MBa®

MORTGAGE BANKERS ASSOCIATION

October 31, 2023

Kemba E. Walden, Acting National Cyber Director
Office of the National Cyber Director, Executive Office of the President
1600 Pennsylvania Ave NW, Washington, DC 20500

RE: Request for Information on Cyber Regulatory Harmonization [RIN: 0301-AA00]

Dear Ms. Walden,

Thank you for the opportunity to comment on the Office of the National Cyber Director (ONCD) Request for Information (RFI) on cyber regulatory harmonization. MBA members are strong proponents of protecting consumer data.[1] Maintaining up-to-date data security practices remains a top priority for the real estate finance industry. Since the Gramm-Leach Bliley Act (GLBA) passed in 1999, the financial services sector has operated under an effective and comprehensive privacy and data security regime. Protecting consumer financial data is a cornerstone of the trust customers place in those with whom they do business. The financial service industry was identified as a critical infrastructure sector under Presidential Policy Directive 21 and MBA members take that responsibility seriously.[2] MBA supports the harmonization of cybersecurity regulations through a singular Federal data security regime. A single regime strengthens execution and is in the best interest of consumers and financial services providers alike. Until that is achieved, federal and state governments should work to minimize the cost of complying with multiple data security laws where doing so will not compromise consumer protection.

[1] The Mortgage Bankers Association (MBA) is the national association representing the real estate finance industry, an industry that employs more than 400,000 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 more than 2,200 companies includes all elements of real estate finance: independent mortgage banks, mortgage brokers, commercial banks, thrifts, REITs, Wall Street conduits, life insurance companies, credit unions, and others in the mortgage lending field. For additional information, visit MBA's website: www.mba.org.

[2] Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience, the White House, Office of the Press Secretary (Feb. 12, 2013).

Our members devote significant resources complying with federal data security regulations. These regulations, requirements, and guidelines are enforced by dozens of regulatory bodies exercising overlapping jurisdiction, including but not limited to the Securities and Exchange

Commission, the Federal Deposit Insurance Corporation, the Federal Reserve System, the Federal Trade Commission, the National Credit Union Administration, the Office of the Comptroller of the Currency, the Financial Industry Regulatory Authority, and the Consumer Financial Protection Bureau. These requirements govern all areas of data protection.

Financial firms expend time and resources to safeguard consumer data, protect data from malicious actors, and defend against adversaries that target financial institutions. Financial institutions develop data security plans, train their front-line employees in best practices, and hire experts to implement protective measures for the mortgage industry. A data breach or system disruption can have company-threatening impacts as it could result in lost business, reputational harm, and potentially harsh legal and regulatory consequences.

Although a company offering financial services might serve customers in many states, these organizations typically have one technology and security infrastructure that serves all of their customers. In other words, a company does not create a data security program for each state. Doing so would be wildly impractical and ineffective. Security experts create a security program based on the risks to their organization and customers. They then evaluate the compliance of their chosen security program with the various federal and state requirements. Compliance and technology officers must navigate a web of federal and state laws and regulations to ensure compliance. This regime creates unnecessary costs to companies attempting to address shared concerns of consumer protection and can detour resources that should be focused on executing to a single federal regime.

I. MBA Data Protection Principles

MBA continues to support a federal response to data security threats that must be tailored in a way that is technologically neutral and fosters innovation. MBA previously published Data Protection Principles.[3] These principles are meant to provide high-level guideposts for lawmakers and regulators to address these challenges.

Consumer data security should be addressed at the federal level. Currently, data security law is created at both the state and federal levels. The core of the problem is that multiple states are setting data security standards with little to no coordination. Navigating this web of laws increases companies' compliance costs without effectively furthering the central concern of consumer safety. A patchwork of state laws and federal regulations confuses

[3] Mortgage Bankers Association, MBA Data Protection Principles (Aug. 2019), https://www.mba.org/docs/default-source/policy/state-relations/mba-data-protection-principles.pdf?sfvrsn=7276ed6_1.

businesses and ultimately harms consumers. The internet does not stop at a state border, and Congress should establish a framework that encourages compliance and allows for

flexibility. The recent executive order by the White House addressing the use of artificial intelligence is an example of appropriately addressing a national issue at the federal level.[4]

In enacting national data security laws, regulators should ensure that these rules can be crafted in ways that respect the different challenges faced by different industries. Each industry sector presents a unique set of characteristics and risks that should be addressed separately on the federal level. The mortgage industry handles a large amount of data provided by consumers. This raises a different set of concerns than third-party service providers who hold both company and consumer data, which itself is separate from critical energy infrastructure which holds little consumer data but does present national security concerns. No one-size-fits-all solution exists for industries that vary widely in size and nature.

To accommodate emerging technologies, federal and state governments should adopt a risk-based framework approach to regulating. As technology advances, so do consumer expectations about how it works. The full implications or possibilities of new technology may not be apparent until the industry, consumers, and regulators grow familiar with these changes. This is a natural gap since innovation necessarily comes first. Often, the regulatory response arises during the time between the introduction of new technology and consumers fully understanding its beneficial uses and inherent trade-offs. This can most evidently be seen in the recent consumer interest in generative artificial intelligence and large language models. Several states are moving to regulate this technology before its full implications – both benefits and risks – can be understood. These regulations risk disrupting market-driven innovations or failing to capture the risks actually presented by this innovation. While this technology is developing, federal and state governments should promote third-party risk-management frameworks to foster responsible innovation. The NIST AI Risk Management Framework, focusing on frequent testing and risk management, has been particularly instructive.[5]

Any framework should remain technologically neutral to ensure businesses can remain flexible and adapt to evolving threats. This principle of technological neutrality should be applied to data security laws. Many states and some federal agencies have started to require that companies adopt particular data security practices. For example, the Federal Trade Commission Safeguards Rule (Safeguards Rule) and New York Department of Financial Services Cybersecurity Regulations (NY DFS Rule) require companies to adopt specific

[4] FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence, the White House (Oct. 30, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/.

[5] National Institute of Standards and Technology, U.S. Dep't of Commerce, Artificial Intelligence Risk Management Framework (AI RMF 1.0) (Jan. 2023), https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.

technology and functionality.[6] While some of these specific practices may be adopted by some companies, requiring them is misguided. A security framework must not be prescriptive or static. These determinations are best left to market participants, who are better positioned

to react to technological changes and specific business circumstances while acting within the guidelines.

II. Harmonizing Data Security Requirements

Data security requirements are effectively set by whichever state creates the most stringent data security rules. For example, both the FTC Safeguards Rule and the NY DFS Rule require covered entities to report unauthorized access to information systems.[7] However, the NY DFS Rule requires reporting attempted or successful unauthorized access to *electronic* information, whereas the FTC Safeguards Rule requires reporting attempts to access *electronic* or *physical* information systems. Given the wider scope of the FTC Safeguards Rule, companies may respond to this incongruence by following the FTC requirements and overreport events to the NY DFS.

This dynamic becomes untenable when conflicts between laws do arise. If data security laws conflict, firms could be forced to maintain separate information security compliance programs based on each regulation. This would add a considerable amount of time to monitor and make it difficult for companies to demonstrate compliance. For example, the NY DFS Rule requires companies to maintain an audit trail related to financial transactions for five years and to maintain an audit trail of "cybersecurity events" for three years.[8] The FTC Safeguards Rule requires that companies minimize the retention of data and dispose of consumer information within two years of the data being used to provide a product or service.[9] Although there are exceptions to this rule that could ameliorate this conflict, navigating several potentially conflicting data retention requirements increases the complexity of managing a data security program.

Increasingly prescriptive data security rules from a state, while well intentioned, may be misguided and have unintended consequences. For example, the NY DFS Rule and the Safeguards Rule both require companies to implement multi-factor authentication (MFA). While the Safeguards Rule allows companies to use a risk-based approach to decide which systems require MFA, the recent version of the NY DFS Rule requires MFA for remote access to all third-party applications where personal information is accessible.[10] This change effectively requires covered entities to switch their systems to comply with the NY DFS rule. The consequences of this fall most heavily on smaller firms. Companies that do not frequently

[6] 16 C.F.R. Part 314; 23 N.Y.C.R.R. § 500.
[7] 16 C.F.R. § 314.2(p); 23 N.Y.C.R.R. § 500.01(d).
[8] 23 N.Y.C.R.R. § 500.06(b).
[9] 16 C.F.R. § 314.4(c)(6).
[10] 16 C.F.R. § 314.4(c)(5); 23 N.Y.C.R.R. § 500.11(b)(1).

interact with data security laws face the heaviest costs of compliance and must navigate these different laws while addressing the underlying security concern. The industry supports one set of federal rules that preempts state law and preserves flexibility for companies to address a myriad of concerns.

Enforcement by different states and federal agencies can create conflicts in the law even if state and federal data security requirements are facially similar. Agencies may interpret similar requirements differently. This can cause compliance issues where different regulators place emphasis or create separate requirements for different aspects of data security. For example, both the NY DFS Rule and the Safeguards Rule require an individual to act as a Chief Information Security Officer.[11] Although this individual must be qualified in both cases, there is nothing explaining what makes an individual qualified to serve as a CISO. This creates the risk that examiners will read the same position to require different credentials.

The Federal Financial Institutions Examination Council (FFIEC) has attempted to address the problems identified in this section by publishing their Information Security Standards, Self-Assessment Tool, and Information Security Booklet. MBA believes these artifacts have the potential to deliver significant value to regulated entities and our consumers. In fact, MBA has utilized the FFIEC Cybersecurity Self-Assessment Tool in our education courses to help lending organizations to understand their risk profile and to implement appropriate cybersecurity practices. These tools also have the benefit of educating the entities conducting cybersecurity reviews on behalf of the constituent regulatory organizations. However, these standards and tools have only been adopted by participating FFIEC regulatory bodies. On the federal level these artifacts do not guide the FTC, SEC and other regulators that also have oversight over financial institutions. Nor do the standards or tools cover examinations by state regulators or attorneys general. The potential benefit of a collaborative approach is significant, but only if the vast majority of regulators defer to the collaborative product.

III. Data Security Compliance Costs

Companies spend a considerable amount of resources to meet data security requirements. Managing these programs requires internal resources, contractor support, and numerous tools to meet legal requirements. In addition to centralizing decisions about data security rules and guidelines, regulators and lawmakers should consider other ways to lower the cost of administering these programs without harming consumer security.

Current data security requirements give companies responsibility for conducting third-party vendor oversight. However, this leads to multiple companies conducting oversight of the same vendor. Additionally, companies often rely on several third-party vendors for their business.

[11] 16 C.F.R. § 314.4(a) ("[Covered entities shall designate] a qualified individual responsible for overseeing and implementing your information security program and enforcing your information security program"); 23 N.Y.C.R.R. § 500.04 ("[e]ach Covered Entity shall designate a qualified individual responsible for overseeing and implementing the Covered Entity's cybersecurity program and enforcing its cybersecurity policy…").

Taken together, companies must oversee dozens or hundreds of vendors that are also overseen by all of those vendor's other clients. This creates massive costs without enhancing consumer protection. Firms have turned to third-party assessments, such as SOC 1 and SOC 2 reports, to evaluate the data security of third-party firms. However, this is a voluntary practice and does not provide any legal safeguards to the firms relying on these assessments. The federal government should create some form of third-party accreditation for data security vendors and a legal safeguard for companies relying on those assessments.

IV. Conclusion

MBA greatly appreciates the opportunity to comment on this RFI on cybersecurity harmonization. Should you have questions or wish to discuss this issue further, please contact Gabriel Acosta at gacosta@mba.org or Rick Hill at rhill@mba.org.

Sincerely,

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

APPENDIX

Response to Specific RFI Questions

Question 1: Conflicting, mutually exclusive, or inconsistent regulations – If applicable, please provide examples of any conflicting, mutually exclusive, or inconsistent Federal and SLTT regulations affecting cybersecurity – including broad enterprise-wide requirements or specific, targeted requirements - that apply to the same information technology (IT) or operational technology (OT) infrastructure of the same regulated entity. Be as clear, specific, and detailed as possible.

Data security requirements are effectively set by whichever state creates the most stringent data security rules. For example, both the FTC Safeguards Rule and the NY DFS Rule require covered entities to report unauthorized access to information systems.[12] However, the NY DFS Rule requires reporting attempted or successful unauthorized access to *electronic* information, whereas the FTC Safeguard Rules require reporting attempts to access *electronic* or *physical* information systems. Given the wider scope of the FTC Safeguard Rules, companies may respond to this incongruence by following the FTC requirements and overreport events to the NY DFS.

This dynamic becomes untenable when conflicts between laws do arise. If data security laws conflict, firms could be forced to maintain separate information security compliance programs based on each regulation. This would add a considerable amount of time to monitor and make it difficult for companies to demonstrate compliance. For example, the NY DFS Rule requires companies to maintain an audit trail related to financial transactions for five years and to maintain an audit trail of "cybersecurity events" for three years.[13] The FTC Safeguards Rule requires that companies minimize the retention of data and dispose of consumer information within two years of the data being used to provide a product or service.[14] Although there are exceptions to this rule that could ameliorate this conflict, navigating several potentially conflicting data retention requirements increases the complexity of managing a data security program. Moreover, resources expended in managing divergent data security and privacy standards do not provide greater consumer protection and would be better deployed executing to a single robust federal standard.

Increasingly prescriptive data security rules from a state, while well intentioned, may be misguided and have unintended consequences. For example, the NY DFS Rule and Safeguards Rule both require companies to implement multi-factor authentication (MFA). While the Safeguards Rule allows companies to use a risk-based approach to decide which systems require MFA, the recent version of the NY DFS Rule requires MFA for remote access

[12] 16 C.F.R. § 314.2(p); 23 N.Y.C.R.R. § 500.01(d).
[13] 23 N.Y.C.R.R. § 500.06(b).
[14] 16 C.F.R. § 314.4(c)(6).

to all third-party applications where personal information is accessible.[15] This change effectively requires covered entities to switch their systems to comply with the NY DFS rule.

The consequences of this fall most heavily on smaller firms. Companies that do not frequently interact with data security laws face the heaviest costs of compliance and must navigate these different laws while addressing the underlying security concern. The industry supports one set of federal rules that preempts state law and preserves flexibility for companies to address a myriad of concerns.

Enforcement by different states and federal agencies can create conflicts in the law even if state and federal data security requirements are facially similar. Agencies may interpret similar requirements differently. This can cause compliance issues where different regulators place emphasis or create separate requirements for different aspects of data security. For example, both the NY DFS Rule and Safeguards Rule require an individual to act as a Chief Information Security Officer.[16] Although this individual must be qualified in both cases, there is nothing explaining what makes an individual qualified to serve as a CISO. This creates the risk that examiners will read the same position to require different credentials.

However, in enacting national data security laws, Congress should ensure that these rules can be crafted in ways that respect the different challenges faced by different industries. Each industry sector presents a unique set of characteristics and risks that should be addressed separately on the federal level. The mortgage industry handles a large amount of data provided by consumers. This raises a different set of concerns than third-party service providers who hold both company and consumer data, which is itself separate from critical energy infrastructure which holds little consumer data but does present national security concerns. No one-size-fits-all solution exists for industries that vary widely in size and nature.

Question 2: Use of Common Guidelines – Through the Federal Financial Institutions Examination Council (FFIEC), regulators of certain financial institutions have issued common Interagency Guidelines Establishing Information Security Standards and have developed a Common Self-Assessment Tool and an Information Security Booklet to guide examinations of entities in the financial sector.

The Federal Financial Institutions Examination Council (FFIEC) has attempted to address the problems identified in this section by publishing their Information Security Standards, Self-Assessment Tool, and Information Security Booklet. MBA believes these artifacts have the

[15] 16 C.F.R. § 314.4(c)(5); 23 N.Y.C.R.R. § 500.11(b)(1).

[16] 16 C.F.R. § 314.4(a) ("[Covered entities shall designate] a qualified individual responsible for overseeing and implementing your information security program and enforcing your information security program"); 23 N.Y.C.R.R. § 500.04 ("[e]ach Covered Entity shall designate a qualified individual responsible for overseeing and implementing the Covered Entity's cybersecurity program and enforcing its cybersecurity policy…").

potential to deliver significant value to regulated entities and our consumers. In fact, MBA has utilized the FFIEC Cybersecurity Self-Assessment Tool in our education courses to help lending organizations to understand their risk profile and to implement appropriate cybersecurity practices. These tools also have the benefit of educating the entities conducting cybersecurity reviews on behalf of the constituent regulatory organizations. However, these

standards and tools have only been adopted by participating FFIEC regulatory bodies. On the federal level these artifacts do not guide the FTC, SEC and other regulators that also have oversight over financial institutions. Nor do the standards or tools cover examinations by state regulators or state attorney general investigations. The potential benefit of a collaborative approach is significant, but only if the vast majority of regulators defer to the collaborative product.

Question 4: Third-Party Frameworks – Both the government (for example, through the NIST Cybersecurity Framework) and non-government third parties have developed frameworks and related resources that map cybersecurity standards and controls to cybersecurity outcomes. These frameworks and related resources have also been applied to map controls to regulatory requirements, including where requirements are leveled by multiple agencies.

Current data security requirements give companies responsibility for conducting third-party vendor oversight. However, this leads to multiple companies conducting oversight of the same vendor. Additionally, companies often rely on several third-party vendors for their business. Taken together, companies must oversee dozens or hundreds of vendors that are also overseen by all of those vendor's other clients. This creates massive costs without enhancing consumer protection. Firms have turned to third-party assessments, such as SOC 1 and SOC 2 reports, to evaluate the data security of third-party firms. However, this is a voluntary practice and does not provide any legal safeguards to the firms relying on these assessments. The federal government should create some form of third-party accreditation for data security vendors and a legal safeguard for companies relying on those assessments.

While AI technology is developing, federal and state governments should promote third-party risk-management frameworks to foster responsible innovation. The NIST AI Risk Management Framework, focusing on frequent testing and risk management, has been particularly instructive.