ELECTRONIC TRANSACTIONS ASSOCIATION

1620 L Street NW
Suite 1020
Washington, DC 20036

www.electran.org
T 800.695.5509
T 202.828.2635
F 202.828.2639

February 13, 2017

Via electronic submission to
regs.comments@federalreserve.gov
regs.comments@occ.treas.gov
comments@fdic.gov

Robert deV. Frierson, Secretary
Board of Governors of the Federal Reserve System
20th St. and Constitution Ave. NW
Washington, DC 20551

Legislative and Regulatory Activities Division
Office of the Comptroller of the Currency
400 7th St. SW, Suite 3E-218, Mail Stop 9W-11
Washington, DC 20219

Robert E. Feldman, Executive Secretary
Federal Deposit Insurance Corporation
550 17th St. NW
Washington, DC 20429

Re: Enhanced Cyber Risk Management Standards
Docket No. R-1550/RIN7100-AE-61 (Board)
Docket ID OCC-2016-0016 (OCC)
RIN 3064-AE45 (FDIC)

On October 19, 2016, in the above captioned dockets, the Board of Governors of the Federal Reserve System ("Board"), the Office of the Comptroller of the Currency ("OCC"), and the Federal Deposit Insurance Corporation ("FDIC") (collectively, the Agencies) issued an Advanced Notice of Proposed Rulemaking ("ANPR") regarding enhanced cyber risk management standards ("Enhanced Standards") for large and interconnected entities under their supervision and those entities' service providers.[1]

The Electronic Transactions Association ("ETA")[2] appreciates this opportunity to provide comments on the Enhanced Standards ANPR. ETA is the leading trade association for the payments industry, representing nearly 550 companies worldwide involved in electronic transaction processing products and services. The purpose of ETA is to influence, monitor, and shape the payments industry by providing leadership through education, advocacy, and the

[1] 81 Fed. Reg. at 74315.
[2] http://www.electran.org/.

ELECTRONIC TRANSACTIONS ASSOCIATION
1620 L Street NW
Suite 1020
Washington, DC 20036
www.electran.org
T 800.695.5509
T 202.828.2635
F 202.828.2639

exchange of information. ETA's membership spans the breadth of the payments industry, and includes financial institutions, payment processors, independent sales organizations, and equipment suppliers.

ETA supports the Agencies' efforts to strengthen cybersecurity within the country's financial system. However, we do not believe that developing another set of regulations as proposed in the ANPR is the right approach at this time. As discussed in detail below, financial institutions and their third-party service providers are already subject to an inordinate number of cybersecurity rules and frameworks as a result of uncoordinated efforts taking place at the federal, state and industry levels. Rather than issue another set of compliance obligations, ETA respectfully requests that the Agencies place this effort on hold, and work with the appropriate government and industry groups to harmonize existing cybersecurity rules, which already address many of the Enhanced Standards proposed in the ANPR. Should any regulatory gaps be identified as a result of these efforts, the Agencies' may consider addressing those specific deficiencies, but developing an additional set of blanket cybersecurity rules will only exacerbate the current problem of disjointed regulation in this space.

I. Financial Services Sector Leadership on Cybersecurity Practices and Regulation

The financial services industry, including financial institutions and their third-party service providers, is a leader in cybersecurity. Since the advent of the Internet and the migration of financial services to the online sphere, the financial services sector has demonstrated a robust and sustained commitment to ensuring the protection of customer information and the integrity of financial systems and networks. The best-in-class security protocols and controls developed by the financial services sector are the product of intense study and dedicated research devoted to the pursuit of innovation and the deployment of new security technologies to protect financial information. These advancements driven by collective investment by the sector will continue, and will extend into the areas of mobile devices, cloud services, and beyond.

In part, the sector's leading security practices and processes reflect the sensitivity of the data itself and the consequences that would arise for consumers and the economy as a whole should financial services networks and system be compromised significantly or repeatedly.

The industry also was the first to formalize information sharing about threats and vulnerabilities, through the establishment of the information sharing and analysis center FS-ISAC. FS-ISAC is a recognized globally as the gold standard for industry collaboration and dedication to the mission of reducing cybersecurity risks through the process of individual companies sharing information related to attempted and successful cyberattacks, so that the entire industry can benefit from the knowledge and experience.

Throughout this time, financial institutions have been subject to rigorous and comprehensive cybersecurity regulations, supervisory guidance and are regularly examined by federal and state authorities. These include the Gramm-Leach-Bliley Act of 1999 (including the

"Interagency Guidelines Establishing Information Security Standards" regulation), the Fair Credit Reporting Act, the Right to Financial Privacy Act as well as extensive regulations, and supervisory guidance from the Federal Financial Institutions Examination Council ("FFIEC," or "Council") addressing information security, vendor management and business continuity risks.

Subsequently, in February 2013, President Obama directed the Department of Commerce, through NIST, to develop a voluntary framework for improving critical infrastructure cybersecurity.[3] From the start, the financial services sector was supportive and engaged in this process, participating in all six NIST cybersecurity workshops and submitting responses to the various Federal Register requests for information. The final Framework released by NIST includes several of the recommendations provided by the financial services sector, including the decision to adopt a risk-based methodology. The open and transparent process that led to the NIST Framework resulted in a document that has been widely embraced beyond the critical infrastructure sector by thousands of business and enterprises and across all sectors of the economy.

Moreover, as recently as September 2016, the New York State Department of Financial Services ("DFS") also announced the release of cybersecurity regulations for financial service companies, which are scheduled to go into effect on March 1, 2017.[4] Under the regulations, covered entities are required to develop a cybersecurity program designed to address six core functions and at least fourteen specified areas, including but not limited to: cyber risk assessment and governance, asset inventory and device management, systems and network security, vendor and third party service provider management, and incident response and recovery. Commencing February 15, 2018, covered entities will have to certify annually that they are in compliance with the rules and retain supporting records for five years.

II. Need for Harmonization of Existing Cybersecurity Frameworks

The cybersecurity regulations and initiatives discussed in these comments are by no means exhaustive. Cybersecurity has become a prominent, if not paramount, issue for many financial regulators, and many of those regulators are engaged in ongoing efforts to address cybersecurity issues faced by the entities that they regulate. As is often the case with regulatory efforts that are new and evolving, different financial regulators are still trying to make sense of the regulatory landscape, and are using different types of regulatory tools, moving at different speeds, and using differing degrees of comprehensiveness.

For example, the FFIEC's Cybersecurity and Critical Infrastructure Working Group ("CCIWG") has developed and is beginning to push the use of a new cybersecurity assessment tool as part of the prudential regulation regime of the banking regulators and their holding companies.[5] The Commodity Futures Trading Commission ("CFTC") has finalized rules that

[3] Exec. Order No. 13,636, 78 Fed. Reg. 11739 (Feb. 12, 2013).
[4] http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf.
[5] *See* https://www.ffiec.gov/cyberassessmenttool.htm.

would apply certain cybersecurity standards to derivatives clearing organizations, designated contract markets, swap execution facilities, and swap data repositories.[6] The Securities and Exchange Commission ("SEC") has been engaged in issuing more piecemeal cybersecurity guidance, primarily through subdivisions of the agency like the Office of Compliance Inspections and Examinations ("OCIE") and the Division of Investment Management. The Financial Industry Regulatory Authority ("FINRA") and National Futures Association ("NFA"), the self-regulatory organizations ("SROs") that enforce many of the nation's securities, commodities, and derivatives trading laws, also have been active on cybersecurity regulation. In early 2015, FINRA issued a report intended to help broker-dealers and others address cybersecurity issues, and in October 2015, the NFA issued a new interpretive notice regarding protection of Information Technology ("IT") systems containing customer or financial information.

In addition to being at times contradictory and superfluous, these various and substantial compliance obligations are imposing significant compliance costs on businesses and are affecting the ability of enterprises to institute customized information programs that reflect their unique needs, instead creating compliance-focused programs that depart from entities' optimal cybersecurity posture. Costs of compliance with regulatory directives are high, and these costs are compounded where multiple regulatory regimes apply. Any efforts in this space should allow flexibility to be tailored based on risk profiles. In the two years since it was issued, the NIST Framework has been widely followed among financial firms, yet inconsistencies between the Framework and the emerging regulatory guidance noted above is triggering substantial security and compliance concerns.

Rather than issue another set of regulations, what would be most helpful to the financial services industry at this time is a concerted effort to harmonize the various rules and frameworks already in existence. This effort would not only benefit industry, but would also benefit our regulators from the perspective of being able to focus efforts more efficiently and effectively in areas that have not yet been addressed and may cause the most risk. Harmonization would move us all a step in the right direction of starting to address the growing thicket of cybersecurity compliance obligations that are spreading across the financial services sector. In addition, this would allow for continued marketplace competition where market participants have consistent expectation across regulators.

With the industry's cybersecurity leadership, changing landscape and various regulatory work streams in mind, ETA respectfully requests that the Agencies place this rulemaking on hold and first explore ways in which the Agencies might take leadership in or join existing efforts to harmonize the cybersecurity rules and frameworks already in place. Should any regulatory gaps be identified as a result of these efforts, the Agencies' may consider addressing those specific deficiencies, but developing an additional set of blanket cybersecurity rules will only exacerbate the current problem of disjointed regulation in this space.

---

[6] *See* http://www.cftc.gov/idc/groups/public/@newsroom/documents/file/federalregister090816c.pdf; http://www.cftc.gov/idc/groups/public/@newsroom/documents/file/federalregister090816b.pdf.

ELECTRONIC TRANSACTIONS ASSOCIATION

1620 L Street NW
Suite 1020
Washington, DC 20036

www.electran.org
T 800.695.5509
T 202.828.2635
F 202.828.2639

III. Specific Comments on the Enhanced Standards ANPR

To the extent that the Agencies decide to move forward with this rulemaking and propose more developed standards in a future filing, ETA submits the following comments for your consideration.

First, cyber threats vary greatly by institution and by the activities they perform. Indeed, every function that a financial institution or a third party service provider engages in does not create the same potential for risk or impact. Thus, the cybersecurity framework ultimately adopted by the Agencies should contemplate the variances in cyber risks based on the type of institution and by the activities in which the institution participates. As currently written, the ANPR fails to account for these differences.

Moreover, the ANPR considers applying the Enhanced Standards directly to third-party service providers. ETA strongly opposes this measure. As currently proposed in the ANPR, the Enhanced Standards are written from the perspective of financial institutions, and do not necessarily translate over to third party service providers. As discussed above, the proposed Enhanced Standards fail to account for all the different types of functions a third-party service provider can fulfill and the varying level of criticality of such functions. If the Agencies decide to move forward on application then the current oversight of technology service providers connected to U.S. depository institutions by the FFIEC may provide the appropriate guidance to best address the nature of risks covered by the ANPR. The approach in the FFIEC IT Examination Handbook may be suitable to achieve our shared goals when it comes to the supervision of third-party service provider so long as it is sufficiently flexible to be tailored to the specific services being provided.

Finally, of the implementation approaches suggested, ETA most agrees with proposing the standards as a combination of a regulatory requirement to maintain a risk management framework for cyber risks along with a policy statement or guidance that describes minimum expectations for the framework.[7] ETA reiterates its position that the Agencies should not issue any new cybersecurity regulations at this time. However, to the extent the Agencies move forward with this effort, ETA believes that a basic regulatory framework requirement combined with a policy statement is the preferred approach to implementing any Enhanced Standards.

* * *

ETA thanks you for the opportunity to submit these comments.

Respectfully submitted,

[7] ANPR at 44.

ELECTRONIC TRANSACTIONS ASSOCIATION

1620 L Street NW
Suite 1020
Washington, DC 20036

www.electran.org
T 800.695.5509
T 202.828.2635
F 202.828.2639

Scott Talbott
Senior Vice President of Government Affairs
Electronic Transactions Association