

# Morgan Lewis

**Mark L. Krotoski**

Partner  
+1.650.843.7212  
mark.krotoski@morganlewis.com

**Charles Horn**

Partner  
+1.202.739.5951  
charles.horn@morganlewis.com

February 17, 2017

**VIA EMAIL: [regs.comments@federalreserve.gov](mailto:regs.comments@federalreserve.gov)**

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

**Re: Comment Letter on Enhanced Cyber Risk Management Standards;  
Docket No. R-1550 and RIN 7100-AE-61**

**VIA EMAIL: [regs.comments@occ.treas.gov](mailto:regs.comments@occ.treas.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, DC 20219

**RE: Docket ID OCC-2016-0016**

**VIA EMAIL: [Comment@fdic.gov](mailto:Comment@fdic.gov)**

Robert E. Feldman  
Executive Secretary  
Attention: Comments, Federal Deposit Insurance Corporation,  
550 17th Street NW.,  
Washington, DC 20429

**RE: RIN 3064-AE45**

Ladies and Gentlemen:



Morgan, Lewis & Bockius LLP ("Morgan Lewis") appreciates the opportunity to comment on the joint advance notice of proposed rulemaking titled, "Enhanced Cyber Risk Management Standards" (the "Proposal")<sup>1</sup> issued by the Board of Governors of the Federal Reserve System (the

---

<sup>1</sup> Enhanced Cyber Risk Management Standards, 81 Fed. Reg. 74,315 (Oct. 26, 2016).

**Morgan, Lewis & Bockius .LP**

1400 Page Mill Road  
Palo Alto, CA 94304  
United States

 +1.650.843.4000  
 +1.650.843.4001

"Federal Reserve"), the Office of the Comptroller of the Currency ("OCC"), and the Federal Deposit Insurance Corporation ("FDIC") (collectively the "Agencies"). We have reviewed the Proposal and offer our comments for the Agencies' consideration. Many of our clients are regulated by the Agencies, including bank holding companies, national and state banks, and federal and state savings associations, and their service providers. We advise many clients in all phases of their cybersecurity needs and issues, including on cybersecurity risk assessments and prevention measures, responding to cybersecurity incidents, and developing cybersecurity policies and programs. Several of our largest clients fall within the scope of the Proposal and, accordingly, we have an interest in the Proposal.

## **I. Executive Summary**

On October 19, 2016, the Agencies asked for comment on enhanced cybersecurity standards. The Proposal would apply to U.S. bank holding companies and savings and loan holding companies with total consolidated assets of \$50 billion or more, foreign banking organizations' U.S. operations with U.S. assets of \$50 billion or more, and certain other entities under the jurisdiction of the Agencies ("Covered Entities") and their third-party service providers. Under the Proposal, the Agencies would create a tiered system of standards aimed at reducing cyber risk and preventing financial sector disruptions caused by cyber events. We offer our suggestions to the Agencies regarding the Proposal in this comment letter.

In summary, we recommend that:

- The Agencies should take a principles-based approach of proposing the standards as a combination of a general regulatory requirement to maintain a risk management framework along with a policy statement or guidance that describes minimum expectations for the framework and not issue specific and/or detailed cyber risk management standards.
- The burden and costs associated with complying with detailed cyber risk management standards do not promote cybersecurity or significantly increase effectiveness of preventative cybersecurity programs.
- The Agencies should coordinate with other federal agencies to harmonize guidance, with the objective of consistency among federal regulations.

## **II. The Agencies Should Not Adopt Prescriptive Cybersecurity Rules**

The Agencies should propose cybersecurity standards coupled with guidance instead of adopting a prescriptive rule regime that may not be consistent with existing federal regulations applicable to the Covered Entities or their subsidiaries. The Proposal discusses various approaches to implementation of the enhanced standards.<sup>2</sup> Morgan Lewis recommends that the Agencies take an approach where the Agencies would propose the standards as a combination of principles-based regulatory requirements mandating that Covered Entities maintain a risk management framework for cyber risks that is commensurate with the business and risk profile of the Covered Entity, along with a policy statement or guidance that describes minimum expectations for the framework, such as policies, procedures, and practices commensurate with the inherent cyber risk level of the Covered Entity.

---

<sup>2</sup> See, e.g., Enhanced Cyber Risk Management Standards, 81 Fed. Reg. 74,315 (Oct. 26, 2016).

In our experience, flexible and open standards—even those that are voluntarily adopted—enable firms to tailor and focus efforts on certain areas that are specific to the firm’s particular needs and will have a greater impact on the prevention of cyber-attacks and protection of personally identifiable information. It is now widely accepted that cybersecurity policies are most effective when they are tailored to a firm’s unique cyber risks and vulnerable information. The NIST Cybersecurity Framework (“[NIST Framework](#)”)<sup>3</sup> also expressly adopts a risk-based approach. The NIST Framework focuses on “the likelihood that an event will occur and the resulting impact,” and states that, by taking this information into account, “organizations can prioritize cybersecurity activities, enabling organizations to make informed decisions about cybersecurity expenditures” and develop methods to handle the unique risks faced by different firms by “mitigating the risk, transferring the risk, avoiding the risk, or accepting the risk, depending on the potential impact to the delivery of critical services.”

An effective cybersecurity program, by its nature, cannot be a “one size fits all” or “check the box” program. Rather, the most effective cybersecurity programs take into consideration a host of factors related to the relevant business activities. Previous supervision efforts, such as the Interagency Guidelines issued by the Agencies pursuant to the Gramm-Leach-Bliley Act,<sup>4</sup> have applied a principles-based approach to cybersecurity. A principles-based approach is flexible, permitting firms to tailor their cybersecurity programs to their unique needs, resulting in a more effective approach to cybersecurity.

Further, imposing on Covered Entities a particular technology, system, control, or approach may be unnecessarily burdensome and expensive, especially when infrastructures differ significantly, there are a range of alternatives, or the endpoint can be achieved without applying technology.

Many organizations have heterogeneous information technology environments that develop for a variety of reasons: mergers, legacy systems, customer demands, and so forth. Regulations that specify a particular technology, or method of compliance, may make demands that are impossible or inapposite. Flexible standards are often less vulnerable to obsolescence. Detailed specifications may decay quickly when technology changes rapidly, undercutting the efficacy of regulation, or forcing frequent updates to the detailed specifications. Accordingly, we request the Agencies to adopt an approach that is grounded in principles-based standards, with appropriate supervisory guidance on the standards.

---

<sup>3</sup> The NIST Cybersecurity Framework was developed as a result of President Obama’s Executive Order 13636 (Feb. 12, 2013) and involved the participation of over 3,000 cybersecurity professionals from industry, academia, and government, representing the cybersecurity field’s consensus on the most effective approach to improve cybersecurity. The NIST Cybersecurity Framework is expressly based on an assessment of risk and designed to improve companies’ technical, administrative, and physical protections to combat ever-changing cyber threats. Financial firms already have designed their cybersecurity programs to implement the NIST Cybersecurity Framework and avail themselves of the Federal Financial Institutions Examination Council’s Cybersecurity Assessment Tool and cybersecurity regulations under the Gramm-Leach-Bliley Act, which also adopt risk-based approaches.

<sup>4</sup> See, 12 C.F.R. Part 364, Appendix B, Section II.A (requirement that a bank implement a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the bank and the nature and scope of its activities); *id.* at Section III.C (requirement that a bank design its information security program to control identified risks commensurate with the sensitivity of the information as well as the complexity and scope of the bank’s activities).

### **III. The Burden and Costs Associated With Detailed Standards or Rules Do Not Promote Cybersecurity or Significantly Increase Effectiveness**

Detailed regulations may impose costly requirements on Covered Entities, diverting resources to support compliance rather than on tools to bolster cybersecurity efforts. The interests of Covered Entities and of the Agencies are squarely aligned regarding cybersecurity. Cybersecurity remains a top priority for the financial industry. Each year, Covered Entities expend significant resources to safeguard consumer data and defend against cyber crime. Cybersecurity spending by the financial services industry has soared 67% since 2013. In 2016, security investments increased 11% from the year before.<sup>5</sup> Financial institutions, regardless of size, develop information security plans and deploy a variety of defensive software. It is in the interest of all financial institutions, including Covered Entities, to train employees in cybersecurity best practices and retain experts to assist in further developing protective measures tailored to the specific needs of their firms. Further regulations are not necessary in order to prompt Covered Entities into action on these matters. Covered Entities devote a great deal of attention to compliance with existing cybersecurity regulations and requirements.

In addition, it is critical to consider the cost of complying with detailed standards and consider less costly alternatives before imposing regulations. While the full costs and impact cannot be readily determined, they need to be assessed. As an example, the U.S. Commodity Futures Trading Commission (“CFTC”) recently adopted systems safeguards rules that include a cybersecurity component.<sup>6</sup> The CFTC’s Systems Safeguards Testing Requirements, while applicable to designated contract markets and swap data repositories, demonstrate the high costs of compliance.<sup>7</sup>

We urge the Agencies to carefully consider imposing these types of costs on Covered Entities and whether the costs will support the imposition of stringent rules that may only be marginally beneficial.

### **IV. The Agencies Should Harmonize Guidance With Other Federal Agencies with the Objective of Consistency Among Federal Regulations**

The Agencies should coordinate their cybersecurity efforts with other federal and state regulators to prevent inconsistent standards. Government officials and agencies have long-recognized the need for coordination and convergence of cybersecurity regulatory activity. Former U.S. Treasury Secretary Jack Lew encouraged agencies “to collaborate with the private sector to establish cyber security best practices and improve information sharing.”<sup>8</sup> Comptroller of the Currency Thomas J. Curry has underscored that “[o]ne of the lessons we have learned in the bank

---

<sup>5</sup> See PwC, “Global State of Information Security Survey 2017: Financial Services,” <http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/financial-services-industry.html>.

<sup>6</sup> System Safeguards Testing Requirements, 81 Fed. Reg. 64,272 (Sept. 19, 2016).

<sup>7</sup> The CFTC estimates initial average compliance costs for each designated contract markets and swap data repositories of \$410,625, and CME Group, Inc. estimated ongoing compliance costs of \$1.1 million every two years for external penetration testing and \$5.6 million every two years for conducting controls testing. *Id.* at 64,301-64,302.

<sup>8</sup> Remarks of Secretary Jacob J. Lew, Department of the Treasury, at the 2014 Delivering Alpha Conference (July 16, 2014), <http://www.treasury.gov/press-center/press-releases/Pages/jl2570.aspx>.

regulatory community is that collaboration is vital, especially in dealing with highly complex, rapidly evolving challenges like cybersecurity.<sup>9</sup> And former Deputy U.S. Treasury Secretary Sarah Bloom Raskin stressed the need to “figure out ways [to] harmonize [cybersecurity standards]. We don’t want to see emerge the development of multiple sets of standards, multiple guidances.”<sup>10</sup>

Harmonized guidance is the right approach because Covered Entities and their subsidiaries are already subject to numerous cybersecurity regulations and requirements. They are also subject to a variety of regulatory bodies exercising overlapping jurisdiction—including but not limited to the CFTC, the Securities and Exchange Commission (“SEC”), FDIC, the Federal Reserve, The Federal Trade Commission (“FTC”), OCC, the Financial Industry Regulatory Authority (“FINRA”), and the National Futures Association (“NFA”)—who have all promulgated regulations or guidance.<sup>11</sup> States are increasingly becoming involved in the area of cybersecurity. The New York State Department of Financial Services (“NYDFS”) recently adopted cybersecurity rules that will take effect on March 1, 2017, and Covered Entities will be required to comply if they are licensed or otherwise regulated by the NYDFS.

These comprehensive requirements from federal and state regulators govern all areas of cybersecurity protection, including board engagement, corporate governance, staffing and management, written information security plans, cybersecurity training, technical controls, disposal of sensitive information, and numerous other aspects of cybersecurity. Imposing another regime on Covered Entities and their subsidiaries is likely to present compliance and operational challenges. To the extent that the Agencies adopt final rules on cybersecurity, such rules should exempt subsidiaries that are subject to another regulatory agency’s cybersecurity rules.

\* \* \*

We appreciate the opportunity to offer suggestions to the Agencies concerning the Proposal and are available to discuss our comments or any of the issues raised by the Proposal in

---

<sup>9</sup> Thomas J. Curry, Comptroller of the Currency, Remarks at BITS Emerging Payments Forum (June 3, 2015), <https://www.occ.gov/news-issuances/speeches/2015/pub-speech-2015-78.pdf>.

<sup>10</sup> Lalita Clozel, Regulators Must Improve Cybersecurity Coordination: Top Treasury Official, *American Banker* (Mar. 17, 2016) (quoting Deputy Treasury Secretary Sarah Bloom Raskin), <https://www.americanbanker.com/news/regulators-must-improve-cybersecurity-coordination-top-treasury-official>.

<sup>11</sup> See, e.g., CFTC Systems Safeguards, *supra* fn. 7; CFTC System Safeguards Testing Requirements for Derivative Clearing Organizations, 81 Fed Reg. 64,322 (Sept. 19, 2016); SEC Office of Compliance Inspections and Examinations (“OCIE”), National Exam Program, Examination Priorities for 2016; OCIE National Exam Program Risk Alert, OCIE’s 2015 Cybersecurity Exam Initiative, Volume IV, Issue 8 (September 15, 2015); FTC, Start with Security: A Guide for Business (Lessons Learned from FTC Cases); FTC, Protecting Personal Information: A Guide for Business; NFA, Interpretive Notice to NFA Compliance Rules 2-9, 2-36 and 2-49 Information Systems Security Programs (effective March 1, 2016); FINRA Report on Cybersecurity Practices (February 2015); FINRA 2016 Regulatory and Examination Priorities Letter (January 5, 2016); Interagency Guidelines, *supra* fn.4.

February 17, 2017  
Page 6

greater detail with the Agencies or their staff. If the staff has any questions, please do not hesitate to contact Mark Krotoski at 650-843-7212 or [mark.krotoski@morganlewis.com](mailto:mark.krotoski@morganlewis.com) or Charles Horn at 202-739-5951 or [charles.horn@morganlewis.com](mailto:charles.horn@morganlewis.com).

Respectfully submitted,

Handwritten signature of Mark Krotoski in blue ink.

Mark Krotoski, Esq.  
Partner, Morgan, Lewis & Bockius LLP

Handwritten signature of Charles Horn in black ink.

Charles Horn, Esq.  
Partner, Morgan, Lewis & Bockius LLP