintended consequences. It is critical that ENISA, as the agency overseeing the schemes, has the power to negate any mandating under Article 8, should their application by policymakers result in risks to market resilience, for example by removing access to non-EU manufacturers.

7. **The inclusion of the CE Marking and product-specific support requirements within the CRA do not relate to financial products but the applications and software that deliver those products. The haphazard application of consumer legislation, which has never been applied to financial services, serves only to confuse consumers and does not appropriately reflect the intangible nature of products provided by the financial sector.**

    - Consumer protection in the financial sector is proactively disclosed to consumers via enforced disclaimers, transparency regarding regulatory status and communication concerning consumer safeguards. All consumer protections in the financial sector relate to the financial product that is provided to the consumer. The CRA, in comparison, introduces consumer-related communication requirements and visible markings (the CE Marking) that do not apply to any of the financial

products that have been purchased by the consumer. The consumer is likely to not understand that the protections afforded by the CRA apply to the application or piece of software showing the financial product, and not the financial product itself. Members are concerned this introduces confusion and shows an inconsistent application of protections in financial services.

- This is further complicated via support requirements that were intended to relate to tangible digital products and which do not apply to the intangible nature of financial services. A single point of contact or requirement to aid consumers would apply only to the application and not the financial products. A consumer is unlikely to understand the nuanced interpretation of support for the "product with digital elements" with which they do not have any commercial or contractual relationship.

- The CRA includes a requirement that a withdrawn product with digital elements has a minimum support period for five years, retention of technical documentation and user guidance for ten years and proactive communication with the consumer when the support period ends. In financial services, this support period would apply to the applications and have no relation to the financial product that the consumer/s may hold. Members are concerned that any communications with consumers serves only to introduce confusion, with no net benefit from the consumer's perspective.

AFME Contacts

Marcus Corry
marcus.corry@afme.eu
+44 (0)20 3928 2679

Stefano Mazzocchi
stefano.mazzocchi@afme.eu
+32(0) 2883 5546