EPIF response to the Commission's consultation on digital operational resilience framework for financial services - Making the EU financial services sector more secure.

March 2019

ABOUT EPIF (EUROPEAN PAYMENT INSTITUTIONS FEDERATION)

EPIF, founded in 2011, represents the interests of the non-bank payment sector at the European level. We currently have over 190 authorised payment institutions and other non-bank payment providers as our members offering services in every part of Europe. **EPIF** thus represents roughly one third of all authorized Payment Institutions ("PI") in Europe. All of our members operate online. Our diverse membership includes a broad range of business models, including:

- Three-party Card Network Schemes
- E-Money Providers
- E-Payment Service Providers and Gateways
- Money Transfer Operators
- Acquirers
- Digital Wallets
- FX Payment Providers and Operators
- Payment Processing Services
- Card Issuers
- Independent Card Processors
- Third Party Providers
- Payment Collectors

EPIF seeks to represent the voice of the PI industry and the non-bank payment sector with EU institutions, policy-makers and stakeholders. We aim to play a constructive role in shaping and developing market conditions for payments in a modern and constantly evolving environment. It is our desire to promote a single EU payments market via the removal of excessive regulatory obstacles.

We wish to be seen as a provider for efficient payments in that single market and it is our aim to increase payment product diversification and innovation tailored to the needs of payment users (e.g. via mobile and internet).

EPIF's response:

Enhancing existing ICT and risk management requirements contained within existing EU law taking into account global standards or recommendations on operational resilience makes sense, however studies on cybersecurity highlight that no one size fits all so proportionality is required. What is key is that there is a top-down approach from the executives of financial institutions to governing these risks, identifying what is needed to be protected and effective controls exist to mitigate risk. Metrics and indicators are required for all critical controls to understand whether they are functioning effectively to understand whether risks are being managed. EPIF members are compliant with the PSD2 and the EBA Guidelines on operational risk and major incident reporting. This framework is already quite robust and includes many of the requirements discussed in the consultation

EPIF agree that existing operational resilience reporting requirements need to be harmonised and streamlined to improve monitoring and analysis of all operational resilience related risks. Clarity is required in terms of what is reportable, defined thresholds of minimum requirements, timelines, information required and to whom reports, both from a sender and receiver perspective. Harmonised incident reporting can help improve compliance challenges, reduce regulatory and operational burdens that financial institutions and most importantly free up valuable time for both financial institutions and the authorities to deal with business continuity and mitigating further potential damage.

Regarding exchanges of information, what is crucial is that requirements of what information should be shared should be loosely rather than strictly defined. Strict requirements can constraint the scope of willingness to share when operational resilience risks themselves are broad and evolve overtime.

- For the sharing of incident reports between NCAs, it should be limited to cross-border cases and only with those NCAs in the member states affected.
- For the sharing of information between financial services providers, it should not be mandatory, but rather promoted through neutral third-party intermediaries that provide a safe and trusted place for anonymous threat information to be shared.

EPIF agrees on the importance of having a comprehensive digital operational resilience-testing framework as a mechanism to anticipate assess operational vulnerabilities. A strong testing regime helps develop a culture for continuous improvement as issues are first discovered and then fixed. Testing operational resilience defences across a financial institution needs to focus on enhancing the effectiveness of controls across people, process and technology and requires that there is a root cause analysis of incidents and near misses to help challenge the effectiveness of controls. A one-size fits all approach will not work. Proportionality is required to ensure that any framework is flexible enough to allow for the variety of institutions across the EU. Harmony among global approaches to resiliency frameworks also assists financial institutions in focusing efforts on maintaining operational resilience rather than compliance with fractured regulatory rules.

Effective operational resilience also requires enhancing supervisory capabilities by investing time and money in digital technology capabilities so they can better challenge the industry and provide necessary assistance/guidelines. There is possibly a role for the ESAs to assist in raising standards through peer review. One example could be creating an EU central hub for incident reporting, so that the exchange of information can be done through a secure web-based tool to exchange data, which would guarantee the confidentiality of the information.

EPIF agrees that outsourcing to third party providers, whilst bringing many benefits, might pose new operational risks through increased interconnectedness. In addition, widespread market usage can lead to concentration risk with potential implications for financial stability. That said, it is often niche, or more traditional third-party providers that present the greatest threat to operational resilience. As a first step, firms need to analyse potential risks associated with suppliers, which may, or may not be exacerbated by concentration risk. Supervisory need also to work, collaborate and test cross sectorally.

With the delivery of important services increasingly reliant on third party providers, there is a need for a concerted effort to improve the way in which these key relationships are managed. EPIF supports having an EU framework

that provides further guidance on expectations for contractual arrangements with service providers. Ultimately, financial institutions should review contracts to consider how to better align their interests with key suppliers through alignment in operational resilience outcomes.

Effective and timely information sharing helps contribute to enhance operational resilience and prevention of the number and severity of incidents. It is important not to focus on information sharing across Member States and financial services national competent authorities. In the area of payments for example, cyber-attacks can result through use of the telecommunication network and early the interconnectedness across communication channels needs to be reflected in information sharing and cooperation arrangements among public authorities.

The NIS Directive deals more with national security capabilities and is intended to avoid are references to national security. That said, as currently drafted it does mention a number of financial service sectors. Given the increased trend towards outsourcing of non-core operations across both financial and non-financial services and crucially that resilience is only as strong as the weakest link it might be worth reviewing the scope of the Directive.