AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

John Berrigan, Director-General
Directorate-General for Financial Stability,
Financial Services and Capital Markets Union
Rue de Spa 2, 1000 Brussels
Belgium

Brussels, July 2023

Dear Director-General,

The Cyber Resilience Act (CRA) is a horizontal 'digital' product safety regulation that applies to financial services. As the CRA does not delineate between products and services, it applies to all elements of a financial institution's software or digitally accessible services, such as a retail banking application or private banking portfolio allocation services, despite them being covered by existing financial services regulation. Furthermore, the CRA would apply to all software or ICT services that support financial institution's digital services, such as the know-your-customer authentication software that is used for a retail banking application.

The financial services industry understands the importance of improving digital product vulnerabilities. The industry is currently already implementing the existing Digital Operational Resilience Act (DORA), which has the same objectives as the CRA and applies even higher requirements. As financial institutions use ICT systems to provide their services to customers, all in-scope ICT systems for the CRA are already in the scope of DORA. This has not been recognised by non-financial services authorities and the industry will therefore face significant duplication in terms of requirements, with no meaningful gain for improving cyber resilience in the EU – on the contrary, the implementation of CRA may be less effective due to the handling of both regimes from a compliance and risk management perspective.

Other industries, such as the medical devices industry, are recognised within the CRA to have their own equivalent regimes. While we understand that a financial services exemption may not be achievable, a significant amount of duplication could be avoided by, for instance, placing market surveillance powers and enforcement with financial authorities to the extent applicable, which should be taken forward by the policy makers. In addition, some provisions, such as on incident reporting, also have distinct provisions within DORA, which leads to the consequence that the CRA contravenes the aim of DORA to harmonise financial services regulation across the EU.

Further clarity regarding how the CRA applies to services, and more specifically to those provided within highly regulated industries, is required. A gap assessment between the CRA and DORA may be a helpful instrument for the financial services industry to ensure that the CRA does not create unnecessary duplication, which could complicate efforts to control risk.

We would welcome any opportunity to speak further to you about the CRA and how it could impact existing financial services regulation and compliance by financial institutions.

Best regards,
AmCham EU