January 12, 2017

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

Office of the Comptroller of the Currency
400 7th Street, SW
Suite 3E-218, Mail Stop 9W-11
Washington, D.C. 20219

Robert E. Feldman, Executive Secretary
Federal Deposit Insurance Corporation
550 17th Street, NW
Washington, D.C. 20429

Re: Enhanced Cyber Risk Management Standards; Docket ID OCC-2016-0016; RIN 1557-AE06; Docket No. R-1550; RIN 7100-AE 61; RIN 30640-AE45

This letter is submitted on behalf of the Consumer Data Industry Association ("CDIA"). The CDIA is an international trade association with over 140 corporate members that educates policymakers, consumers, and others on the benefits of using consumer data responsibly. CDIA members provide businesses with the information and analytical tools necessary to manage risk and protect consumers. CDIA member products are used in more than nine billion transactions each year and expand consumers' access to financial services in a manner that is innovative and focused on their needs.

On October 26, 2016, the Board of Governors of the Federal Reserve System ("Federal Reserve"), the Office of the Comptroller of the Currency ("OCC"), and the Federal Deposit Insurance Corporation ("FDIC") (collectively, the "Agencies") published a joint advanced notice of proposed rulemaking regarding enhanced cyber risk management standards (the "ANPR").[1] The ANPR invites comment on a wide range of proposals that would require very significant efforts from financial institutions and their service providers to implement new cybersecurity processes and manage these processes on an ongoing basis.

81 Fed. Reg. 74315 (Oct. 26, 2016).

The CDIA writes to emphasize that its members already are subject to and comply with several robust cybersecurity standards, including federal laws such as the Gramm-Leach-Bliley Act ("GLBA") and the Fair Credit Reporting Act ("FCRA") and other frameworks such as the Payment Card Industry Data Security Standard ("PCI DSS") and National Institute of Standards and Technology ("NIST") Cybersecurity Framework. Adding yet another layer of cyber risk management requirements on CDIA members would impose substantial compliance burdens without meaningfully increasing the security of financial information and create a greater likelihood that inconsistent and overlapping regulations inadvertently lead to the compromise of sensitive customer information. For these reasons, we urge the Agencies to reconsider the broad proposals in the ANPR and instead identify more targeted areas in need of cyber risk guidance and implement such guidance in the context of existing cybersecurity frameworks.

CDIA Members Already Comply with Robust Cybersecurity Standards.

The ANPR introduces a number of proposals that would impose enhanced cyber risk standards on the largest and most interconnected entities under the Agencies' supervision as well as on the services that these entities receive from third parties.[2] Before analyzing these proposals, the ANPR summarizes several cybersecurity standards that are in effect today, such as the NIST Cybersecurity Framework.[3]

However, the ANPR does not analyze all of the numerous and substantial cybersecurity frameworks that apply to financial institutions and consumer reporting agencies ("CRAs"). CDIA members already are obligated to comply with requirements in these frameworks that are designed to provide robust protection for customer data. These existing frameworks address many of the Agencies' cyber risk concerns, by, for example, requiring CDIA members to develop written information security programs, to regularly monitor and test such programs, and to ensure their service providers safeguard the information. These existing frameworks combine to form a robust and comprehensive set of cyber standards that well protect the data collected, maintained, and transmitted by CDIA members. We have catalogued these frameworks below.

Gramm-Leach-Bliley Act & Safeguards Rule

CDIA members are subject to the GLBA's information security requirements and its implementing rule regarding Standards for Safeguarding Customer Information (the "Safeguards Rule") promulgated by the Federal Trade Commission ("FTC").[4] The Safeguards

[2] *Id.* at 74316.

[3] *Id.* at 74316-18.

[4] 15 U.S.C. § 6801; 16 C.F.R. pt. 314. The Safeguards Rule applies to financial institutions within the FTC's jurisdiction. The Agencies have promulgated a substantially similar

Rule imposes specific standards designed to (1) ensure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of such records; and (3) protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any consumer.[5]

The Safeguards Rule requires financial institutions to "develop, implement, and maintain a comprehensive information security program" that includes appropriate administrative, technical and physical safeguards to achieve these objectives.[6] This program is required to be tailored to the institution's size and complexity, the nature and scope of its activities, and the sensitivity of any customer information at issue.[7] Accordingly, financial institutions that are large or complex are already required to implement more robust cybersecurity procedures.

In addition, the institutions must designate an employee to coordinate the program; identify reasonably foreseeable risks to the security of the information and assess the sufficiency of safeguards; and design, implement, and regularly test safeguards to protect against such risks.[8] Finally, the Safeguards Rule obligates financial institutions to oversee their service providers' cybersecurity practices, both by taking reasonable steps to ensure the institutions only deal with service providers that employ strong security practices, and by entering into contracts with the providers that require them to implement appropriate safeguards.[9]

Other FTC Standards

CDIA members are also subject to jurisdiction over cybersecurity matters asserted by the FTC under Section Five of the FTC Act.[10] Pursuant to this section, the FTC is empowered to

information security rule that applies to the financial institutions under their supervision. *See* Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. pt. 30, App. B (interagency guidelines as promulgated by the OCC); 12 C.F.R. Part 208, App. D-2 (as promulgated by the Federal Reserve); 12 C.F.R. pt. 364, App. B (as promulgated by the FDIC) .

5 15 U.S.C. § 6801(b); 16 C.F.R. § 314.4(b).

6 16 C.F.R. § 314.3(a).

7 *See id.*

8 16 C.F.R. § 314..4.

9 16 C.F.R. § 314.4(d).

10 15 U.S.C. § 45.

take action against any company within its jurisdiction that employs cybersecurity practices that are "unfair or deceptive."[11]

The FTC requires that companies employ safeguards for data that are "reasonable in light of the sensitivity and volume of consumer information it holds, the size and complexity of its data operations, and the cost of available tools to improve security and reduce vulnerabilities."[12] While specific cybersecurity requirements under Section 5 are not codified, the FTC has issued detailed guidance that explains what it considers to be reasonable cybersecurity safeguards. These include, among others, practices such as encryption, use of firewalls, use of breach detection systems, maintaining physical security of objects that contain sensitive information, and training employees to protect such information.[13]

Fair Credit Reporting Act

CDIA members also are required by the FCRA to protect consumer data.[14] Pursuant to the FCRA, CRAs must ensure that consumer report information is shared only with persons who have a "permissible purpose" to obtain the information, such as to assess the consumer's creditworthiness or eligibility for insurance.[15] This form of access control helps to prevent the broad-based dissemination of sensitive customer information. A CRA also has an obligation to take reasonable steps to ensure that the accuracy of consumer report information in its possession has not been compromised.[16] Moreover, pursuant to the FCRA and the FTC's implementing rule regarding the Disposal of Consumer Report Information and Records ("Disposal Rule"), CDIA members are subject to detailed requirements about how they dispose of consumer report information.[17]

Payment Card Industry Data Security Standard

CDIA members may be required to comply with the PCI DSS due to their payment and/or data storage practices. The PCI DSS is a set of cybersecurity requirements that are

[11] *See id.; see also* Cong. Res. Serv., The Federal Trade Commission's Regulation of Data Security Under Its Unfair or Deceptive Acts or Practices (UDAP) Authority (Sept. 11, 2014), https://fas.org/sgp/crs/misc/R43723.pdf.

[12] Fed. Trade Comm'n, Data Security (accessed Dec. 15, 2016), https://www.ftc.gov/datasecurity.

[13] *See, e.g.,* Fed. Trade Comm'n, Protecting Personal Information: A Guide for Business (Oct. 2016), https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business.

[14] 15 U.S.C. § 1681 *et seq.*

[15] 15 U.S.C. § 1681b.

[16] 15 U.S.C. § 1681e.

[17] 15 U.S.C. § 1681w; 16 C.F.R. pt. 682.

mandatory for all organizations that store, process, and transmit sensitive payment card information of the major credit card associations.[18] The standard requires CDIA members to take a number of specific steps to ensure the security of certain data. For example, the PCI DSS requires members to install and maintain firewalls, encrypt the transmission of cardholder data, protect against malware and implement and update anti-virus programs, restrict both digital and physical access to cardholder data, regularly test security systems and processes, and maintain a detailed information security policy for all personnel.[19] The standard imposes further detailed and specific technical requirements for the protection of cardholder data, such as a restriction on service providers' storage of personal identification or card verification numbers after card authorization.[20] In addition, the standard requires a service provider to ensure that any third parties with whom it shares data also comply with the PCI DSS.[21]

NIST Cybersecurity Framework

NIST's Cybersecurity Framework is a "risk-based approach to managing cybersecurity risk."'[22] Many CDIA members seek to comply with the NIST Framework. The core of this framework consists of five functions central to effective cybersecurity: identify, protect, detect, respond, and recover. These functions are then broken down into 22 categories and 98 subcategories.[23] While the framework does not prescribe detailed technical requirements or specifications, the functions map to specific steps institutions can take to satisfy the standard, and these functions constitute a "compilation of industry-leading cybersecurity practices" that, when followed, help to solidify an organization's cybersecurity.[24]

* * *

In sum, CDIA members are already subject to robust cybersecurity frameworks and devote significant resources to ensuring the data in their possession is protected. These

[18] Payment Card Industry Security Standards Council, *Requirements and Security Assessment Procedures, Version 3.2* (Apr. 2016).

[19] *Id.* at 5.

[20] *See, e.g., id.* at 38-39.

[21] *Id.* at 12.

[22] Nat'l Inst. of Standards & Tech., *Framework for Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2014) at 4 [hereinafter *NIST Framework].* The NIST framework is issued pursuant to Executive Order 13636 (Feb. 12, 2013).

[23] *NIST Framework* at 4-5; *see also* Mark Francis, Int'l Ass. of Privacy Professionals, The Future of the NIST Cybersecurity Framework (Apr. 25, 2016), https://iapp.org/news/aAhe-future-of-the-nist-cybersecurity-framework/.

[24] Fed. Trade Comm'n., The NIST Cybersecurity Framework and the FTC (Aug. 31, 2016), https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc.

frameworks are effective and flexible in their application, allowing companies to protect against and respond to threats in a manner appropriate to their size, complexity, and the sensitivity of the data they collect. For these reasons, we do not believe that new standards in a framework applicable to the largest and more interconnected financial institutions and their service providers are needed to ensure the security of the financial information.

We appreciate the opportunity to comment on the Agencies' ANPR, and we hope the Agencies will find these comments useful as it considers its next steps.

Sincerely,

Eric J. Ellman
Interim President and CEO