European Financial Services
Round Table

Mr. Valdis Dombrovskis
Executive Vice-President for An Economy
that Works for People
European Commission
Berlaymont
B-1049 Brussels
Belgium

18 March 2020

Strengthening the digital operational resilience framework for financial services in the EU

Dear Executive Vice-President Dombrovskis,

Financial firms, as operators and major users of critical global infrastructure, are exposed daily to cyber security risks due to their primary function as economic intermediaries and to the interconnected global environment in which they operate. An attack on one part of the global financial system can quickly spread to others through dependencies, including newer non-traditional actors such as Fintechs and Big Techs.

The EFR thus very much welcomes the European Commission's initiatives outlined in the 2020 Work Programme to build a robust and agile cyber security policy and supervisory framework. We also note that the European Parliament, the Council and the ESAs have underlined the critical importance of cyber security, highlighting the urgent need for having in place better testing, more information sharing and enhanced coordination between authorities.

In particular, the EFR supports the initiatives that are envisaged to improve the existing framework by both amending existing rules, particularly in the proposed review of the Network and Information Security (NIS) Directive and the consultation on how an enhanced framework for digital operational resilience for financial services could be set up, with the aim to introduce a legislative proposal on financial services cyber resilience in the second half of this year.

In the last few years, the EU cyber security framework has been progressively reinforced, notably with the entry into force of the NIS Directive, the Revised Payment Services Directive, and the General Data Protection Regulation (GDPR). In addition to these EU wide initiatives we have also seen a number of Member States strengthening their own regulatory frameworks for cyber security. But, despite convergence in high level requirements expectations, technical specifications and supervisory practices still differ across EU jurisdictions, leading to a complex and fragmented regulatory

landscape across Europe. This is evident in the different interpretations by national authorities of EU rules which lead to uncertainty and potential delay to an efficient and collaborative response to cyber attacks. As an example, there is a lack of uniformity of the implementation of the NIS directive across member states since they individually determine which organisations are classified as operators of essential services. The European Commission's own Report of October 2019 assessing "the consistency of the approaches in the identification of operators of essential services" found that some Member States have not identified any operators of essential services in the banking sector, citing that operators are providing services covered by "leges speciales". There is also a lack of consistency regarding the levels of detail, definitions, and thresholds and to which authority incident notifications should be made. This matters because it makes it more challenging both to identify incident trends and accurately estimate the true scale of the risk in a disinterested data-based manner. In a globalised digital environment, an overarching regulation would provide a more consistent and harmonised overall level of digital operational resilience in the EU. Therefore, the EFR believes that the existing EU Directive on security of network and information systems (NIS Directive) should be transformed into a regulation. Moreover, although GDPR and NIS address different objectives, there is considerable overlap between the two pieces of legislation due to the GDPR's provisions on security and the likelihood that most organisations covered by NIS will also be data controllers (or even data processors). NIS requires notification to competent authorities if an incident takes place. But where an incident is, or becomes, a personal data breach, then there is also need to inform data protection authorities separately. Timelines, content and competent authorities vary in the different pieces of legislation, while the incident management processes of private companies are one and the same.

The EFR therefore agrees with the ESAs recent advice to the European Commission to consider a comprehensive and harmonised system of Information and Communication Technology ("ICT") incident reporting requirements for the financial sector. We also support the EC objective of streamlining and improving existing rules in the EU regulatory and supervisory framework for cyber security and making it more risk-based by focusing on actual cyber threats. We note that any system that will be set up will not only depend on adequate formal rules, but most certainly also on trust between the parties involved. Moreover, the alignment on international norms such as ISO 27001, will help to ensure that a common language exists to interpret the requirements and that a trained workforce exists in the EU Market to facilitate the implementation of the regulation.

In addition to the harmonisation of regulations, the EFR considers that it is very important to establish a mechanism for effective cyber risk information sharing among industry and public authorities based on trust, due to the borderless nature of risks and the level of interconnectedness of large financial institutions and the broader economic infrastructure. A crucial priority therefore is sharing intelligence and information on cyber incidents in a bi-directional way among key public and private actors through an efficient, robust and secure process. At present there is no Europe-wide mechanism for large financial institutions to share cyber intelligence.

Because many cyber security risks and cyber attacks also originate outside the financial sector, public authorities and the financial sector should reflect on possibilities - just as with KYC / AML - for cooperation beyond the financial sector in order to successfully mitigate cyber related risks to the global IT infrastructure. Part of a framework for information sharing could be the ability for the financial sector to have also access to cross-sector data with external trends. Through cross-sector analysis, planning, and strategic industry partnership efforts, the EU should be leading the effort to both defend critical infrastructure and ensure its resilience.

In conclusion, we would recommend for the European Commission to take into account the following considerations:

- The EFR recommends that the European Commission, in cooperation with the ESAs, develops a coherent cyber resilience testing framework for the EU financial sector, and in particular to provide guidelines and principles to supervisors to promote an EU-wide understanding of good practices; cost-effective in order to take into account firms' size and importance for the market. Incident reporting through such platform should align with and industry standard reporting framework such as Mitre Att&ck. This framework should be mandatory also for the payment players (FinTech, BigTech) in order to be fully effective.
- EFR recommends that the European Commission should expand the scope of the upcoming legislative initiative to align, as a minimum, the incident reporting requirements of the NIS Directive and GDPR to deliver a more coherent approach to cyber security, which will be essential for the resilience objective. Data privacy and cyber security are very important policy objectives and they can both co-exist to the benefit of all those concerned.
- Sharing of cyber security intelligence and incident information among industry peers and public authorities is widely acknowledged as essential to combatting cyber crime. **EFR believes that further EU action in this area would be beneficial**, in particular through the harmonisation of legislation to explicitly allow such information sharing by systemic institutions. For its part, the EFR has been exploring different modalities and options under which such a European platform could be set up.

We encourage the European Commission to continue pursuing these important policies. The EFR looks forward to engaging with you and your services to ensure a framework that will be more effective and will strengthen cyber security in Europe.

Yours sincerely,

Jean Lemierre
EFR Chairman
Chairman BNP Paribas