March 19, 2020

Submitted electronically
European Commission
Rue de la Loi / Wetstraat, 170
B-1049 Bruxelles/Brussel
Belgique/België

Re: Financial services – improving resilience against cyberattacks (new rules)

Dear Sir or Madam:

The European Network of Credit Unions (ENCU) appreciates the opportunity to comment on the European Commission's initiative on improving resilience against cyberattacks in the financial services sector.[1] Credit unions are consumer-owned, not-for-profit financial cooperatives that promote financial inclusion in underserved European communities by offering their members affordable and easily understandable financial products. There are approximately 1,000 credit unions in the European Union (EU) with more than EUR 20 billion in total assets and 7 million physical person members.[2]

ENCU supports the European Commission's (Commission) effort to amend existing rules, specifically the Network and Information Security (NIS) Directive, which is a new law on digital operational resilience for financial services. We further agree with the Commission's objective to harmonize requirements to address Information and Communication Technology (ICT) security risks through "effective monitoring of compliance by regulated financial entities with (increased) operational resilience provisions"[3] ENCU respectfully requests, however, that the weight of any new rules do not disproportionately impact credit unions and other financial cooperatives compared to their larger banking counterparts.

We caution that regulators do not insist that any definitive or narrowly construed system be required as that can be prohibitive for smaller institutions. Extending limited resources on cybersecurity expertise, training, staffing and programs are expensive and are a large investment that require careful consideration before implementing; therefore, credit unions need proportional rules that are tailored to the size, risk, and complexity of the institution. This allows credit unions and other small financial institutions to implement a system without the need to

[1] The European Commission's *Financial services – improving resilience against cyberattacks (new rules)*, *available at*: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act-.
[2] *See* "Credit Unions in Europe;" http://creditunionnetwork.eu/cus_in_europe.
[3] See Inception Impact Assessment; Ref. Ares(2019)7834637 - 19/12/2019, Regulation on Digital Operational Resilience for the Financial Sectors.

creditunionnetwork.eu
Rue du Trône 60, 1st Floor
Brussels 1050
Belgium
Tel: +32 2 626 9500
Fax: +32 2 626 9501
info@creditunionnetwork.eu

utilize cost prohibitive resources or engage in extensive analysis that can be scrutinized by a regulator.

The Commission has expressly stated that it is contemplating policy considerations such as "targeted amendments to EU financial services legislation (while the possible revision of the NIS Directive may bring along the opportunity to revisit its scope and the depth of its substantive requirements) and a general yet bespoke legal framework addressing the digital operational resilience for all regulated financial entities, applying across the different financial sectors taking into account, where relevant, specific needs arising for financial services sectors."[4] ENCU would like to highlight that the specific needs of the credit union sector includes a risk-based, proportional, and tailored approach to any implementation of new rules law on digital operational resilience for financial services. Furthermore, we would recommend the Commission's approach to this initiative include no mandatory rules to any particular solution, but instead provide guidance and a roadmap.

In the United States, the National Credit Union Association (NCUA), which regulates federal credit unions and insures deposits at all federally insured credit unions, relies on Federal Financial Institutions Examination Council (FFIEC) to promote uniform supervision of financial institutions; and prescribe uniform principles, standards, and report forms for the federal examination of financial institutions. The FFIEC has addressed "significant changes in… financial institution technology since 1996.They incorporate changes in technology-related risks and controls and follow a risk-based approach to evaluating risk management practices."[5] Both banks and credit unions use the FFIEC Self-Assessment tool, which it is not mandatory but provides valuable guidance on how to approach cybersecurity and additionally allows for a tailored approach for credit unions. Tiering requirements to allow for a range of appropriate functionalities would benefit credit unions as this would likely result in systems more appropriate for their size and complexity and likely allow for less expensive systems to be developed.

Finally, ENCU would like to urge the Commission to reinforce their objective to harmonize requirements across the EU, but allow for enforcement and tailoring of any cybersecurity requirements to one national-level prudential regulator. Multiple requirements from more than one regulator has proven to be conflicting, convoluted and complex for credit unions. Any confusion can escalate duplicating efforts, therefore increasing costs and depleting much needed resources within the credit union.[6] We note that currently all regulatory bodies in the EU currently expect regulated institutions to have a board-approved information security strategy, policy and procedures for cyber risk and cyber resiliency. As such, we urge focusing on

[4] Id at. section B. Objectives and Policy Options.
[5] See NUCA website at: https://www.ncua.gov/regulation-supervision/regulatory-compliance-resources/cybersecurity-resources.
[6] *See* Basel Committee on Banking Supervision Report on Cyber Resilience Practices (December 2018) *available at* https://www.sullcrom.com/files/upload/SC-Publication-Basel-Committee-Surveys-Cybersecurity-Regulation-Across-Globe.pdf

information sharing practices among institutions and among regulators, but with a close eye to limiting increased regulatory burden on credit unions.

ENCU reiterates its support for the Commission's initiative "to strengthen the digital operational resilience of the EU financial sector entities"[7], however, we respectfully appeal to the Commission to consider the unique structure of credit unions and the disproportionate compliance requirements that are posed on them when finalizing your rules. We respectfully ask the Commission for risk-based and proportional requirements that are tailored to credit unions; and we request consideration for non-mandatory guidelines instead of hard rules to address digital operational resilience; and we request that the Commission appoint one prudential regulator for consistency in enforcement and regulation. These elements will aid credit unions in their mission to improve financial inclusion and provide affordable and necessary services to the underserved European Union community. The European Network of Credit Unions appreciates the opportunity to comment on the European Commission's initiative on money laundering & terrorism financing action plan. Please do not hesitate to contact me (information below) or Denitsa Marchevska by email at info@creditunionnetwork.eu or phone at +32 2 626 9500 should you have any questions regarding our comments.

Sincerely,

Panya Monford, Esq.
Advocacy Counsel
European Network of Credit Unions
World Council of Credit Unions
pmonford@woccu.org
T: +1-202-510-9347
C: +1-202-256-9897

[7] See Inception Impact Assessment; Ref. Ares (2019)7834637 - 19/12/2019, Regulation on Digital Operational Resilience for the Financial Sectors; section B. Objectives and Policy Options.