INDEPENDENT COMMUNITY BANKERS of AMERICA®

REBECA ROMERO RAINEY
Chairman
R. SCOTT HEITKAMP
Chairman-Elect
TIMOTHY K. ZIMMERMAN
Vice Chairman
DEREK B. WILLIAMS
Treasurer
J. MICHAEL ELLENBURG
Secretary
JACK A. HARTINGS
Immediate Past Chairman
CAMDEN R. FINE
President and CEO

February 14, 2017
Via electronic submission to:

Robert de V. Frierson, Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Ave, NW
Washington, D.C. 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, D.C. 20219
Regs.comments@occ.treas.gov

Robert E. Feldman, Executive Secretary
Attention: Comments
Federal Deposit Insurance Corporation
550 17th Street NW
Washington, D.C. 20429
comments@fdic.gov

Re: Joint advance notice of proposed rulemaking, "Enhanced Cyber Risk Management Standards." *Board*, Docket No. R-1550; RIN 7100-AE-61; *OCC*, Docket ID OCC-2016-0016; *FDIC*, RIN 3064-AE45.

Dear Mesdames and Sirs:

I. Introduction

The Independent Community Bankers of America (ICBA)[1] appreciates the opportunity to comment on the joint advance notice of proposed rulemaking entitled,

[1] **The Independent Community Bankers of America®, the nation's voice for** nearly 6,000 community banks of all sizes and charter types, is dedicated exclusively to representing the interests of the community banking industry and its membership through effective advocacy, best-in-class education and high-quality products and services.

With over 50,000 locations nationwide, community banks employ 700,000 Americans, hold $4.0 trillion in assets, $3.2 trillion in deposits, and $2.7 trillion in loans to consumers, small businesses, and the agricultural community. For more information, **visit ICBA's website at www.icba.org.**

"Enhanced Cyber Risk Management Standards," ("ANPR") issued by the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corporation ("Agencies").

II. General Comments

Cybersecurity is important for all sectors, including the financial services sector. The financial services industry and community banks, including their boards, management and employees recognize and take seriously their responsibility to protect customer data and personal information. Beyond existing regulatory and statutory requirements specific to protection of customer data and cyber security, the community bank business model is founded on customer trust and service. A failure to safeguard customer personal information, as well as to safeguard the institution as a whole, would have a significantly negative impact on any community bank. Compromised customers of such institutions have multiple choices in the financial marketplace. Beyond any legal or regulatory requirements, cybersecurity is a business imperative for community banks in the digital marketplace, which community banks take very seriously.

Cybersecurity risks are constantly evolving. Community banks are cognizant of these risks and invest in security controls to protect their individual data and critical systems. In addition, public-private partnerships and organizations that support the financial sector are working diligently and collaboratively to mitigate some of these risks through enhanced information sharing through the Financial Services Information Sharing and Analysis Center (FS-ISAC) and other avenues, such as through the Department of Homeland Security's Automated Information System.

To provide some background, community banks protect institutional and customer data, by employing a multitude of voluntary cybersecurity frameworks, tools and assessments based on their risk tolerance, including, but not limited to, the National Institute of Standards and Technology *Cybersecurity Framework* (*"NIST CSF"*),[2] Control Objectives for Information and Related Technology ("COBIT"), the SANS CIC Critical Security Controls, and the Federal Financial Institutions Examination Council ("FFIEC") *Cybersecurity Assessment Tool ("CAT")*. This is, of course, in addition to the guidance outlined in the *FFIEC Information Technology Examination Handbook* booklets *("IT Handbook")*,[3] the standard by which banks are examined on information technology and security. It is not uncommon for community banks to employ parts, or multiple parts, of various voluntary frameworks, tools and assessments to provide a tailored cybersecurity program for their institution, based on the banks' risk, size and scope. **It is therefore critical that the Agencies recognize this approach to cybersecurity and neither require nor penalize any community bank that wishes to employ a part or parts of various voluntary frameworks, tools and assessments for cybersecurity protections**

---

[2] National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity: Version 1.0.* 12 February 2014. Available at: https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[3] FFIEC *IT Handbook* booklets can be found online at: http://ithandbook.ffiec.gov/.

and further, not require the use of one framework, tool or assessment over another. At the same time, it is important for regulators to recognize that not all institutions have the vast resources available to map each and every framework to the regulatory requirements set forth in the *IT Handbook*. Mappings, such as those found in the *CAT* to both the *NIST CSF* and the *IT Handbook*, are helpful for community bank cybersecurity professionals. ICBA encourages the Agencies to update these mappings as the *IT Handbook* is updated and following any update to the *NIST CSF*.

The ANPR is aimed at a growth in technology dependence within the financial services sector. The "interconnectedness of the U.S. financial system" means that a "cyber incident or failure at one interconnected entity may not only impact the safety and soundness of the entity, but also other financial entities, with potentially systemic consequences." As drafted, the enhanced cybersecurity standards in the ANPR would apply to certain entities, on an enterprise-wide basis, with total consolidated assets of $50 billion or more ("covered entities"),[4] including the systems of covered entities that are critical to the financial sector.[5] Each agency would apply these standards subject to their jurisdiction.[6] The Agencies are also considering broadening or narrowing the scope of entities to which the enhanced standards apply.[7] ICBA strongly believes that the ANPR should not intentionally or unintentionally trickle down, through regulation or best practice, to small financial institutions, such as community banks, that do not have the interconnectedness of large multinational entities.

As additional cybersecurity regulations are proposed for the financial services sector, ICBA urges the Agencies not to layer additional frameworks on top of existing regulatory guidance and requirements. Any new or proposed frameworks or guidance should be incorporated into, or consistent (harmonized) with, existing frameworks or guidance. By adding new frameworks or guidance without incorporating or harmonizing them with existing standards, the Agencies risk "framework fatigue" among the financial sector as resources are allocated to reconciling the differing approaches rather than combating cyber threats.

Although ICBA believes that adding another cybersecurity requirement to the financial sector is not the solution to efficiently address the Agencies' goals,[8] if any such initiative is developed, we believe it is appropriately targeted to the nation's largest, most interconnected firms.[9] It is critically important that enhanced standards not be applied to our nation's community banks as they are subject to existing guidance, standards and

---

[4] *Federal Register*. Vol. 81, No. 207. 26 October 2016. 74318.
[5] Ibid. 74319.
[6] A detailed description of the types of entities this regulation might apply, separated by agency jurisdiction, is available at Id., 74318.
[7] See Id., "Questions on the Scope of the Application," Question 1. 74318.
[8] The purpose of enhanced standards, as stated in the ANPR, is "to increase covered entities' operational resilience and reduce the potential impact on the financial system in the event of a failure, cyber-attack, or the failure to implement appropriate cyber risk management." Id., 74316.
[9] ICBA believes a scope of both a definitive asset-size threshold alongside a risk-based and interconnectedness measurement is appropriate.

examinations already, which address each institution's operational resiliency and are reflective of each institution's risk, scope and complexity. Additionally, community banks, by and large, do not have the sheer number of interconnections as systemically significant financial intuitions.

III. Expanding Applicability to Smaller Banking Organizations

The Agencies are seeking comment on the criteria to evaluate whether a financial entity that would not otherwise be subject to the enhanced standards, such as a smaller banking organization, should be subject to sector-critical standards.[10] ICBA strongly supports an asset-size threshold with an additional risk and interconnectedness assessment to sufficiently evaluate whether a financial entity should be subject to enhanced standards. Such criteria would delineate institutions that are critical and the most interconnected to the financial sector.

Applying both a definitive asset-size threshold with a risk and interconnectedness measurement ensures that the enhanced standards apply to those firms with sufficient market share in one or more critical financial markets to present systemic risk in the instance of a cyber event. Additionally, such an assessment utilizes risk-based principals to properly account for the nature of the risk flowing through the interconnections of large multi-national entities.

As the Agencies are aware, and acknowledge in this ANPR, community banks are regulated and examined by existing rules, regulations and guidance on cybersecurity standards, including, but not limited to, those requirements outlined in the *IT Handbook* and accompanying examination materials. Community banks are already appropriately examined and supervised based on operational resiliency, scope, risk and complexity with regard to cybersecurity.

These examinations should prove sufficient for community bank cybersecurity protections and should provide information necessary to determine the application of enhanced standards to the nation's most interconnected institutions. Requiring community banks to expend additional resources to identify whether the enhanced standards apply will impose a disproportionate burden on community banks, diverting resources away from cybersecurity protections and customer service to regulatory compliance. Unlike smaller banking organizations, significantly important banks have dedicated legal, compliance and information security/technology staff to absorb and respond to additional regulatory requirements and their associated costs.

Additionally, Congress and the Agencies have consistently differentiated between small banking institutions and large, interconnected firms. There are important and significant differences between community banks and significantly important institutions and it is critical for the Agencies to recognize this difference. Smaller banking organizations do not hold nearly as many interconnections, either domestically or

[10] Id., 74320.

internationally, as systematically important institutions nor do community banks operate significantly or systemically important sector systems. Combining an asset-size threshold, as well as a risk-based and interconnectedness measurement, will assist the Agencies in identifying complex institutions that pose systemic risk to the financial sector and the U.S. economy in the event of a failure, cyberattack, or the failure to implement appropriate cyber risk.[11]

IV. Scope of Application

The Agencies are also seeking comment on whether any alternative size thresholds or measures of risk should be considered in determining the scope of application of the enhanced standards. It is essential that the Agencies outline specific and clear criteria to determine whether systems or entities fall under these categories and make a delineating determination of these criteria.

ICBA strongly supports the definitive asset-size threshold application in the ANPR; however, this alone is not sufficient to measure the risk to the safety and soundness of the financial sector and the U.S. economy. Applying both a definitive asset-size threshold with a risk-based and interconnectedness measurement ensures that the enhanced standards apply to those firms with sufficient market share in one or more critical financial markets to present systemic risk in the instance of a significant cyber event as well as utilizes risk-based principals to properly account for the nature of the risk flowing through the interconnections of large multi-national entities.

Applying the regulation on risk or interconnectedness alone would require all financial institutions, including community banks, to undertake an additional risk assessment to determine whether the institution is subject to enhanced standards. ICBA contends that a clear distinction of applicability for enhanced standards would balance the costs of imposing such standards to the financial sector with the potential benefits to the financial system.[12]

V. External Dependency Management

The Agencies are considering management standards, organized into five categories, which seek to enhance cyber risk management standards for covered entities to increase the entities' operational resilience and reduce the potential impact on the financial system as a result of, for example, a cyberattack at a firm or the failure to implement appropriate cyber risk management.[13] Category 4 – *"External Dependencies,"* refers to an entity's relationships with outside vendors, suppliers, customers, as well as

---

[11] See Footnote 8.

[12] For example, the Federal Reserve considers a number of factors including the size of the institution, interconnectedness, lack of readily available substitutes for the services they provide, complexity and global activities to designate a firm as a systemically important financial institution (SIFI). See *Supervision and Regulation Letter, SR 12-17*. 17 December 2012. Available at: https://www.federalreserve.gov/bankinforeg/srletters/sr1217.htm

[13] *Federal Register*. Vol. 81, No. 207. 26 October 2016. 74320.

other external organizations. The term also includes service providers the entity depends on to deliver services as well as the information flows and interconnections between the entity and those external parties. In addition, the external dependency management category includes the management of interconnection risk associated with non-critical external parties that maintain trusted connections to important systems.[14] As part of an external dependency management strategy, the Agencies are considering a requirement that covered entities establish effective policies, plans, and procedures to identify and manage real-time cyber risks associated with external dependencies, particularly those connected to or supporting sector-critical systems and operations throughout their lifespans.

The Agencies are considering that covered entities have a current, accurate, and complete awareness of all external dependencies. The ANPR also requires that covered entities ensure policies, standards and procedures for external dependency management throughout the lifespan of the relationship are established and regularly updated. Elements of this management include the due diligence process, contracting and subcontracting, onboarding, ongoing monitoring, change management and off-boarding. Additionally, a covered entity must ensure that appropriate compliance mechanisms and appropriate metrics are in place to measure effectiveness in reducing cyber risks associated with external dependencies.

The ANPR seeks comments on whether the comprehensiveness and effectiveness of the enhanced standards for external dependency management is achieving the Agencies' objective of increasing the resilience of covered entities, third-party service providers to covered entities, and the financial sector.[15]

Community banks that hold accounts at, are customers of, or utilize the services of covered entities may be considered a "customer" under this definition. For example, services that community banks may contract with significantly important institutions include, but are not limited to, Treasury management services, global trade services, credit services such as Federal fund lines for liquidity, letters of credit to support customer trade activity or lending activity, interest rate management, brokerage/investment advisory services, international banking and foreign exchange, institutional custody services, securities, and wires. Community banks may be considered a "customer" in this category and therefore subject to additional oversight by the covered entity. These types of services offered to, and used by, community banks would be considered sector-critical according the *Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System.*[16] ICBA strongly recommends that the Agencies exempt community banks from the covered entity's external dependencies requirements by excluding from the definition of customer, an entity that is currently regulated and examined by a prudential regulator.

---

[14] 74323.

[15] Ibid. Question 17, 74324.

[16] *Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System*. 8 April 2003. Available at https://www.federalreserve.gov/boarddocs/srletters/2003/SR0309a1.pdf.

External Dependency Management is already in existence for community banks and is called risk management for third-party relationships. Community banks must assess and manage the risks associated with all business arrangements made with another entity. They comply with and are examined for their due diligence in assessing and managing these risks associated with all third-party relationships. Because the Agencies already examine community banks' effectiveness in reducing the cyber risks associated with their third-party relationships, requiring covered entities to do the same is duplicitous and is both extremely and overly burdensome. Taken further, external dependency management by a covered entity over community banks as customers is unnecessary, as noted above, given they are already comprehensively examined by the Agencies. Covered entities should be permitted to rely on the regulators to adequately and effectively examine the external dependencies between two federally supervised entities - community banks and covered entities. Additionally, covered entities become the enforcers of the Agencies' regulatory requirements.

VI. Incident Response, Cyber Resilience, and Situational Awareness

The ANPR's consideration of requirements for recovery plans and preservation of critical records mentioned in Category 5—*"Incident Response, Cyber Resilience, and Situational Awareness,"* is similar to a private-sector initiative - Sheltered Harbor - designed to improve the financial services sector's resilience and enhance protections for financial institutions' customer accounts and data. Recognizing the importance of all financial institutions being on a level playing field in this crucial area, ICBA is pleased to collaborate with other stakeholders to make this initiative a successful reality for financial services firms.

ICBA urges the Agencies to encourage broad industry participation in this initiative and to avoid any regulatory activity that could impede efforts to achieve broad adoption. A secure, ongoing public-private sector collaboration could offer a venue for sharing Sheltered Harbor details and confidentially addressing regulatory questions while protecting Sheltered Harbor's intellectual property.

VII. Closing

Again, ICBA appreciates the opportunity to comment on this ANPR. Please do not hesitate to contact me at Jeremy.Dalpiaz@icba.org or (202) 659-8111.

Respectfully Submitted,

/s/
Jeremy J. Dalpiaz
Assistant Vice President
Cyber Security and Data Security Policy