CDFR Group Comment Letter to "Enhanced Cyber Risk Management Standards"
Docket ID OCC-2016-0016

February 17, 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

The undersigned, a group of companies in the financial services technology industry that helps consumers and small businesses manage their financial needs, which we call the Consumer Financial Data Rights Group ("CFDR Group") submits the following comments in response to 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") (together, "Agencies") proposed rule entitled, Enhanced Cyber Risk Management Standards ("Enhanced Standards" or "ANPR").

As a group, we appreciate the opportunity to offer comments on the ANPR and support the Agencies' efforts to strengthen cybersecurity in the financial services industry. The financial services technology industry, like many other industries, is built fundamentally on information. Advances in digital connectivity and analytics mean that the information on which the financial services industry is built increasingly and, in some instances, exclusively resides on digital devices that are either always connected to or can be accessed by other digital devices. In that context, we agree that financial services providers, like all information businesses, should invest in technology and infrastructure to protect themselves and their customers from cyber threats.

With that said, we believe that cyber risks vary by institution and by function within an institution and that they are manageable through a variety of means, including the design and construction of information systems. In the design and construction of information systems, cyber security is simply one concern among many. Financial and strategic concerns also influence the choices that firms make in deciding how to design and build their information systems. And we worry that the call for greater oversight of the cyber security practices of various firms, both those that are directly supervised by the Agencies and those that are not,

could be used to increase regulatory and compliance burdens for third parties and to use cybersecurity concerns to justify restricting access to consumer data held by financial institutions.[1]

As a group we have one overriding concern with the Enhanced Standards. We believe that the Enhanced Standards fail to account for the differences among both regulated institutions and the firms that connect to them. In our view, only a small fraction of regulated institutions and service providers to those institutions present the types of risks that the Enhanced Standards seek to address—i.e., cyber risks that threaten the stability of regulated institutions and the smooth functioning of critically important economic infrastructure such as securities clearing and bank settlement. In our view, the Enhanced Standards should account for the diversity of risk that may be presented by institutions and the activities they engage in. We note that the Agencies appear to have this concern in mind as relates to regulated institutions themselves. The ANPR makes clear that with regard to already supervised entities, the Enhanced Standards will only apply to "the largest and most interconnected entities."[2]

Unfortunately, this concern appears to have been lost in the potential application of the Enhanced Standards to entities that the Agencies do not currently regulate or supervise. According to the text of the proposal, the Enhanced Standards will apply to any third party that provides "services to depository institutions and their affiliates."[3] The undersigned worry that the broad application of the Enhanced Standards will be used to justify the refusal by covered financial institutions to connect to third parties that refuse to assume the compliance burden of becoming service providers to those institutions.[4] Indeed, the Enhanced Standards could even create criminal liability for third parties.[5]

---

[1] Bank advocates have already called for heightened regulatory requirements for nonbanks, particularly with respect to third party supervision. *See Ensuring Consistent Consumer Protection for Data Security: Major Banks vs. Alternative Payment Providers*, The Clearing House (August 2015), available at https://www.theclearinghouse.org/~/media/files/research/tchconsumer%20protection%20for%20data%20security%20august%202015%20final.pdf; *see also* Jamie Dimon, *Letter to Shareholders* at 21, available at https://www.jpmorganchase.com/corporate/investor-relations/document/ar2015-ceolettershareholders.pdf ("[I]nstead of giving a third party unlimited access to information in any bank account, we hope to build systems that allow *us* to 'push' information – and only that information agreed to by the customer – to that third party.").

[2] ANPR at 8, available at https://www.federalreserve.gov/newsevents/press/bcreg/bcreg20161019a1.pdf.

[3] ANPR at 14-15 ("As noted, the agencies are considering whether to apply the standards to third-party service providers with respect to services provided to depository institutions and their affiliates that are covered entities.").

[4] Put slightly differently, promulgation of the Enhanced Standards could be used by large financial institutions to impose a strict access taxonomy on third parties. Either third parties are customers and are permitted by the financial institution to access their systems under whatever limitations the financial institutions impose or they are service providers and must agree to subject their cyber security practices to direct supervision by the Agencies.

[5] Although the risk of criminal liability from such a taxonomy may seem farfetched, a panel of the Ninth Circuit recently relied on precisely this justification to impose liability on a third party under the Consumer Fraud and Abuse Act of 1984. *See* 18 U.S.C. § 1030; *see also Facebook, Inc. v. Power Ventures, Inc.*, 828 F.3d 1068, 1077 (9th Cir. 2016) ("[A] defendant can run afoul of the CFAA when he or she has no permission to access a computer or when such permission has been revoked explicitly. Once permission has been revoked, technological gamesmanship or the enlisting of a third party to aid in access will not excuse liability."). As information security scholars have observed, the rationale on which this justification is explicitly premised—*i.e.*, that a party which enters physical property is committing trespass—does not easily apply to systems that are connected to the internet. *See* Orin Kerr, *9th Circuit: It's a Federal Crime to Visit a Website After Being Told Not to Visit It*, THE WASHINGTON POST,

We believe that the Enhanced Standards will chill efforts on the part of entrepreneurs and developers to help consumers and small businesses make more appropriate use of the services provided by regulated financial institutions. The Enhanced Standards can be read to impose significant new costs and regulatory burdens on any institution that connects to a regulated financial institution, regardless of the nature or scope of that connection. In our view, the burden reflected in the Enhanced Standards should only fall on firms—regulated or not—that pose a true cybersecurity risk and, even then, should be aimed at ensuring that firms design their systems in such a way as to confine those threats. Simply put, every entrepreneur or developer who wants to help a consumer or small business better manage their finances and who necessarily needs access to information housed within a financial institution should not have to undertake the same type of cyber security review as, for example, SWIFT.

We also believe that the Enhanced Standards should take into account the different kinds of activities that both banks and the third parties with which they partner engage in. Every function that a bank engages in does not create the same potential for risk. The focus of the effort to enhance cybersecurity should be based on a hierarchy of risk. Activities that pose the most systemic risk such as the number and integrity of transaction records for financial markets, the integrity of debits/credits of interbank settlement, the daily calculation of assets and liabilities for leveraged institutions, and primary storage of customer account information should receive the most attention and protection. Activity like granting third parties read-only access to consumer financial account data is fundamentally less risky than securities clearing or interbank settlement. Allowing a third party to simply view data does not pose a significant risk in the event of a cyber attack because there are limits to what can be done with the data. Even activities that might otherwise seem similar—e.g., money movement—will present very different risks depending on the types of counterparties involved (e.g., bank-to-bank or person-to-person) and the size of particular transactions.

In short, we recommend that the Agencies use a risk-based framework to define the scope and application of the Enhanced Standards related to cyber security. The Enhanced Standards ultimately promulgated by the Agencies should focus on those third-party providers to covered financial institutions whose provided services and/or depth of connections to those institutions would represent a significant risk if attacked. As part of this effort to focus these new rules, the Agencies should also allow for variation by size, function and profile of regulated institutions.

As drafted, the scope of the existing proposal is overbroad in the extreme. Virtually the entire information technology industry would fall within its scope even though the vast majority of firms that connect even to significant financial institutions do not present any meaningful risk to those institutions or the stability of the financial system. Rather than broadly assert supervisory authority over an entire industry, we recommend that the Agencies identify critical functions within covered institutions and apply the Enhanced Standards to those functions, including functions maintained and supported by third parties on behalf of bank customers.

(Jul. 12, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/07/12/9th-circuit-its-a-federal-crime-to-visit-a-website-after-being-told-not-to-visit-it/?utm_term=.287876b70272 (last visited Dec. 6, 2016).

The CFDR group appreciates this opportunity to provide its perspective in response to the Agencies' proposal. Should we be able to provide any additional information, please do not hesitate to contact Steven Boms (sboms@yodlee.com) at (202) 997-0850.

Sincerely,

Affirm

Betterment

Envestnet | Yodlee

Kabbage