MBa®

MORTGAGE BANKERS ASSOCIATION

July 30, 2019

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue NW
Suite CC-5610 (Annex B)
Washington, D.C. 20580

Re: Safeguards Rule, 16 CFR Part 314, Project No. 14507

Dear Ms. Tabor,

The Mortgage Bankers Association ("MBA")[1] appreciates the opportunity to comment on the Federal Trade Commission's ("FTC" or the "Commission") notice of proposed rulemaking ("NPRM") regarding *Standards for Safeguarding Customer Information* ("Safeguards Rule").[2] The Commission faces a significant challenge in addressing aging standards in light of technological developments and an increase in cyber threats. It is imperative that the FTC maintains its original "process-based" approach to ensure businesses retain the flexibility necessary to adapt to rapidly evolving attacks and to adopt developing technologies to protect consumer information.

Under the Gramm-Leach-Bliley Act ("GLBA") financial institutions are obligated to respect the privacy of their customers and to protect the security and confidentiality of those customers' nonpublic personal information.[3] The FTC issued the Safeguards Rule in 2002 to provide details on implementing this statutory mandate.[4] The Safeguards Rule provided general requirements and guidance for an information security program without imposing rigid, checklist-like descriptions of a program's components. This process-based approach provided valuable flexibility in the midst of rapidly evolving technological capabilities.

Seventeen years later, the FTC has proposed expanding coverage of the Safeguards Rule and several new additional requirements.[5] While the FTC has laudably aimed to maintain the general

[1] The Mortgage Bankers Association ("MBA") is the national association representing the real estate finance industry, an industry that employs more than 280,000 people in virtually every community in the country. Headquartered in Washington, D.C., the association works to ensure the continued strength of the nation's residential and commercial real estate markets, to expand homeownership, and to extend access to affordable housing to all Americans. MBA promotes fair and ethical lending practices and fosters professional excellence among real estate finance employees through a wide range of educational programs and a variety of publications. Its membership of over 2,300 companies includes all elements of real estate finance: mortgage companies, mortgage brokers, commercial banks, thrifts, REITs, Wall Street conduits, life insurance companies, and others in the mortgage lending field. For additional information, visit MBA's website: www.mba.org.
[2] 84 Fed. Reg. 13158 (April 4, 2019). ("Proposed Rule").
[3] 15 U.S.C. § 6801(a).
[4] *See* Standards for Safeguarding Information, Final Rule, 67 Fed. Reg. 36484 (May 23, 2002).
[5] *See* generally, Proposed Rule.

process-based approach, there are few instances where the FTC's proposed changes should be tailored to ensure financial institutions remain adaptable. The sections below offer comments on specific issues raised by the FTC's NPRM.

I. The Safeguards Rule should provide a safe harbor for covered entities that adopt a cybersecurity framework.

The National Institute of Standards and Technology ("NIST") developed its Cybersecurity Framework ("CSF") as a means to provide guidance to entities on how to protect their computer systems.[6] Alongside NIST, multiple other frameworks addressing similar issues arose.[7] The Safeguards Rule appropriately has not imposed any particular framework on financial institutions.

The CSF and other frameworks have several components that must be assessed individually for implementation. Entities who are considering those frameworks make assessments based on the size of their business and the nature of their transactions. In many instances companies employ multiple frameworks, selecting particular components and investing greater resources into data security.[8] Companies will employ additional access controls, compartmentalize their business processes, and adapt their security protocols as they grow in size. Businesses must also expend a significant amount of resources to hire the appropriate personnel, establish policies, and implement those policies within the context of their needs. The resources required and the cost involved vary significantly depending on the size of the business and its consumer-base.

For these reasons and others, the FTC is correct in not prescribing a particular framework. The FTC should, however, consider modifying the Safeguards Rule so that financial institutions that use the NIST CSF would be in *de facto* compliance with the Rule. This safe harbor should protect those that adhere to the recognized framework but also make clear that adherence to any other framework or the rule's stated requirements is still in compliance so long as the requirements of the FTC's rule are met.

II. The definition of "financial institution" should remain within the FTC's purview.

When the Privacy Rule was promulgated in 2000, the FTC determined that companies engaged in activities that are "incidental to financial activities" would not be considered "financial institutions."[9] Rather, the FTC felt adding the requirement that entities be "significantly engaged" in financial activity was the appropriate decision.[10] This had the practical impact that any decisions

---

[6] NIST Cybersecurity Framework 1.1, available at https://www.nist.gov/cyberframework.
[7] *See generally*, Payment Card Industry Data Security Standard ("PCIDSS"), ISO 27001, and others.
[8] *See generally,* Trends in Security Framework Adoption: A Survey of IT and Security Professionals. Tenable Network Security (March 2016), *available at* https://www.tenable.com/whitepapers/trends-in-security-framework-adoption. Key findings indicate 44 percent of those surveyed use more than one security framework.
[9] *See* 16 C.F.R. § 313.3(k); *see also* 65 Fed. Reg. 33646, 33654 (May 24, 2000).
[10] 16 C.F.R. § 313.3(k).

made by the Federal Reserve Board ("FRB") to expand the scope of "incidental activities" would not impact the Safeguards Rule and its subject entities.[11]

The Proposed Rule puts forth the question of whether the FTC should adopt the broader "incidental activities" definition. Unfortunately, this broader definition would produce uncertainty that relies upon decisions made by the FRB for purposes that may be unrelated to privacy and data security. Businesses seeking to innovate would be subject to an unknown factor that could have a significant impact on the business needs of entities not typically covered by the FRB's rules. Though the FRB has only expanded the definition of "incidental activities" once to date, it is free to expand this definition as it sees fit. As financial technology evolves, there is significant potential for an emerging business model (or established one that attracts FRB attention) to be brought under the Safeguards Rule without properly assessing the impact. Giving the FRB decision-making authority on what entities the Safeguards Rule should also apply to would have significant consequences. It is unlikely that the FRB would fully consider the implication of its decision on regulatory matters outside of its authority.

The Commission is the proper agency to determine which covered entities should be subject to the Safeguards Rule. As authors of the Rule and primary regulator for nonbank financial institutions on this matter, the FTC is best situated to assess new business models and whether they warrant being deemed "significantly engaged" with financial activities for coverage under the Safeguards Rule. The FTC should retain its original definition of "financial institution" as it appears in the FTC's Privacy Rule to ensure any new business models are properly assessed by the appropriate regulator.[12]

III. The FTC should tailor their Incident Response Plan requirement to account for the diversity of covered entities and adopt the model definition of a "cybersecurity event."

a. Incident Response Plan

While well intentioned, the FTC's proposal to require financial institutions to establish incident response plans must be fine-tuned due to the breadth of entities potentially subject to this requirement. The proposal expects incident response plans to be "designed to promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity, or availability of customer information" in the financial institution's possession.[13] Focusing on prompt and appropriate responses, along with mitigation efforts, the proposal sets seven goals.[14]

---

[11] *See* 65 Fed. Reg. 80735 (Dec. 22, 2000); 12 C.F.R. § 225.86(d)(1). Specifically, this has occurred once, as the Federal Reserve Board determined that acting as a "finder" is an activity that is "incidental to a financial activity." The Federal Reserve Board defined "finding" as bringing together buyers and sellers of products or services for transactions that the buyers and sellers themselves negotiate and consummate.

[12] 12 C.F.R. § 1016.3(l).

[13] Proposed 16 C.F.R. § 314.4(h).

[14] *Id.*

The proposed IRP sets a checklist of items that has failed to account for the size and scope of the covered entity. These goals would be ambitious for a well-equipped institution. However, institutions of smaller sizes may not necessarily be capable of addressing all seven of the proposed goals.

Any proposed IRP should address the nature of the information involved and the breadth of the event that triggered the IRP in the first place. Failing to do so would have the potential to cripple small businesses under the pressure of repeatedly checking the boxes for potentially harmless events. For example, keystroke errors would require meticulous documentation that requires identifying the weakness that caused the error (in this case poor typing skills leading to inadvertent mailings or misfiled documentation). Consequently, a small business would be required to document every incident and evaluate and revise their IRP in light of such events. A large business would face the same dilemma, but its response (like the small business) would vary on the volume of issues and its response appetite. The Proposed Rule does not account for an issue that could require a varying response dependent on the size and nature of the business. Rather it proposes to require *every* entity to check off *each* goal, potentially incentivizing a lowest common denominator approach. The FTC should modify the requirement to establish a written IRP by incorporating the understanding of an institution's size and scope, as well as the nature of business being conducted. Events that trigger the IRP, should be based upon a volume threshold appropriate for the entity's size and the scope of the event.

b. Security Event

An incident response plan naturally raises the question of what constitutes a "security event." In defining "security event," the proposal casts an excessively large net that will create long-standing negative effects. The proposal suggests that a "security event" be defined as "an event resulting in unauthorized access to, or disruption or misuse of, an information system or information stored on such information system."[15] By using the term "security event" rather than "cybersecurity event," the definition arguably envelopes all data, including encrypted or de-identified information.

There are significant concerns revolving around incorporating harmless data with this broad definition. Namely, this would have the potential to skew assessments and audits that must be conducted under the proposed changes. Resources and attention would be diverted to address harmless issues with immaterial consequences, potentially to the detriment of severe issues. With the proposed changes requiring businesses to adjust their information security program to incorporate mandated assessments and audits, the proposal seems to suggest a paradigm where business would be forced to divert their focus to harmless concerns and away from more critical issues.

The Proposed Rule defines "security event," in part, based on the insurance data security model law issued by the National Association of Insurance Commissioners.[16] The Model Law, however,

[15] Proposed 12 C.F.R. § 314.2(c).
[16] National Association of Insurance Commissioners, *Insurance Data Security Model Law* (2017), *available at* https://www.naic.org/store/free/MDL-668.pdf. ("Model Law").

focuses on a "cybersecurity event" and incorporates an exemption the FTC has foregone. This exemption states that an event "does not include the unauthorized acquisition of Encrypted Nonpublic Information if the encryption, process or key is not also acquired, released or used without authorization."[17] The exemption is a logical extension of what constitutes a threat to the security of a customer's information. A business that takes the step to encrypt a customer's information has effectively safeguarded that data as long as the encryption key remains protected. Encryption, by definition (even as proposed), constitutes the "transformation of data into a form that results in a low probability of assigning meaning without the use of a protective process or key."[18] Practically speaking, data that is encrypted is unreadable. If customer information is encrypted, anyone who obtains that data and fails to obtain the protective key will be unable to read any customer information.

The Commission has stated that it believes financial institutions should "still engage in its incident response procedures to address the failures in its information security that allowed such events to occur."[19] While understandable, there are more efficient methods to achieving this goal that don't trigger an IRP response that is typical for large-scale cybersecurity events. A more appropriate method for engaging in an incident response for harmless issues is to acknowledge the need for a bifurcated IRP process that accounts for unsecure information and minor paper-related breaches. A targeted response to a harmless individual error is far more appropriate than a comprehensive review of policies and procedures (as required under an IRP as proposed). Essentially, an event that exposes encrypted information or involves a minor paper-related issue shouldn't constitute a full incident response, but rather a more nuanced process tailored to the individual entity because no consumer harm has occurred.

The current Proposed Rule's definition of "security event" would encompass harmless issues. This has the potential to skew the proposed penetration testing, risk assessments, and audit trails. Invariably, this would harm the routine review and evaluation of an information security program by focusing on issues that do not necessarily harm consumers, while taking focus off more serious concerns. The FTC should adopt the NAIC Model Law definition of "cybersecurity event" and its accompanying exemption, rather than the overly broad proposed definition of "security event."

IV. The FTC should provide greater clarity to its definition of "encryption."

The FTC adds several provisions to the elements of an information security program. Notably, one of the many risk assessment controls that must be designed and implemented includes data encryption. The proposal requires that entities "protect by encryption all customer information held or transmitted by you both in transit over external networks and *at rest*."[20] Encryption is defined as the "transformation of data into a form that results in a low probability of assigning

[17] *Id*. at § 3(D).
[18] Proposed 12 C.F.R. § 314.2(e).
[19] *See* Proposed Rule at p. 23.
[20] Proposed 12 C.F.R. § 314.4(c)(4). (Emphasis added).

meaning without the use of a protective process or key."[21] While the FTC has avoided requiring any particular technology or technique, the proposal raises two issues.

First, the focus on encryption is misguided. The Proposed Rule requires the encryption of all customer information in transit and at rest. For purposes of safeguarding customer information, data at rest is a point of concern, however the transmission of data that is a key vulnerability. Data at rest is protected at multiple levels. The Proposed Rule itself mandates the implementation of access controls, which would protect any data at rest. As a practical matter, storage devices typically have native encryption capabilities. A requirement that imposes encryption for data at rest creates a potentially confusing redundancy that limits usability. Data that is routinely accessed must be indexed by systems to ensure prompt responses. Encryption significantly raises the difficulty of indexing. Additionally, the lack of clarity raises questions on whether single files would require encryption or if single storage devices require encryption. Rather than implement this confusing redundancy, resources would better be served encrypting data in transmission while implementing robust access controls for data at rest. Data is most vulnerable in transmission and is considered the most common security challenge due to the difficulty in understanding which parties have access to a moving target. The industry standard, Payment Card Industry Data Security Standard ("PCI DSS"), was established in part due to concerns over the transmission of cardholder data. The FTC should define "encryption" to focus on the necessity to protect data in transit.

Second, the proposal's attempt to provide flexibility raises concerns. To the extent an entity determines that encryption is "infeasible," they may instead secure the information using "effective alternative compensating controls…"[22] Though the FTC is seeking to model this requirement after the Health Insurance Portability and Accountability Act ("HIPAA") Security Rule,[23] it creates a different standard for variation. Specifically, the standard under HIPAA rests on "reasonableness" as opposed to "feasibility." Simply because encryption may be feasible, or could be done in practice, does not mean that encryption would be the *reasonable* route for businesses of varying sizes. The FTC should model their approach to flexibility after HIPAA, and allow entities to secure information by other effective means if encryption is "unreasonable."

V. The FTC should provide greater clarity to its definition of "multi-factor authentication."

An additional access control being proposed is required multi-factor authentication ("MFA"). Specifically, the proposal would mandate financial institutions "implement multi-factor authentication for any individual accessing customer information" or "internal networks that contain customer information."[24] In order to properly implement MFA, the FTC should provide

[21] Proposed 12 C.F.R. § 314.2(e).
[22] Proposed 12 C.F.R. § 314.4(c)(4).
[23] *See* 45 C.F.R. § 164.306(d)(3).
[24] Proposed 16 C.F.R. § 314.4(c)(6).

more clarity to this requirement and address security necessities as opposed to extraneous access controls.

Many entities, including private businesses and government entities, make use of standard access controls. Individuals, or authorized users, access their workstations via a login ID and password. Certain databases require additional credentials, while some entities make use of physical keys. However, through the use of MFA, single sign-on ("SSO") has become increasingly prevalent. SSO is an authentication process that allows users to access multiple applications with one set of login credentials. Where an authorized user is accessing various resources within an entity's local area network, SSO is highly useful. Coupling SSO with MFA eliminates redundancies, improves productivity, streamlines workflow, minimizes phishing, and ensures authorized use. Under the Proposed Rule, it is not clear that an entity could make use of SSO, even in conjunction with MFA. Additionally, the Proposed Rule refers to "internal networks" without consideration for remote access. The FTC should provide greater clarity on MFA by indicating that the control is necessary for access to a single local area network, and not necessarily for each individual database that must be accessed. Similarly, on-site access to internal networks should be clearly differentiated from accessing an entity's local area network via an external network.

***

MBA appreciates the consideration of these comments and the Commission's willingness to engage with stakeholders in considering changes to its Safeguards Rule. MBA looks forward to continuing to work with the FTC and with other state and federal regulators on data protection requirements applicable to financial institutions. Should you have any questions or wish to discuss any aspect of these comments, please contact Justin Wiseman, Associate Vice President and Managing Regulatory Counsel (jwiseman@mba.org) or Sheraz Syed, Regulatory Associate (ssyed@mba.org).

Sincerely,

Pete Mills
Senior Vice President
Residential Policy and Member Engagement
Mortgage Bankers Association