August 2, 2019

Via Electronic Submission through
https://www.regulations.gov/docket?D=FTC-2019-0019

David Lincicum and Allison M. Lefrak
Division of Privacy and Identity Protection
Bureau of Consumer Protection
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: Notice of Proposed Rulemaking – Standards for Safeguarding Customer Information, RIN 3084-AB35 (Safeguards Rule, 16 C.F.R. part 314, Project No. P145407)

Ladies and Gentlemen:

The Bank Policy Institute (BPI) – BITS, the American Bankers Association (ABA), and the Securities Industry and Financial Markets Association (SIFMA) (collectively, the "Associations")[1] appreciate the opportunity to comment on the Federal Trade Commission's ("FTC") proposal to amend the Standards for Safeguarding Customer Information (the "Safeguards Rule" or "Rule").[2] We share your commitment to protecting the interests of all Americans by safeguarding their personal information. We agree with the FTC's view that it is important "to provide financial institutions with the flexibility to shape [] information security programs to their particular business and to allow the programs to adapt to changes in technology and threats to the security and integrity of customer information."[3]

The Associations also appreciate the FTC's efforts to clarify the scope of the Safeguards Rule in light of changes to the authority of the Privacy Rule. We also appreciate the FTC's efforts to coordinate key aspects of its proposed amendments with other agencies' regulatory provisions, notably, amending the definition of "financial institution" so that it cross-references permissible activities enumerated by the Federal Reserve Board in 12 C.F.R. §§ 225.28 and .86.[4]

---

[1] Descriptions of the Associations are provided in *Annex A* of this letter.

[2] 16 C.F.R. part 314.

[3] Safeguards Rule, 84 Fed. Reg. 13,158, 13,159 (proposed Apr. 4, 2019) (to be codified at 16 C.F.R. pt. 314).

[4] Lists of permissible non-banking activities for bank holding companies and financial holding companies, respectively.

To further streamline and avoid overlap, however, we recommend that the FTC harmonize the remaining proposed amendments to its Safeguards Rule with the Federal Financial Institutions Examination Council ("FFIEC") Interagency Guidelines Establishing Information Security Standards ("Interagency Guidelines"),[5] rather than selecting and altering provisions from the New York Department of Financial Services ("NYDFS") Cybersecurity Requirements for Financial Services Companies[6] and the National Association of Insurance Commissioners ("NAIC") Insurance Data Security Model Law.[7] We also recommend that the FTC map its amendments to the industry-supported Financial Services Sector Coordinating Council ("FSSCC") Cybersecurity Profile to allow cybersecurity professionals at covered firms to remain focused on the important work of identifying, managing, and mitigating data security risks, rather than on revising policies and procedures to align with the FTC's revised regulations.

In particular, we are concerned that the FTC's proposal represents a substantial departure from the historical risk-based approach that the FTC and other regulators have taken with respect to implementing Gramm-Leach-Bliley Act ("GLBA") security requirements. For example, the FTC's proposal would impose prescriptive and one-size-fits-all requirements on financial institutions subject to the FTC's authority under the GLBA. In doing so, the FTC risks incentivizing those financial institutions to approach security as a compliance exercise rather than focusing on maintaining a comprehensive program that focuses primarily on identifying and addressing risks.

I. Executive Summary

In adopting a revised version of the Safeguards Rule, it is important that the FTC endeavor to harmonize any new regulatory requirements with existing rules. Such harmonization is critical to ensuring that the limited pipeline of cybersecurity professionals can focus their time and energy on front-line defense and security rather than check-the-box compliance exercises. Harmonization is also critical to help consumers understand their rights and responsibilities. Successful harmonization cannot be achieved, however, by selecting and altering certain provisions from newly developed and limitedly adopted state-level laws or regulations. In Part I, we explain the importance of harmonization and why the FTC should utilize the longstanding and extensively-used FFIEC Interagency Guidelines and IT Examination Handbook for the revised Safeguards Rule, rather than the selected and modified provisions from the NYDFS cybersecurity regulations and NAIC Model Law.

To ease unnecessary compliance burden, ensure that a revised version of the Safeguards Rule does not include significant substantive gaps, and to improve regulator visibility into sector wide, firm specific and third-party practices, the FTC should also map any new or revised regulatory requirements to the FSSCC-developed Cybersecurity Profile. As explained in further detail in Part II, the Cybersecurity Profile is a scalable and extensive assessment framework, organizing the web of cybersecurity regulatory requirements – including those from the FFIEC – around the National Institute of Standards and Technology ("NIST") Cybersecurity Framework.

---

[5] 12 C.F.R. pt. 30, app. B (as incorporated into the OCC regulations for national banks).

[6] N.Y. Comp. Codes R. & Regs. tit. 23, pt. 500, https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf.

[7] NAIC Model Laws, Regulations, Guidelines & Other Resources, Insurance Data Security Model Law (2017), https://www.naic.org/store/free/MDL-668.pdf.

Finally, in Part III, we describe some of the specific challenges with the FTC's proposed Rule, including longstanding challenges with respect to the selected provisions from the NYDFS cybersecurity regulations and NAIC Model Law, as well as new challenges that would arise with the FTC's amended language. These specific concerns include: (i) the limited manner in which the risk assessment is incorporated into the Rule, (ii) the static nature of the multi-factor authentication requirement, (iii) the potentially security limiting encryption requirement, and (iv) the nature and frequency of the penetration testing, vulnerability assessment, and continuous monitoring requirements. Here, we explain our concerns with the proposed Rule, place these concerns in the context of the FFIEC and/or NYDFS cybersecurity standards, and propose alternative approaches to address these issues.

II. The FTC should harmonize the proposed amendments to the Safeguards Rule with the FFIEC Interagency Guidelines, rather than selecting and altering provisions from less-broadly adopted, fluctuating state models.

As discussed in the notice of proposed rulemaking, the Interagency Guidelines require financial institutions to adopt robust information security programs that include: (i) board of director involvement, with at least annual reporting to the board; (ii) risk assessment; (iii) risk management and control; (iv) oversight of service providers; (v) an incident response program; and (vi) periodic updating. These requirements are well-established and widely used within the financial sector, including critical third parties and across all fifty states. These guidelines have proven effective in safeguarding consumer data and are further supplemented by the FFIEC IT Examination Handbook and various guidance documents issued by the FFIEC agencies.

In accordance with these requirements, financial institutions' data security programs generally address issues related to governance; information security program management (including risk identification, measurement, mitigation, monitoring, and reporting); security operations; and information security program effectiveness, as outlined in detail in the FFIEC IT Examination Handbook: Information Security Booklet. Other parts of the FFIEC IT Examination Handbook include relevant information security requirements and standards (e.g., Booklets on Outsourcing Technology Services, E-Banking, and Retail Payment Systems). The FFIEC also regularly publishes guidance based on evolving threats and best practices, which banks use to enhance their information security programs. These standards are widely used and—though regularly supplemented with topical guidance as changing technologies and threats warrant—have been "battle tested" over the many years since they were first issued.

In contrast, the NYDFS cybersecurity regulations and NAIC Model Law were recently released, and the NAIC Model Law by NAIC's last count in April has only been adopted by four states. By selecting and modifying various provisions from each, the benefits of leveraging these regulatory frameworks are outweighed by an increased cybersecurity regulatory patchwork and the disproportionate amount of time needed to reconcile this complex maze with a financial institution's cybersecurity program. Moreover, as discussed below, certain provisions selected from the existing regimes, including the requirements regarding multi-factor authentication, encryption, and testing/monitoring, retain some of the challenges inherent in those provisions when originally proposed by NYDFS.

A. Harmonization with FFIEC standards is appropriate as they are comprehensive, flexible, and effective in ensuring that financial institutions maintain and improve their information security programs while also protecting customer information.

In developing upgraded cybersecurity standards for members of the financial sector, the Associations recommend that the FTC look to the widely-used and longstanding FFIEC Interagency Guidelines and FFIEC IT Handbook. These regulations, standards, and guidance documents should be used because they provide for a risk-based approach, more comprehensively address the security controls, and are the most battle tested and widely used models across the financial services sector and the third parties that service the sector's firms.

The Interagency Guidelines' comprehensive, yet flexible, risk-based approach has proven effective in ensuring that financial institutions maintain and improve their information security programs on a continuous basis and in protecting customer information. With new technologies and advancing threats, the Guidelines' adaptability has been enhanced with the development of additional guidance documents, such as the Interagency Guidance on Response Programs, the FFIEC IT Handbook, and more informal one-off guidance. In addition to the requirements mentioned in the Executive Summary, the Interagency Guidelines also require:

- Board involvement in the security program beyond receiving annual reports;
- Management involvement in the security program (other than the Chief Information Security Officer ("CISO"));
- Employee background checks;
- Business continuity programs;
- Network segmentation;
- Anti-malware or anti-virus protection;
- Dual control procedures; and
- Data breach notification.

In contrast, the Safeguards Rule as proposed does not include these additional requirements, assuring substantive gaps in information security best practices.

B. Selecting and modifying isolated provisions from the NYDFS Cybersecurity Regulations and NAIC Model Law will <u>not</u> further the FTC's laudable goals of balancing flexibility with prescriptive detail and utilizing existing, widely-adopted regulatory frameworks.

The Associations appreciate the FTC's goal in revising the Safeguards Rule to include more guidance, specificity and certainty to financial institutions while maintaining a flexible and adaptable approach as is suggested in the proposal's preamble.[8] We also commend the FTC's goal of using existing

[8] In the preamble, the FTC explained that it leveraged the NYDFS cybersecurity regulations and NAIC Model Law as models based on the belief that both "maintain the balance between providing detailed guidance and

regulatory models that are broadly applicable and widely adopted.[9] The selection and alteration of isolated provisions from the NYDFS cybersecurity regulations and NAIC Model Law do not further those goals, however.

First, as explained more fully below in Section III, certain provisions in the FTC proposal, including the multi-factor authentication, encryption, and testing/monitoring requirements, add to and/or retain some of the problematic language and overly prescriptive and inflexible requirements of these models. These include, for example, (i) requirements that the CISO personally approve alternative controls to multi-factor authentication and encryption (rather than allowing the CISO's designee to approve some such alternatives and otherwise provide financial institutions the flexibility to leverage innovative authentication and data protection technologies); (ii) overly broad and impractical mandatory encryption requirements that attempt to draw clear distinctions between "external" and "internal" networks in a manner that is not consistent with the realities of modern IT infrastructure; and (iii) overly prescriptive penetration testing requirements disconnected from actual risks.

Second, with respect to the applicability and use of the recently developed NYDFS cybersecurity regulations and NAIC Model Law, only certain states have adopted these regimes. Accordingly, given this adoption patchwork and the inherent dissonance in expectation that stems from it, they are not as optimal for a national regulatory expectation as the more broadly adopted, time tested FFIEC Interagency Guidelines and supplementary guidance. As acknowledged in the Dissenting Statement of Commissioners Phillips and Wilson, "[w]e do not have data about the impact and efficacy of those regulations, so whether to adopt a version of them at the federal level and whether that version should be a floor for or should preempt state-level rules seem like questions worthy of more study."[10] To the extent that the NYDFS cybersecurity regulations and NAIC Model Law do apply, they apply narrowly to certain financial institutions subject to the authority of the NYDFS and to covered insurers in certain states.

Adding to this patchwork might not only cause confusion for the most seasoned compliance professional, but it certainly would for the average customer seeking to understand data security requirements across the different types of institutions he or she might entrust with his or her information.

C. Harmonization is needed to address the fragmented regulatory landscape for data security requirements, thereby creating a level playing field for covered businesses and better protecting consumer information.

The current fragmented approach to cybersecurity regulation causes financial firms to

---

avoiding overly prescriptive requirements for information security programs." Safeguards Rule, 84 Fed. Reg. at 13,163.

[9] *See, e.g.*, *id.* ("The Commission is interested in receiving data, research, case studies, or other evidence related to business efforts to comply with the Cybersecurity Regulations or state laws mirroring the Model Law," suggesting that the applicability and adoption of the NYDFS cybersecurity regulations and NAIC Model Law are sufficiently widespread such that these types of evidence would exist).

[10] *Id.* at 13,177.

expend a disproportionate amount of senior leadership and frontline personnel's time and other resources to reconcile notionally similar, but semantically different, cybersecurity proposals and agency expectations. It introduces inefficiencies by requiring institutions to identify, draft, and compile functionally equivalent sets of data from and for the same systems to satisfy each different regulator and each different regulatory standard, whether requirements that apply directly or ones that apply indirectly as a result of "flow-through" contractual requirements of key third parties subject to an additional regulator. As a result, institutions are forced to create single-use compliance/assessment data, rather than focusing their time on developing security and mitigation techniques that improve a firm's cybersecurity program and protects customers. These inefficiencies also handicap the ability to protect consumer data by consuming resources that could be far better spent on security rather than stand-alone, immaterial compliance information requests.

When the sector surveyed its information security teams in late 2016, CISOs reported that approximately 40% of their cyber team's time was spent on compliance related matters, not on cybersecurity.[11] Due to one framework issuance, in particular, the reconciliation process delayed one firm's implementation of a security event monitoring tool intended to better detect and respond to cyber-attacks by 3-6 months. With respect to another issuance, another firm stated that 91 internal meetings were held to determine how that issuance aligned with its program and in gathering data for eventual regulatory requests.

While each agency's set of requirements may individually have merits, when continuously layered on institutions – as opposed to incorporating by reference prior effective cybersecurity regulatory regimes as the Associations recommend – the added complexity is unsustainable. One significant problem is that the unnecessary complexity creates a heightened demand for cybersecurity professionals to attempt to reconcile the inconsistencies, and there are simply not enough cybersecurity professionals available to perform the necessary work. According to the 2018 Cybersecurity Workforce Study by $(ISC)^2$, there are nearly 3 million unfilled cybersecurity jobs worldwide, with nearly 500,000 in North America.[12] The study further found that 63% of surveyed organizations reported a shortage of IT staff dedicated to cybersecurity (including 23% with a "significant" shortage), and 59% said that their respective companies were "at moderate or extreme risk of cybersecurity attacks due to [this] shortage."[13] This shortage of qualified professionals is further aggravated when these professionals focus their time and energy reconciling – or attempting

---

[11] In written testimony before the Senate Homeland Security and Governmental Affairs Committee last year, BITS President Chris Feeney submitted charts of the over 30+ issuances that industry had been tracking since the release of the NIST Cybersecurity Framework in 2014 that directly impacted firms in the financial services sector. Those charts can be found in Appendix A and can be accessed here: https://www.hsgac.senate.gov/imo/media/doc/Testimony-Feeney-2017-06-21.pdf. Since that time, BITS has not resumed the tracking because of the volume of proposals at the state and international level. This estimate predated the Financial Stability Board's announcement in 2017 that 72% of its 25 member jurisdictions were self-reporting that each had plans to issue further cybersecurity regulatory frameworks and guidance.

[12] $(ISC)^2$, Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens: $(ISC)^2$ Cybersecurity Workforce Study at 4 (2018), https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx?la=en&hash=4E09681D0FB51698D9BA6BF13EEABFA48BD17DB0.

[13] *Id.* at 5.

to reconcile – disparate regulatory requirements instead of focusing on strengthening cybersecurity.

The lack of harmonization also complicates efforts to coordinate across critical infrastructure sectors and with the federal government for cyber incident response. A key focus for the federal government and DHS, in particular, has been to foster a "whole of nation" approach to cybersecurity. This effort to foster greater public-private partnership is critical if we are to effectively protect our economy, our customers, and our citizens from cyber threats. As regulations pull financial institutions away from using the more recognized and widely deployed approaches, such as those called for in the Interagency Guidelines and the accompanying FFIEC IT Examination Handbook, the NIST Cybersecurity Framework, or the FSSCC Cybersecurity Profile, which is based on both, this could endanger not only our sector, but other critical infrastructure sectors if a coordinated response is needed.

The Interagency Guidelines and accompanying IT Examination Handbook are widely used, time tested, and are incorporated within the Profile, which is further discussed below. The provisions selected from the NYDFS cybersecurity regulations and NAIC Model Law and at times modified, however, are not as widely known. And perhaps more importantly, the modifications represent the type of topical overlap combined with semantic differences that require firms to pull cyber professionals from frontline defense to assist with reconciling new terminology for old concepts against their existing programs. Further, while the FTC has proposed to select and modify certain components of the NYDFS cybersecurity regulations (and the NAIC Model Law), the NYDFS rules were themselves developed by selecting and modifying different aspects of other data security standards. Because the NYDFS regulations already represent "cherry-picking" from various cyber standards, additional selective selection and modification of these standards deepens the fragmentation between the different regulatory standards. Without mapping these expectations consistently, as done in the Profile, the time needed for reconciliation is only heightened.

III. The FTC should map its amendments to the FSSCC Cybersecurity Profile to allow cybersecurity professionals at covered firms to remain focused on managing data security risks, rather than on revising policies and procedures.

To address appropriate agency concern and allow for better sector-wide and third-party cybersecurity risk management comparison, while also allowing cyber professionals to focus their time on frontline activities, the FSSCC developed the Cybersecurity Profile. The Profile is a scalable and extensive assessment framework that organizes the multitude of cybersecurity regulatory expectations – most notably, the Interagency Guidelines and accompanying FFIEC IT Examination Handbooks – around the commonly used and well-understood structure and taxonomy of the NIST Cybersecurity Framework. The Profile synthesizes examination requests into a concise set of diagnostic questions mapped to specific agency issuances and information security controls, such as those from the International Standards Organization ("ISO"). For version 1.0, developers were able to reduce over 2300 regulatory provisions to 277 diagnostic assessment questions, an 88% reduction of topically similar but semantically different provisions.

The Profile was developed from and peer-review through 50+ working sessions and NIST-hosted, publicly open workshops. These sessions included CISOs, Chief Information Risk Officers, cyber and regulatory attorneys, and policy specialists from over 150 financial institutions and FinTechs, including banks of all sizes, brokerage firms, asset managers, insurance companies, market utilities, and associations, each offering their subject matter expertise. Development also included input, review, and

feedback from numerous financial services agencies, self-regulatory organizations, and regulatory associations (e.g., NYDFS and NAIC). With their input, the Profile was developed to be scalable across the financial services industry, unlike the proposed standards for the Safeguards Rule which are generally more prescriptive and applicable to fewer firms.

The Profile, by design, is an assessment that supports the entire industry, as well as third parties such as FinTechs, as diagnostic questions are suited to the risks inherent in a firm's business model, geographic footprint and complexity. It (i) applies, through tiering, to community banks/credit unions as well as complex multi-national organizations; (ii) synthesizes regulatory expectations into condensed diagnostic question sets, thereby simplifying cybersecurity reviews and regulatory examinations, and (iii) can be used for internal firm cybersecurity assessment and for assessment of external third parties. Furthermore, the Profile was designed to cover the majority of cyber best practices while enabling regulators – such as the FTC – to add additional areas of focus through their own mappings of subsequently issued regulations or guidance.

The Profile is not designed to dictate regulation, but to provide a methodology for organizing regulation. A key difference, then, is that the Profile can adapt over time as technologies evolve while the proposed changes to the Safeguards Rule are more static and less adaptable. For example, as new protections evolve, encryption might turn out to not be the appropriate solution nor best method for protecting data. The Profile also allows increased focus of cybersecurity experts' time on protecting global financial platforms across numerous fronts including operational, risk and resiliency areas versus performing non-additive compliance activity. For a global economy already burdened with a well-documented shortage of skilled cybersecurity professionals, streamlining compliance while maintaining and increasing security activity would serve to enhance overall cybersecurity.

Mapping the Safeguards Rule, revised as proposed, to the Profile would clarify where the revised Safeguards Rule would leave gaps when compared to the well-regarded risk management framework adopted in the NIST Cybersecurity Framework. Our preliminary mapping indicates that the proposed Safeguards Rule would retain significant gaps in a number of Functions, including:

- Governance: independent risk management function and audit;
- Respond: communications, analysis, and mitigation;[14]
- Recover: recovery planning and communications; and
- Dependency Management: internal dependencies, resilience, and business environment.

For the regulatory community, Profile use would also enhance transparency and improve visibility across institutions, subsectors, third parties, and sectors, enabling better analysis and mitigation of systemic and concentration risks. In particular, it assists financial institutions by improving boardroom and executive engagement, understanding and prioritization of cyber risks and enhancing

[14] While some of these are required to be addressed in the incident response plan that would be required under the proposed revisions to the Rule, the Rule does not include any specific requirements for these steps themselves.

the efficient management of third-party vendors. It also assists regulators by tailoring examinations to institutional complexity, thereby enabling "deeper dives" in those areas of greater concern to that particular agency and enabling supervisory agencies to better discern the sector's systemic risk, with more agency time for specialization, testing and validation. More broadly, the Profile improves the financial services sectors' approach to managing data security and cyber risk as it (i) allows for greater intra-sector, cross-sector and international cybersecurity collaboration and understanding; (ii) enables collective action to better address collective risks; and (iii) facilitates greater innovation as technology companies, including FinTechs, are able to evidence security against the standardized set of compliance requirements.

IV. Concerns with specific, proposed provisions, which would diminish security and deviate from the FTC's own well-established risk-based approach.

As noted at the outset, the Associations are concerned with specific proposal provisions that they believe, if enacted, would represent a significant departure from the historical risk-based approach that the FTC and other federal regulators have taken with respect to implementing the GLBA's data security mandates and run counter to the overall goal of safeguarding customer information. Proposal requirements to implement specific technical controls regardless of what a risk assessment might reveal would eliminate the discretion covered financial institutions need to tailor their security program and controls based on the nature of each particular covered financial institutions' business and risk profile. By failing to tie requirements to a risk assessment's recommendations, the FTC's proposal would have the unintended consequence of fostering a "checklist" approach to security that compels financial institutions to focus only on the controls identified in the rule without taking a holistic and risk-based approach that incorporates safeguards designed to address identified risks.

In addition to the above concern, the Associations also have a number of specific concerns related to the proposed provisions concerning multi-factor authentication, encryption, penetration testing, vulnerability assessments, and continuous monitoring. If enacted as proposed, these provisions would increase the complexity of compliance while failing to enhance consumer security – either by repeating mistakes from the NYDFS regulations or the NAIC Model Law or by failing to cure those mistakes (or introducing new concerns) in the manner in which the FTC has proposed to modify those provisions. For each requirement, we propose using FFIEC materials as the model for the particular requirement.[15]

A. Risk assessment expectations should be flexible and risk-based rather than the prescriptive expectations identified in the proposed Rule.

While the proposed revised Safeguards Rule would require that financial institutions conduct a risk assessment, the manner in which this requirement is included in the proposed Rule would leave the remaining prescriptive requirements unmoored from this risk assessment. Specifically, as revised, the Safeguards Rule would require covered financial institutions to "[b]ase [their] information security program on a risk assessment," as one of the requirements for developing, implementing, and

[15] To the extent the FTC declines to follow these recommendations, the Associations also propose modest modifications to the current proposed language that would, at least to some extent, address the concerns raised herein.

maintaining a compliant information security program.[16] It then would require that financial institutions "[d]esign and implement safeguards to control the risks … identif[ied] through [the] risk assessment, including" a number of delineated specific and prescriptive requirements (e.g., implementing access controls, deploying encryption (as described further in Section IV.C, below), adopting secure development practices, implementing multi-factor authentication (as described further in Section IV.B, below)).[17] While the various safeguard requirements are, therefore, framed as being based on the risk assessment, the prescriptive requirements that follow give no indication that FTC-regulated financial institutions would have the flexibility to eschew implementation if, based on the institutions' risk assessments, they determine that such a stringent and/or organization-wide control is not warranted or appropriate.

By contrast, the FFIEC Interagency Guidelines provide that financial institutions regulated by FFIEC agencies should "[d]esign [their] information security program[s] to control the identified risks," and "adopt those measures the [financial institution] concludes are appropriate," including various specific examples of controls.[18] The Associations therefore recommend that the FTC revise its requirements to specifically provide for the flexibility to adopt the various outlined controls as appropriate based on each institution's particular risk analysis.[19]

Rewriting the proposed Rule in the above manner has the potential to change the entire character of the regulation by enabling financial institutions to apply a risk-based approach to the planning and implementation of all of the controls identified in the proposed Rule. This would optimize resources and attention on addressing the risks that the firm truly faces, enabling frontline defenders to better secure the customer and corporate data that they are entrusted to protect.

---

16 16 C.F.R. § 314.4(b) (as proposed to be amended).

17 *Id.* § 314.4(c) (as proposed to be amended).

18 12 C.F.R. pt. 30, app. B, § III.C.1.

19 The NYDFS cybersecurity regulations were also modified, through the rulemaking process, to ensure the requirements could be implemented based on the risk assessment. *See, e.g.*, N.Y. Comp. Codes R. & Regs. tit. 23, § 500.05 ("The cybersecurity program for each Covered Entity shall include monitoring and testing*, developed in accordance with the Covered Entity's Risk Assessment* . . . . Entities shall conduct: (a) annual Penetration Testing of the Covered Entity's Information Systems determined each given year *based on relevant identified risks in accordance with the Risk Assessment*; and (b) bi-annual vulnerability assessments, including any systematic scans or reviews of Information Systems reasonably designed to identify publicly known cybersecurity vulnerabilities in the Covered Entity's Information Systems *based on the Risk Assessment*" (emphasis added)); *Id.* § 500.06(a) ("Each Covered Entity shall securely maintain systems that, *to the extent applicable and based on its Risk Assessment* . . . ." (emphasis added)). If the FTC declines to follow the approach followed by the FFIEC agencies, it should revise the prescriptive requirements to ensure that the specific requirements apply only as warranted by each institution's respective risk assessment.

B. The proposed Rule's multi-factor authentication expectations are overly prescriptive and vague and should be revised to provide for requirements similar to those in the FFIEC Interagency Guidelines and authentication guidance, requiring risk-based, layered authentication protocols.

Under the proposal, covered institutions would be required to "[p]lace access controls on information systems, including controls to authenticate and permit access only to authorized individuals to protect against the unauthorized acquisition of customer information and to periodically review such access controls."[20] The proposed Rule would also require covered financial institutions to then "[i]mplement multi-factor authentication for any individual accessing customer information. Multi-factor authentication shall be utilized for any individual accessing your internal networks that contain customer information, unless your CISO has approved in writing the use of reasonably equivalent or more secure access controls."[21] While drawn from the NYDFS requirements, the provisions differ significantly in that NYDFS requires its covered entities (i) to protect against unauthorized access through the implementation of "effective controls," *potentially* including multi-factor authentication *or risk-based authentication*, based on the entity's risk assessment; and (ii) absent CISO approval, to use reasonably equivalent or more secure controls, use multi-factor authentication when accessing internal networks *from an external network*.[22]

As proposed, the FTC Safeguards Rule is confusing, introduces problems not present in the NYDFS regulations, and repeats an error inherent in the NYDFS regulations. As an initial matter, it is unclear whether the multi-factor authentication in the proposed FTC Rule is actually one requirement – with the second sentence adding greater specificity to the requirement in the first sentence – or two requirements, i.e., is written CISO approval of equivalent controls required solely for access to internal networks or also to those accessing customer information?

Moreover, unlike the NYDFS rule, the proposed revisions to the Safeguards Rule specifically require multi-factor authentication for any individual accessing customer information – rather than deferring to the institution's risk assessment and requiring more broadly that the institution use effective, layered, risk-based authentication and access controls to protect the information and systems. This difference is compounded by the ambiguity described above – i.e., it is unclear if the FTC proposal would permit the CISO to authorize the use of alternative, equally effective controls. To the extent the second sentence represents a distinct requirement (and the only requirement here subject to CISO override), this imposes a fractured compliance burden, not tied to an institution's risk profile or even effective security. Other security controls may be equally effective or potentially even more effective, as the FFIEC authentication guidance referenced below implicitly recognizes in avoiding a specific multi-factor authentication requirement.[23]

---

[20] 16 C.F.R. § 314.4(c)(1) (as proposed to be amended).

[21] *Id.* § 314.4(c)(6) (as proposed to be amended).

[22] N.Y. Comp. Codes R. & Regs. tit. 23, § 500.12.

[23] *See* FFIEC, Supplement to Authentication in an Internet Banking Environment at 2 (June 28, 2011), https://www.ffiec.gov/pdf/Auth-ITS-Final%206-22-11%20(FFIEC%20Formated).pdf ("[M]alware can compromise some of the most robust online authentication techniques, including some forms of multi-factor authentication.").

Additionally, while the NYDFS rule makes clear that the multi-factor authentication requirement for access to internal networks applies only to access from external networks, the proposed Safeguards Rule revisions seemingly would apply the requirement to any access to internal networks – including from internal networks. This is cumbersome and adds minimal, if any, additional security. However, it would become an unwieldy regulatory burden.

Lastly, the proposed revisions to the FTC Safeguards Rule retain an unnecessary requirement in the NYDFS regulations for CISO approval for each and every mechanism by which internal networks are accessed other than by multi-factor authentication. We urge the FTC to revise this requirement, as we did with the NYFDS, because it does not accurately reflect best practices, or operate as an effective cybersecurity measure. If a financial institution's information security team determines that multi-factor authentication is not the best means by which to secure an entity's internal networks, or that a different control would provide more security, such determination should not require approval by a CISO on every occasion. A host of new, innovative risk-based authentication tools are currently being tested, using risk-based analyses, to determine when a second factor is warranted or otherwise moving towards password-less solutions. Financial institutions should have the flexibility to shift to these new technologies, once proven effective, without having to go through unnecessarily formulaic approvals to do so. Instead, the requirement to use multi-factor authentication for access to internal networks should be revised to allow for other effective controls based on an entity's risk assessment. That would be consistent with existing standards that provide individual institutions with the ability to assess and manage their risks *as appropriate* and also prevent trapping institutions into an approach that might become quickly outdated.

By comparison, the Interagency Guidelines include a requirement that is similar to the proposed Safeguards Rule requirement in that it requires covered institutions adopt "[a]ccess controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means."[24] However, through supplementary authentication guidance, the FFIEC states that firms must implement layered security around authentication (potentially, but not necessarily, including in some instances multi-factor authentication), adjusted based on periodic risk assessments.[25]

As such, the Associations recommend that the FTC revise the multi-factor authentication requirement to provide for requirements similar to those in the FFIEC Interagency Guidelines and authentication guidance, requiring risk-based, layered authentication protocols rather than mandating use of multi-factor authentication in specific circumstances unmoored from risk assessments.[26] Any

---

[24] 12 C.F.R. pt. 30, app. B, § III.C.1.a.

[25] FFIEC, Supplement to Authentication in an Internet Banking Environment.

[26] To the extent the FTC declines to follow the FFIEC's well-established and tested approach, the FTC should still modify the language in the proposed rule to correct the specific issues identified above, as follows:

> Implement multi-factor authentication for any individual accessing customer information~~. Multi-factor authentication shall be utilized for any individual accessing~~ on your internal networks~~ that contain customer information~~ from an external network, unless ~~your CISO approved in writing the use of~~

mandatory and inflexible regulatory requirement that would likely be in effect for years, if not decades, would risk stifling innovations in authentication technologies that could be more efficient, less cumbersome, and ultimately more secure. Because the financial services sector is often a leader in purchasing and implementing new, enhanced, and state-of-the-art data security controls, limiting the financial sector's ability to leverage technological innovations could cripple the market for new technologies, with ripple effects across the economy.

C. The proposed Rule's mandatory encryption requirements will cause massive delays in data processing times and stretch critical in-house personnel with questionable security benefit and should be revised to align with FFIEC expectations.

Under the proposal, covered financial institutions would be required to "[p]rotect by encryption all customer information held or transmitted by [the institution] both in transit over external networks and at rest. To the extent [the institution] determine[s] that encryption of customer information, either in transit over external networks or at rest, is infeasible, [the institution] may instead secure such customer information using effective alternative compensating controls reviewed and approved by [the] CISO."[27] This requirement is based on the NYDFS regulation.

As we stated in comment letters to NYDFS during the comment period on such requirements, a broad-spectrum encryption requirement is not only infeasible, but also detrimental to financial institutions' ability to maintain a fluid, evolving cybersecurity program. Implementing mandatory encryption requirements will cause massive delays in data processing times and stretch critical in-house personnel with questionable security benefit.

As with NYDFS, the FTC attempts to distinguish between "external" and "internal" networks. Due to the complexity of current network environments, the line between external and internal networks has become increasingly blurred, to the point that seasoned information technology and information security professionals frequently have different definitions for each. Moreover, requiring data encryption across-the-board weakens security controls by: (a) blocking standard surveillance of such data to detect intruders; and (b) requiring the broad distribution of encryption keys to allow applications to access such data, increasing the number of vulnerability points. In this way, although encryption is frequently thought of as a catch-all for cybersecurity, broadly mandating encryption of data increases cybersecurity challenges for covered financial institutions, complicates in-house access to this data, and decreases in-house mobility toward a more advanced cybersecurity posture. This is further compounded in the proposed FTC version of this requirement by excluding the NYDFS provision's requirement that this be based on the institution's risk assessment. The FTC's proposal also retains the requirement that encryption be "infeasible" without articulating "feasibility" or "infeasibility" criteria.

Mass encryption of data, specifically data at rest, creates numerous information security challenges. Implementing encryption throughout existing programs and applications, thereby requiring encryption keys for basic system access, would dramatically impede normal business operations.

~~reasonably equivalent or more secure access~~ based on your risk assessment, other controls are appropriately effective.

[27] 16 C.F.R. § 314.4(c)(4) (as proposed to be amended).

Moreover, if encryption key(s) are lost, or compromised, the availability and/or confidentiality of an institution's information systems and data would be placed at unnecessary risk. Finally, as noted above, the CISO should not be required to approve every single alternative control, with permissive use of a designee in the alternative.

To achieve a similar outcome in protecting data, the Associations recommend that the FTC instead adopt the FFIEC's approach to data encryption. Specifically, under the Interagency Guidelines, FFIEC-regulated financial institutions are required to implement, as appropriate, "[e]ncryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access."[28] The FFIEC IT Examination Handbook Information Security Booklet further makes clear that this should be a risk-based assessment, instructing management to "implement the type and level of encryption commensurate with the sensitivity of the information."[29] Adopting this approach has the benefits of ensuring necessary flexibility, requiring the use of encryption on systems where unauthorized access is reasonably foreseeable, and making regulator expectations clear that the extent and type of data encryption used should be based on the sensitivity of the data.

Cybersecurity is a fluid area, and institutions require flexibility to ensure robust programs to meet the needs of a diverse industry. Although encryption is a useful and commonly used tool, it is neither the required nor the preferred approach for the broad range of situations mandated in the FTC's proposed revisions. The FTC should model our proposed revisions in the multi-factor authentication requirement, recognizing that encryption is currently one possible component of cybersecurity practice, though new and better tools may be developed and adopted in the future.[30]

---

[28] 12 C.F.R. pt. 30, app. B, § III(C)(1)(c).

[29] FFIEC IT Examination Handbook, Information Security Booklet § II.C.19 (Sept. 2016).

[30] If, however, the FTC continues to follow an approach based on the NYDFS regulations rather than the Interagency Guidelines and FFIEC guidance, the FTC should still modify the language in the proposed rule to correct the specific issues identified above, as follows:

> Based on your risk assessment, implement controls to protect ~~by encryption~~ all customer information held or transmitted by you ~~both in~~, which shall include encryption for transit over external networks ~~and at rest~~. To the extent you determine that encryption of customer information, either in transit over external networks ~~or at rest,~~ is not reasonably ~~in~~feasible or based on your risk assessment, that other controls are appropriately effective, you may instead secure such information using effective alternative compensating controls reviewed and approved by your CISO (or a qualified designee).

Revising the language in this manner will provide firms with much-needed flexibility to adopt new technologies that supersede encryption, rather than unnecessarily requiring FTC-regulated financial institutions to adopt massive encryption efforts.

D. The proposed Rule's penetration testing, vulnerability assessments, and continuous monitoring expectations are too broad, overly prescriptive in their required frequency, and do not adequately describe the processes by which systems and applications are tested and should instead leverage the FFIEC's expectations.

Similar to the NYDFS rule, the proposed Safeguards Rule would require covered financial institutions to "[r]egularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures, including those to detect actual and attempted attacks on, or intrusions into, information systems."[31] This is to include "continuous monitoring or periodic penetration testing and vulnerability assessments," and, "[a]bsent effective continuous monitoring or other systems to detect, on an ongoing basis, changes in information systems that may create vulnerabilities," to conduct (i) annual penetration testing of information systems determined each year based on the risk assessment and (ii) biannual vulnerability assessments, including "any systemic scans or reviews of information systems reasonably designed to identify publicly known security vulnerabilities" in information systems based on the risk assessment.[32]

As with the NYDFS requirement, as drafted, the scope of this requirement is too broad, overly prescriptive in the required frequency, and does not adequately describe the processes by which systems and applications are tested. The scope of the systems subject to the annual penetration test requirement – based on the risk assessment – does not adequately clarify that a financial institution should conduct penetration testing and vulnerability assessments *as appropriate to the relevant risks*. Further, while penetration testing is a useful security tool, it is not appropriate for all systems and scarce testing resources should be tailored to where they can have the greatest impact—including high risk Internet-accessible systems. FTC-regulated financial institutions should be permitted to develop a testing program based on its perceived risks (e.g., annual tests on critical systems and applications, with less frequent tests on new or updated systems and applications). Relatedly, these institutions should be permitted to use methods that rely on different techniques but have similar intent and may (in certain cases) be equally or more effective, such as red teaming. This is especially critical for smaller companies that have limited resources.

As such, we propose following the FFIEC's approach for testing requirements. Similar to the requirements discussed above, the FFIEC requirements take a flexible, risk-based approach, permitting regulated financial institutions to identify and prioritize key systems for testing, use a variety of testing methods as deemed appropriate, and test "regularly" without a prescribed timeline. In particular, under the Interagency Guidelines, FFIEC-regulated financial institutions are instructed to "[r]egularly test the key controls, systems and procedures of the information security program. The frequency and nature of such tests should be determined by the [institution's] risk assessment. Tests should be conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs."[33]

---

[31] 16 C.F.R. § 314.4(d)(1) (as proposed to be amended).

[32] *Id*. § 314.4(d)(2) (as proposed to be amended).

[33] 12 C.F.R. pt. 30, app. B, § III(C)(3).

The FFIEC IT Examination Handbook, particularly in the Information Security Booklet, elaborates on factors financial institutions should *consider* in developing its testing, assessment, and monitoring program, as opposed to setting forth prescriptive mandates. For example:

- "Management should ascertain that the information security program is operating securely, as expected, and reaching intended goals by doing the following: [1] Testing and evaluating through self-assessments, tests, and audits with appropriate coverage, depth, and independence[; 2] Aligning personnel skills and program needs[; and 3] Establishing and implementing a reporting process that includes the assembly and distribution of assurance reports that are timely, complete, transparent, and relevant to management decisions."[34]
- "Periodic self-assessments typically should be performed by the organizational unit being assessed."[35]
- "The frequency and scope of a penetration test should be a function of the level of assurance needed by the institution and determined by the risk assessment process."[36]
- "[T]he frequency of the performance of vulnerability assessments should be determined by the risk management process. Scanners and other tools can be run continuously, generating metrics that are reported and acted upon continuously. Alternatively, they can be run periodically."[37]
- "Audits should review every aspect of the information security program, the environment in which the program runs, and outputs of the program. Audits should assess the reasonableness and appropriateness of, and compliance with, policies, standards, and procedures; report on information security activity and control deficiencies to decision makers; identify root causes and recommendations to address deficiencies; and test the effectiveness of controls within the program. Internal audit should track the results and the remediation of control deficiencies reported in audits and additional technical reviews, such as penetration tests and vulnerability assessments."[38]
- "E-banking introduces information security risk management challenges. Financial institution directors and senior management should ensure the information security program addresses these challenges and takes the appropriate actions. . . . [including: (1)] Implement[ing] security controls sufficient to manage the unique security risks confronting the institution. Control considerations include: . . . [r]apid identification and mitigation of vulnerabilities . . . . [and (2)] Monitor[ing] and independently test[ing] the effectiveness of the institution's security program."[39]

---

34 FFIEC IT Examination Handbook, Information Security Booklet, § IV.A.

35 *Id.* § IV.A.2(a).

36 *Id.* § IV.A.2(b).

37 *Id.* § IV.A.2(c).

38 *Id.* § IV.A.2(d).

39 FFIEC IT Examination Handbook, E-Banking Booklet at 26-27 (Aug. 2003).

This type of risk-based approach provides regulated entities with the necessary flexibility to design their monitoring and testing programs based on their risk assessments and in consideration of safety and soundness principles (including resource allocation), while still providing sufficient detail to convey regulator expectations regarding the thoroughness, diversity, and regularity of expected testing, auditing, and monitoring. We therefore recommend that the FTC adopt this approach.[40]

* * * * *

We appreciate the opportunity to comment on the proposal. The Associations commend the Commission's efforts to ensure that all Americans' personal information is protected. However, as the FTC seeks to make extensive revisions to its Safeguards Rule, it should do so in a manner that harmonizes new requirements with existing rules. Such harmonization will optimize cyber professionals' time on frontline defense versus reconciling another topically similar, but semantically different regulatory regime, increase consumer understanding concerning the protection requirements for their data, and ultimately result in greater security across the entire ecosystem. As such, and for the reasons outlined above, the FTC should model the revised Safeguards Rule on the widely-used and risk-based FFIEC Interagency Guidelines, IT Examination Handbook and other supplementary guidance, and map

---

[40] While the Associations contend that the FFIEC approach is the most appropriate in this context, in the event that the FTC determines that adopting an amended version of the NYDFS regulation is its preferred approach, we recommend that the FTC revise the proposed language as follows:

> (1) Regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures, including those to detect actual and attempted attacks on, or intrusions into, information systems.
>
> (2) The monitoring and testing shall include continuous monitoring or periodic penetration testing and vulnerability assessments. Absent <u>other reasonably</u> effective ~~continuous~~ monitoring or other systems to detect, on an ongoing basis, changes in information systems that may create vulnerabilities, you shall conduct <u>the following, at a minimum, with respect to your information systems determined to be high risk pursuant to the risk assessment</u>:
>
> > (i) ~~Annual~~ <u>Periodic</u> penetration testing of your <u>Internet-accessible</u> ~~information~~ systems ~~determined each given year based on relevant identified risks in accordance with the risk assessment~~; and
> >
> > (ii) ~~Bi~~annual vulnerability assessments, including any systemic scans or reviews of information systems reasonably designed to identify publicly known security vulnerabilities in your information systems ~~based on the risk assessment~~.

We also recommend that the FTC revise the definition of penetration testing to more accurately reflect real-life testing processes, as follows:

> Penetration testing means a test methodology in which assessors attempt to circumvent or defeat the security features of an information system by ~~attempting~~ <u>simulating</u> penetration of databases or controls from outside or inside your information systems.

the revised rule to the FSSCC Cybersecurity Profile, rather than selecting and altering provisions from the less widely adopted NYDFS cybersecurity regulations and NAIC Model Law.

If you have any questions, please feel free to contact Josh Magri (Josh.Magri@bpi.com), Angelena Bradfield (Angelena.Bradfield@bpi.com), Rob Rowe (rrowe@aba.com), Bill Boger (wboger@aba.com), and/or Melissa MacGregor (mmacgregor@sifma.org).

The Undersigned Associations of:

The American Bankers Association (ABA)
The Bank Policy Institute (BPI)- BITS
SIFMA

ANNEX A

The Bank Policy Institute/Business Innovation Technology Security. BPI is a nonpartisan public policy, research and advocacy group, representing the nation's leading banks. Our members include universal banks, regional banks and the major foreign banks doing business in the United States. Collectively, they employ nearly 2 million Americans, make 72% of all loans and nearly half of the nation's small business loans and serve as an engine for financial innovation and economic growth.

The Business-Innovation-Technology-Security division (better known as BITS), is a division of BPI that brings BPI members and BITS affiliate members, such as insurers, asset managers, sector utilities, etc., together in an executive-level forum to discuss and promote current and emerging technology, foster innovation, reduce fraud and improve cybersecurity and risk management practices for the nation's financial sector.

The American Bankers Association. The ABA is the voice of the nation's $18 trillion banking industry, which is composed of small, regional, and large banks that together employ more than 2 million people, safeguard nearly $14 trillion in deposits, and extend more than $10 trillion in loans.

The Securities Industry and Financial Markets Association. SIFMA brings together the shared interests of hundreds of securities firms, banks, and asset managers. SIFMA's mission is to support a strong financial industry, investor opportunity, capital formation, job creation, and economic growth, while building trust and confidence in the financial markets. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA).