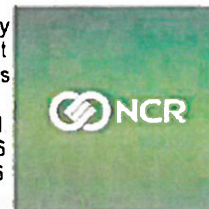


Justin Clay
Vice President
Global Government Relations

3097 Satellite Blvd
Duluth, GA 30096
T: 770.689.2286
www.ncr.com



February 17, 2017

Robert deV. Frierson
Secretary
Board of Governors of the Federal Reserve System

Legislative and Regulatory Activities Division
Office of the Comptroller of the Currency

Robert E. Feldman
Executive Secretary
Federal Deposit Insurance Corporation

**Re: Advance Notice of Proposed Rulemaking, Enhanced Cyber Risk
Management Standards
Federal Reserve: Docket ID R-1550
OCC: Docket ID OCC-2016-0016
FDIC: RIN #3064-AE45**

Dear Sirs:

Thank you for the opportunity to comment on the proposed enhanced cyber risk management standards jointly issued by the Federal Reserve Board, the Office of the Comptroller of the Currency (OCC), and the Federal Deposit Insurance Corporation (FDIC).

Introduction to NCR:

NCR is a world leader in consumer transaction technologies that make the everyday easier for consumers and businesses. We have a proud 132-year heritage of innovation in financial services, payments, and consumer technologies. With our extensive portfolio of software, hardware, services and Omni-channel platforms, NCR today is the leading global provider of ATMs, hospitality solutions and retail self-check-out systems.

We are deeply committed to building strong defenses against malicious cyber activity. We build standards-based security features into every solution we offer, starting at the outset of the design phase, and continuing at every stage in the development process. We work with our customers on an on-going basis to ensure that security is strong and agile and incorporates the most recent innovations.

Comments:

Our comments will focus primarily on the scope of application of the proposed standards. Our views are laid out below in responses to questions #5 and #1.

5. What are the advantages and disadvantages of applying the standards directly to service providers to covered entities? What challenges would such an approach pose?

Maintaining the existing regulatory framework of applying standards directly to regulated financial institutions would best enable the regulating agencies to achieve their goal of enhancing protections of the U.S. financial system from malicious cyber-attacks. Creating a parallel regulatory structure for service providers would create a number of new challenges without offering significant additional benefits.

Potential challenges that would be created by a departure from the existing regulatory framework include the following. First, defining "service providers" to whom enhanced cybersecurity standards would apply would be difficult and would create uncertainty in the marketplace and difficulty in application. For example, would standards apply to service providers of a certain size (revenues, earnings, number of financial institutions served), or would they apply to service providers who work with financial institutions of a certain size? Would enhanced standards apply only to technology providers, or would they apply to any service provider that could potentially impact cybersecurity? One could make a case that a very broad range of service providers could impact cybersecurity, ranging from data processors to custodial crews.

Second, the client relationships of service providers are constantly changing. A company that provides services to several large financial institutions this year may find itself providing services to none next year. Maintaining an accurate inventory of service providers to whom regulatory standards apply would be burdensome and time-consuming for the regulatory agencies. Financial institutions are in a much better position to manage their service provider relationships.

Third, expanding the universe of entities to whom regulatory standards apply directly is likely to place a strain on agency resources that are already stretched thin. FFIEC examiners and agency compliance personnel have limited resources, and the list of service providers that could potentially become covered entities is likely to be lengthy.

Fourth, providers of technology services to financial institutions generally also serve other industries with other regulatory regimes. Applying financial institution standards directly to service providers will potentially expose those service providers to conflicting standards and requirements, resulting in increased overhead and cost to those service providers to address and manage these conflicts – and taking away resources that may otherwise be applied to innovation. This potential conflict is more neatly avoided when requirements are extended to service providers through their contractual relationships with their financial institution customers.

For all of these reasons, we believe that the objective of improving cyber preparedness would be better served by maintaining the existing framework of applying standards to financial institutions themselves and allowing the financial institutions to ensure the compliance of their service providers. Establishing a new, expanded regulatory and compliance framework would likely be unnecessarily disruptive at a time when the entire industry is working diligently to adapt to the new regulatory structures of the last several years.

1. How should the agencies consider broadening or narrowing the scope of entities to which the proposed standards would apply? What, if any, alternative size thresholds or measures of risk to the safety and soundness of the financial sector and the U.S. economy should the agencies consider in determining the scope of application of the standards? For example, should "covered entity" be defined according to the number of connections an entity (including its service providers) has to other entities in the financial sector, rather than asset size? If so, how should the agencies define "connections" for this purpose?

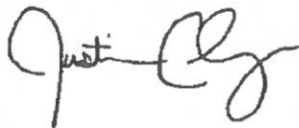
A financial institution's asset size is a satisfactory measure for determining the threshold for applying enhanced cyber risk management standards. For the reasons stated below, utilizing an alternative measure, such as number of connections, would be difficult to implement and offer little additional value.

Attempting to measure a financial institution's connections to other entities is likely to be a burdensome process that may draw resources away from more important and valuable undertakings. First, defining the term connections (IT connections, contractual connections, financial connections, human connections, etc.) will not be a simple task in and of itself. In addition, identifying and tallying those connections, and then keeping the tally current, will be a resource-intensive process, especially for large institutions. In general, it is fair to assume that the more assets a financial institution has, the more complex its business, and hence, the more connections it is likely to have, and vice versa. As such, asset size is a satisfactory measure of an institution's importance to the overall financial system, and developing an alternative measurement is not likely to add significant value.

Conclusion:

Thank you for the opportunity to share our views on these important issues. We share your commitment to ensuring that our financial system is protected from cyber intrusions, and we are constantly working to strengthen cyber defenses throughout the industry. We look forward to working with you in this area, and we would be happy to answer any questions you might have.

Sincerely,

A handwritten signature in black ink, appearing to read "Justin Cluz". The signature is fluid and cursive, with the first name "Justin" written in a larger, more prominent script than the last name "Cluz".

Vice President
Global Government Relations