Yodlee 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

Envestnet Yodlee ("Yodlee") respectfully 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").

Yodlee is the leading global account aggregation platform provider. Yodlee, which is supervised by the OCC, provides consumer-permissioned account aggregation capabilities on a business-to-business basis to millions of consumers around the world, which include some of the nation's largest banks and leading financial technology companies. Yodlee's client base includes 12 of the 20 largest banks in the United States and the largest global banks in more than 20 countries. Yodlee also acts as a critical technology partner that enables the growth of the FinTech marketplace by supporting many well-known companies that are innovating within the financial services sector.

Yodlee appreciates the opportunity comment on the ANPR and supports the Agencies' efforts to strengthen cybersecurity within the country's financial system. On a general level, Yodlee agrees that firms of all kinds, including financial services providers, should invest in

technology and infrastructure to protect themselves and their customers from cyber threats. However, cyber threats vary greatly by institution and by the activities they perform, as do the potential implications on both consumers and the broader financial system of a cyber attack on a particular firm. Thus, the cybersecurity framework ultimately adopted by the Agencies should contemplate the variances in cyber risks based on the type of institution and by the activities in which the institution participates. As currently written, the ANPR fails to account for these differences. Instead, the ANPR attempts to apply an inflexible and overly broad mandate that could theoretically capture *any* institution, regardless of its size, function, or actual risk posed.

Accordingly, Yodlee respectfully recommends that the Agencies adopt and define a risk-based framework that applies the Enhanced Standards according to the level of criticalness the institution presents based on the nature and size of the institution, as well as the functions it performs.

Specific Comments

Question 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?*

The two metrics proposed (the amount of volume processed on a daily basis and the size of the balance sheet) are good proxies for the systemic risk posted by the institutions' cybersecurity efforts. However, as stated previously, the Enhanced Standards do not take into account the different levels of risk that various activities that financial institutions and their third parties engage in that may raise in the wake of a cyber attack. Indeed, every function that a financial institution or a third party service provider 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.[1] On the other hand, activities that do not pose the type of risk that the ANPR seeks to address, should be exempt from the Enhanced Standards, as the costs of implementing any requirements would not be offset by any significant benefit.[2] Because the ANPR is aimed at mitigating risks that "could

[1] *See Cybersecurity 101: A Resource Guide for Bank Executives*, Conference of Bank Supervisors (Dec. 2014), available at https://www.csbs.org/CyberSecurity/Documents/CSBS%20Cybersecurity%20101%20Resource%20Guide%20FINAL.pdf (acknowledging that financial institutions are a prime target for cyber attacks and security breaches at financial institutions could pose a "significant threat" to the nation's financial stability).

[2] ANPR, at 13. available at https://www.federalreserve.gov/newsevents/press/bcreg/bcreg20161019a1.pdf.

have a significant impact on the safety and soundness of the entity, other financial entities, and the U.S. financial sector," applying the Enhanced Standards to entities, like Yodlee, that do not engage in activities that pose this level of risk would be gratuitous.

Question 6 – *What factors are most important in determining an appropriate balance between protecting the safety and soundness of the financial sector through the possible application of the standards and the implementation burden and costs associated with implementing the standards?*

The Enhanced Standards do not take into account the different kinds of activities that both banks and the third parties with which they partner engage in that may raise significant risk in the wake of a cyber attack versus those that pose little or no risk. 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 to the financial system, to the financial institution, or to the institution's customers if attacked.

The Agencies should also recognize that all institutions that touch sensitive financial information, whether directly regulated by the Agencies, regulated as service providers to directly regulated institutions, and even institutions that simply receive financial data from consumers but are not otherwise regulated, already have an obligation to protect such data from external threats under the Gramm-Leach-Bliley Act ("GLBA").[3]

The broad scope of the ANPR also raises concerns that regulated financial institutions may rely on the Enhanced Standards as a basis for securing a competitive advantage or obtaining more bargaining power over nonbanks in the name of cybersecurity as they have historically done.[4] Regulated financial institutions may use cyber security concerns as a proxy for granting themselves the power to dictate which third parties receive data related to accounts maintained by their customers. For example, banks may claim that the Enhanced Standards provide a justification to prevent consumers from exercising their right, codified by Section 1033 of the Dodd-Frank Act, to access and to delegate to third parties access to information related to their accounts.

Accordingly, Yodlee recommends that the Agencies refrain from imposing new cybersecurity requirements that will create significant new costs, may not do much to protect banks or their customers from cyber threats, could create new barriers to competition, and could limit or deny the ability of consumers to access and use technology-powered tools that empower them to improve their financial wellbeing. Instead, the Enhanced Standards should operate as a flexible standard that can be met by a variety of cybersecurity measures that are suitable to the

[3] 15 U.S.C. 6801 *et seq.*
[4] *See* Dimon, *supra* note 5.

unique operations and structure of all potentially covered institutions that is based on the types of risk data presents.

Question 17 – *The agencies request comment on the comprehensiveness and effectiveness of the proposed standards for internal and external dependency management in achieving the agencies' objective of increasing the resilience of covered entities, third-party service providers to covered entities, and the financial sector.*

As drafted, the External Dependency Management category could significantly limit consumers' access to their own financial data and will create an enormous administrative burden. The APNR defines "external dependencies"[5] in sweeping terms. The definition captures all third parties regardless of the whether the "external dependency" poses cyber risk, or, if it does, the level of cyber risk it presents. With such a broad definition, the proposed requirements for external dependency management would require banks and service providers to banks to develop detailed descriptions of relationships with third parties regardless of the risk posed by that third party.[6] Further, Yodlee is concerned that financial institutions, in an effort to comply with such broad guidelines, would decide to limit the amount of data their customers would be permitted to access and permission to technology tools that empower them to improve their financial wellbeing.[7]

Specific requirements magnify the potential burden. For example, as drafted, the External Dependency Management category would require covered banks to "identify and periodically test alternative solutions" for third-party service providers such as Yodlee that do not provide critical infrastructure to banks or even help them service their customers. Rather, Yodlee enables third parties to provide services to customers based on information hosted by banks. As a service provider that delivers "information flows" to the covered entities, however, Yodlee would be subject to the same external dependency management requirements as retail payment systems.

Further, the ANPR presupposes that third-party service providers are not already subject to stringent regulatory oversight. With 12 of the top 20 U.S. financial institutions as its customers, Yodlee is supervised and examined by the OCC. The examination covers a wide array of topics related to cybersecurity, such as threats, risk management, third party

---

[5] The ANPR defines the term "external dependencies" as an entity's "relationships with outside vendors, suppliers, customers, utilities, and other external organizations and service providers that the entity depends on to deliver services, as well as the information flows and interconnections between the entity and those external parties." The external dependency management category also includes "the management of interconnection risks associated with non-critical external parties that maintain trusted connections to important systems." ANPR, at 33.

[6] They require institutions to (1) establish effective policies, plans, and procedures to identify and manage real-time cyber risks associated with each of their external dependencies; (2) ensure the ability to monitor in real time all of their external dependencies and trusted connections; (3) identify and periodically test alternative solutions for each external dependency; (4) continually apply and evaluate appropriate controls to reduce the cyber risk of each external dependency to the covered entities' enterprise. ANPR, at 33-35.

[7] *See* 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.").

assessments, and third party risk management. Yodlee once again suggests that not all "external dependencies" are created equal; those currently examined and supervised by prudential bank regulators logically have already implemented the governance and risk management standards required by those regulators.

Once again, Yodlee appreciates this opportunity to provide our perspective on the Agencies' proposal. Should we be able to provide any additional information, I hope you will not hesitate to contact me at (202) 997-0850 or sboms@yodlee.com.

Sincerely,

Steven Boms
Vice President, Government Affairs
Envestnet Yodlee