February 13, 2017

Via Electronic Submission

Robert deV. Frierson
Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Washington, DC 20551
regs.comments@federalreserve.gov

Legislative and Regulatory Activities Division
Office of the Comptroller of the Currency
400 7th Street, SW, suite 3E-218, mail stop 9W-11
Washington, DC 20219
regs.comments@occ.treas.gov.

Robert E. Feldman
Executive Secretary
Attn: Comments, Federal Deposit Insurance Corporation
550 17th Street, NW
Washington, DC 20429
Comments@fdic.gov

Re: (Fed) Docket No. R-1550 and RIN 7100-AE-61, (OCC) Docket ID OCC-2016-0016, (FDIC) RIN 3064-AE45

Dear Sirs and Madams:

NACHA – The Electronic Payments Association ("NACHA") welcomes the opportunity to provide comments on the joint advance notice of proposed rulemaking (the "ANPR") regarding enhanced cyber risk management standards published by 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").

NACHA supports the comments being submitted separately by the Financial Services Sector Coordinating Council ("FSSCC") and The Clearing House Association L.L.C. ("TCH"). Like those organizations, NACHA believes that: (i) there is not a demonstrated need for the enhanced cybersecurity standards contemplated by the ANPR; (ii) if the Agencies determine upon further review that there are gaps in existing guidance, any standards adopted should be risk-based, flexible and not overly prescriptive; (iii) the Agencies should not create a newly defined category of "sector-critical systems" for this purpose when the existing category of designated systemically important financial market utilities ("SIFMUs") adequately identifies the group of entities that should be considered

"critical" for this purpose; and (iv) to the extent enhanced standards apply to third-party service providers, they would be applied more effectively via direct oversight by the Agencies in situations where the Agencies have that authority. After first providing background on NACHA, we offer additional comments in each of these areas.

I. Background: The ACH Network – Who We Are

The ACH Network is a hub for the electronic movement of money and other related data, providing a safe, secure and reliable network for direct consumer, business and government payments. It is a fully electronic payment system that enables movement of money between accounts held at virtually all of the nation's financial institutions.

The general public is most familiar with the ACH Network through various "direct deposit" programs, which are widely used for payroll, tax refunds and government benefit payments, including Social Security. Automated and online bill payments are other common and growing uses of the ACH Network by individual customers. Businesses use the ACH Network for similar purposes, as well as to convert payments made by checks into electronic debits. The single largest user of the ACH Network is the Federal government, which uses the ACH Network for employee payroll and retirement distributions, benefit payments, tax collections and refunds, vendor payments and collections of other payments from individuals and businesses.

The ACH Network is managed and operated by NACHA and the ACH Operators. Currently, there are two ACH Operators in the ACH Network: The Clearing House Payments Company L.L.C., an affiliate of TCH (the "Private Operator"), and the Federal Reserve Banks (the "Fed Operator"). Each ACH Operator serves as an intermediary among participating financial institutions holding the accounts from which ACH transactions (both debit and credit) are initiated and the financial institutions to which such ACH transactions are destined. The ACH Operators sort the transactions initiated in the ACH Network by destination and make files available to each receiving financial institution. In each case, interbank positions are then netted and settled by the ACH Operator via transfers among the settlement accounts of the participating financial institutions or their correspondents (generally the institution's reserve or clearing account held with a Federal Reserve Bank). With respect to the Private Operator, this interbank settlement is effected through the Federal Reserve's Net Settlement Service.

NACHA is the not-for-profit organization that, through its board of directors, staff and various committees, manages the ACH Network. NACHA develops and maintains standards for electronic fund transfers using the ACH Network, authors the *NACHA Operating Rules*, and enforces the *NACHA Operating Rules* through its National System of Fines. The *NACHA Operating Rules* govern the exchange of ACH payments, establish transaction formats and authorization requirements, and define the roles and responsibilities of ACH Network participants. These participants include:

- Originators (account holders that initiate credit or debit entries into the ACH Network);
- Receivers (account holders that have authorized receipt of a credit or debit entry by their financial institutions);

- ODFIs (depository financial institutions that hold the accounts of Originators, originate entries on behalf of their account-holding Originators and debit or credit such entries to the accounts of their Originators), and

- RDFIs (depository financial institutions that hold the accounts of Receivers, receive ACH entries through the ACH Network and debit or credit such entries to the accounts of their Receivers).

Since 1974, NACHA has successfully administered these private-sector operating rules governing the exchange of ACH payments, and defining the roles and responsibilities of financial institutions and other participants in the ACH Network. In its role as the standards organization for payments through the ACH Network and author of the *NACHA Operating Rules*, NACHA represents and brings together over 11,000 participating financial institutions of all sizes and types throughout the United States, both directly and through 11 Regional Payments Associations. NACHA also brings together nearly 400 other companies and organizations through our industry membership programs, advisory groups, and committees.

The *NACHA Operating Rules* are amended through a deliberative and inclusive process similar to that used by Federal agencies under the Administrative Procedures Act. This allows participants in the ACH Network – commercial banks, community banks, credit unions, large corporations, small businesses, consumer advocates, and industry vendors – the opportunity to comment on proposed rule changes. Through this inclusive process, NACHA is able to maintain a fair and equitable set of rules that create certainty for all parties using the ACH Network. The *NACHA Operating Rules* work in concert with applicable laws and regulations to provide a legal and business foundation for the use of ACH payments.

Private-sector rulemaking provides the flexibility to promptly identify and respond to participant requirements and new technologies, and to define in sufficient detail the roles and responsibilities of participants in the ACH Network. From this foundation, the *NACHA Operating Rules* promote innovation and efficiency, and provide security and certainty regarding ACH payments.

II. Comments on the ANPR

In further support of the points made by FSSCC and TCH, we offer the following comments.

A. The ANPR Does Not Adequately Address the Need for Enhanced Standards

NACHA respectfully suggests that the ANPR does not demonstrate a need for yet another set of cybersecurity standards, and that additional work should be done before a decision is made to establish and implement such standards. Entities that would be subject to the enhanced standards are already subject to a myriad of requirements that relate to cybersecurity. For example:[1]

[1] A more complete recitation of recent agency cybersecurity releases is attached to the FSSCC comment letter.

- the Gramm-Leach-Bliley Act and the subsequent Interagency Guidelines Establishing Information Security Standards require covered institutions to develop and maintain comprehensive information security programs that include administrative, technical, and physical safeguards to protect the security, confidentiality and integrity of nonpublic personal information;

- the Federal Financial Institutions Examination Council ("FFIEC"), of which the Agencies are members, has promulgated a number of relevant materials that are used by the Agencies to examine financial institutions (and certain of their service providers), including the FFIEC IT Examination Handbooks and the FFIEC Cybersecurity Assessment Tool ("CAT");

- the Agencies, individually and at times in combination with each other, have issued their own cyber-related guidance. For example, in 2003 the Board, the OCC and the Securities and Exchange Commission ("SEC") issued the Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System; and in 2013, the OCC issued OCC Bulletin 2013-29 (Risk Management Guidance relating to Third-Party Relationships), which, among other things, addresses security requirements;

- in response to Executive Order 13636 ("Improving Critical Infrastructure Cybersecurity"), which was issued in 2013, the National Institute of Standards and Technology ("NIST") developed, with the participation of thousands of cybersecurity professionals, the NIST Cybersecurity Framework, which reflects a consensus among industry experts on the most effective approach to improve cybersecurity; and

- the Committee on Payments and Market Infrastructure ("CPMI") and the Board of International Organization of Security Commissions ("IOSCO") have issued cyber resilience guidance.

Thus, there already exists a significant body of requirements, guidance and industry standards, based on input from all stakeholders, that the financial industry relies upon in implementing effective cybersecurity protections. Financial institutions have expended significant resources to design cybersecurity programs to address these and other cybersecurity requirements, and in particular to align with the NIST framework and comply with the FFIEC CAT.

The ANPR does not include any significant analysis of whether there are any "gaps" in the existing cybersecurity regulatory framework created by the aforementioned guidance or of how best to address such gaps. Without such a gap analysis, the ANPR is likely to lead to the imposition of duplicative, or even conflicting, requirements. This would cause financial institutions to divert resources from substantive cybersecurity efforts to the unproductive administrative task of mapping and translating the various standards and requirements to ensure compliance. The critical nature of cybersecurity makes it all the more important that the Agencies take care that any initiative in this area enables actual improvements in substantive security efforts, rather than layering processes which do more to impede than to enable that security.

For these reasons, NACHA requests that the Agencies undertake a more detailed assessment of the existing cybersecurity framework and rules, involving industry professionals and other stakeholders, to determine whether there is any need for enhanced standards. As part of that assessment, we believe the Agencies should examine not only whether there are gaps in existing standards, but also whether any existing standards are ineffective, duplicative, conflicting or simply inefficient in terms of the cost of compliance as compared to the effectiveness in minimizing cybersecurity risks. Indeed, given the plethora of existing guidance in the area, an essential element of any further such guidance should be to rationalize current standards. If, based on such an assessment, the Agencies identify areas where existing standards are insufficient, the Agencies could then propose more focused guidance that would be more likely to promote the goal of improved protection against cybersecurity risks.

B. Any Standards Must Be Risk-Based, Flexible and Not Prescriptive

As other commenters have noted, an effective cybersecurity program must be sufficiently flexible to adapt to ever-changing technology and an ever-evolving risk environment. In order to maintain that flexibility, financial institutions cannot be constrained by regulatory mandates that either do not recognize the wide range of circumstances that may be faced by different institutions or that attempt to legislate specific standards that interfere with the ability of institutions to make risk judgments in connection with the allocation of resources to prevent, detect, respond to and recover from cyber-events. Even something as apparently simple as a return to operation timeline may vary significantly among different systems and events. Accordingly, if the Agencies determine to adopt new cybersecurity guidelines, we strongly advise against implementation of requirements that would handcuff institutions to standards that prevent them from making appropriate risk judgments relevant to their specific institutions, products, systems and circumstances.

C. The Agencies Should Rely on the Existing FSOC Process to Designate Systemically Important Financial Market Utilities

The ANPR contemplates two tiers of heightened cybersecurity standards. The first tier would apply to all covered entities. A second tier, which would impose another level of additional, more stringent standards, would apply to sector-critical systems. The ANPR's formulation of what might constitute a sector-critical system, however, is overly broad and ambiguous and, we respectfully believe, not appropriate for the purpose of imposing such heightened requirements.

Section IV of the ANPR states that the Agencies are considering applying heightened standards to systems that "support the clearing or settlement of at least five percent of the value of transactions (on a consistent basis) in one or more of the markets for federal funds, foreign exchange, commercial paper, U.S. Government and agency securities, and corporate debt and equity securities[.]" See 81 Fed. Reg. at 74,319. This proposed test is problematic for several reasons.

First, the proposed definition is dependent on how each of the identified markets is defined, so that an institution may determine whether it is involved in the clearing or settlement of at least five percent of the transactions in any such market. However, it is unlikely that individual institutions will have the visibility or information available to determine the overall value of transactions in a market, which would make it difficult, if not impossible, for the institution to determine whether it meets the

applicable test. Thus, in order for the proposed test to be viable, there would need to be a clear identification of the agencies or organizations that will be responsible for gathering all relevant information about each market, a transparent method for calculating whether individual institutions meet the five percent test over designated periods of time, and the existence of mechanisms to ensure that the test is applied on a consistent basis across the applicable sector.

Further, while the test articulated in Section IV of the ANPR focuses on systems that support clearing and settlement, the language in Section VI of the ANPR suggests that, at least for recovery time standards, security-critical systems "could go beyond core clearing and settlement organizations . . . to include other large, interconnected financial systems where a cyber-attack or disruption also could have a significant impact on the U.S. financial sector." Id. at 74,325. This language introduces further confusion about what institutions and systems would, or should, be subject to the higher standards.

If financial payments, securities and financial transactions systems and the financial institutions that participate in those systems are to be subject to heightened cybersecurity mandates, the industry needs unambiguous guidance as to what systems are covered. In this regard, a clearly defined, risk-based standard to determine whether a system is a sector-critical system, based on the risks that a compromise of such a system would have on the U.S. financial sector as a whole already exists. Specifically, under the Dodd-Frank Act, the Financial Stability Oversight Council ("FSOC") has adopted standards and a formal process to designate SIFMUs. In making its determinations, FSOC assesses whether a financial market utility ("FMU") (an entity that manages or operates a multilateral system for the purpose of transferring, clearing, or settling payments, securities, or other financial transactions among financial institutions or between financial institutions and such entity) is, or likely will become systemically important, considering such factors as an entity's role in clearance and settlement.[2] In short, the determination by FSOC that an entity should be designated as a SIFMU indicates that the entity has a significant role in the overall U.S. financial sector such that the entity's failure would pose a significant risk to the overall economy. That is precisely the standard that should govern whether enhanced cybersecurity standards should apply to a payments, securities or financial transaction system. There is no need to create a new standard or process in this regard because the question of systemic significance goes to the impact from interruption or compromise of service of such an FMU, not the cause of such interruption or compromise. Indeed, if the outage of an FMU would have systemic implications, it is appropriate to ask the FMU to consider all potential risks of such an outage, both natural and man-made; but if an institution is not a SIFMU, it would not be appropriate to impose on that entity new heightened standards to address only cybersecurity risks. In this regard, existing agency guidance already provides cybersecurity standards for institutions that participate in the ACH system.

Moreover, leveraging the FSOC designation process will leave no doubt as to what entities are covered as "systemically important," and in this context, would be subject to heightened cyber-security standards. The entities that operate SIFMUs would have unambiguous obligations, while participants in the systems provided by such SIFMUs would be able to make individualized risk judgments as to their cybersecurity exposures related to the designated entities.

---

[2] *See* 12 C.F.R. Part 234.

D. Any New Third-Party Oversight Requirements Should Be Implemented by the Agencies Themselves

The ANPR seeks comments on whether to apply enhanced cybersecurity standards directly to third-party vendors, or indirectly by requiring covered entities to impose such standards on their service providers. As discussed in Part II.A of these comments, NACHA believes that additional analysis and assessment is needed to determine whether enhanced cybersecurity standards are necessary as a preliminary matter. We believe this is true with respect to imposing standards on third-party service providers as well.

If, after conducting a more detailed gap analysis the Agencies determine that cybersecurity standards should be imposed on service providers, NACHA agrees with other commenters that such standards should be applied directly to such third parties where the Agencies have the relevant authority, rather than adding to the existing burden of covered entities to manage and enforce such standards with respect to service providers. The Agencies are much better positioned to oversee the cybersecurity of such entities on a consolidated basis than could the hundreds or even thousands of institutions that use the services of such a provider. Indeed, a recurring feature of negotiations between financial institutions and providers is the concern among providers that they not be subject to repetitive but often inconsistent demands from multiple financial institution clients stemming from the same underlying regulatory mandate.

Finally, only the third-party service providers that actually perform outsourced servicing of critical features of a systemically important service should be covered by such heightened standards. While further clarification is necessary, presumably the Agencies already directly examine such entities under the existing FFIEC examination program.

* * * * *

NACHA appreciates the opportunity to provide comments on the Proposed Rule. If you have any questions regarding our comments, please do not hesitate to call me at (703) 561-3927, or our counsel at Sidley Austin LLP in this matter, David E. Teitelbaum, at (202) 736-8683.

Sincerely,

Jane Larimer
EVP ACH Network Administration
General Counsel

cc: David E. Teitelbaum, Esq.