



January 9, 2023

Ms. Joanne Berman
New York State Department of Financial Services
c/o Cybersecurity Division
One State Street, New York, NY 10004

RE: Proposed Second Amendment to 23 NYCRR Part 500

Dear Ms. Berman:

Thank you for the opportunity to comment on the New York Department of Financial Services' (NYDFS) proposed second amendment to 23 NYCRR Part 500. The Mortgage Bankers Association¹ and the New York Mortgage Bankers Association² are generally not opposed to what has been presented, however, we recommend improvements to better align with federal standards and mitigate compliance costs. Our associations encourage the NYDFS to consider the following amendments to the proposed rules:

- Align proposed rules with the FTC Safeguards Rule when applicable to create consistency with federal standards.
- Amend data breach notification standard to require notification only when a successful breach of material information has occurred.
- Increase the covered entities limited exemption threshold to account for small mortgage lenders in the state.

¹ The Mortgage Bankers Association (MBA) is the national association representing the real estate finance industry, an industry that employs more than 390,000 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 2,000 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 The New York Mortgage Bankers Association, Inc. (NYMBA), is a 501(c)(6) not-for-profit statewide organization devoted exclusively to the field of real estate finance. NYMBA's rapidly growing membership is comprised of both bank and non-bank mortgage lenders and servicers, as well as a wide variety of mortgage industry-related firms. NYMBA encourages its members to engage only in sound and ethical business practices and informs its members of changes in the laws and regulations affecting the mortgage business. The association helps those engaged in or affected by the mortgage business to be better informed and more knowledgeable. It is dedicated to the maintenance of a strong real estate finance system. This involves support for a strong economy, a public-private partnership for the production and maintenance of single and multi-family homeownership opportunities, and a strong secondary mortgage market. For additional information, visit www.nymba.org

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 a comprehensive privacy and data security regime. Protecting personal information is both an existing regulatory requirement and allows MBA and NYMBA members to maintain the trust of their customers. Each year, financial firms expend significant amounts of 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.

Our association members already devote a great deal of attention to compliance and data security regulations. These regulations, requirements, and guidelines are enforced by dozens of regulatory bodies exercising overlapping jurisdiction, including but not limited to the Commodity Futures Trading Commission, 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. Many other data security regulations have been issued in accordance with the GLBA, a law specifically tailored to consider the needs of financial institutions and their customers. The GLBA's implementing regulations set strong and effective standards for the development and maintenance of comprehensive data security programs. These requirements govern all areas of data protection and consumer privacy. Greater uniformity and the alignment of state and federal standards across supervisory agencies helps lower costs and strengthen the execution of robust compliance programs for the benefit of consumers.

Therefore, we encourage NYDFS to consider the following suggested amendments to their proposed rules to reflect the substantial data privacy and cybersecurity standards our members already comply with and the infrastructure that is currently in place to protect consumer data and personal information.

FTC Safeguards Rule Compliance

The FTC Safeguard rules set data security requirements for independent mortgage bankers (IMBs) and mortgage brokers.³ These Safeguard Rules require IMBs and mortgage brokers to appoint a qualified individual to provide risk assessment reports and information on security events to the board of directors, requires encryption of consumer information and multifactor authentication, and penetration testing.⁴ These requirements match similar provisions of the proposed cybersecurity regulations. However, the proposed cybersecurity requirements are much more prescriptive than the Safeguard Rules, requiring different and sometimes conflicting compliance responses. Lack of alignment increases costs and can undermine effective execution of a cohesive compliance program. NYDFS should mirror federal requirements and create greater consistency with existing federal standards.

³ 16 C.F.R. § 314.1 (2002).

⁴ 16 C.F.R. § 314.4(c), (d), (i) (2002).

Moreover, NYDFS should consider delaying the compliance date of these changes. The FTC recently announced a delay to implementing the recent changes to the Safeguard Rules, citing concerns over the lack of qualified personnel to implement the required information security programs.⁵ Misaligned state requirements will only exacerbate this problem.

Breach Notification Standards

NYDFS' proposed amendments to Section 500.17 raise concerns for our associations because the requirements create significant compliance issues for businesses that must now report *unsuccessful* attempts to access material information. The language in Section 500.17 (a) 1 (ii) (iii) and (iv) creates a substantial burden for most businesses and will result in a deluge of reporting that will divert consumer attention and supervisory resources to instances where there was no consumer harm. A disruption or degradation of a material system does not necessarily mean that any personally identifying information (PII) has been compromised and being required to make that assessment within a 72-hour period could result in additional harm to the business. For instance, it could be a system that has a readily accessible and up to date backup so a disruption, while a nuisance, may not actually lead to harm. Moreover, deployment of ransomware against an institution does not mean that PII has been accessed or compromised. A critical part of a system could contain information that has end to end encryption and the contents would not qualify for reporting.

Most state data privacy or breach notification laws use the "without unreasonable delay" standard and permit 30-45 days to determine whether there was a breach of the system that accessed material information. It is impractical for most organizations, particularly small to medium sized businesses, to properly conclude whether the event is reportable within 72 hours.

Our associations urge NYDFS to consider making the threshold for reporting a breach a *successful* attempt to access material information. This would provide consumers with more valuable information about whether their PII has been compromised and is at risk. In addition, NYDFS should create consistency with other states and provide companies with 30-45 days to properly determine a successful breach of material information.

Covered Entity Limited Exemption Threshold

In the proposed rules, NYDFS provides a limited exemption for certain business entities and their affiliates based on indicia of size. The proposed rules provide an exemption for entities that fall into any one of the following categories:

- Covered entities and their affiliates with fewer than 20 employees and independent contractors.

⁵ FTC Extends Deadline by Six Months for Compliance with Some Changes to Financial Data Security Rule, FEDERAL TRADE COMMISSION, (Nov. 15, 2022), available at https://www.ftc.gov/news-events/news/press-releases/2022/11/ftc-extends-deadline-six-months-compliance-some-changes-financial-data-security-rule?utm_source=govdelivery.

- Covered entities and their affiliates with less than \$5,000,000 in gross annual revenue in each of the last three fiscal years from business operations.
- Covered entities with less than \$15,000,000 in year-end total assets, calculated in accordance with generally accepted accounting principles.

While NYDFS' intention is to address the compliance needs of smaller entities, it does not take into account certain business types such as mortgage finance companies. A small mortgage company that operates in the state of New York will very quickly reach any of these thresholds even though they originate a small number of loans. Rising interest rates have greatly reduced margins for small mortgage companies and has made it harder to serve New York consumers. The added cost of compliance for these rules – particularly breach notice requirements even where there is no consumer harm -- would make it difficult for mortgage companies to sustain operations in an already high cost state. We urge the NYDFS to consider raising the exemption thresholds to help small businesses within the state.

Additional Issues

Section 500.05.a.2 requires automated scans of information systems, and a manual review of systems not covered by such scans to ascertain and report vulnerabilities. Our members perform routine scans of information systems through vulnerability scanning. The scanning frequencies are based on scan type and risk factor. The proposed requirement notes that scans are required promptly after any major system changes. The terms "promptly" and "major" are subjective, and this is a concern because performing a scan after every change is cost prohibitive. We urge NYDFS to provide further clarification on the definition of a "major system change" and "promptly" to avoid an excessively broad and costly application of this requirement.

Section 500.07.b.1 mandates the use of a privileged access management (PAM) tool but does not provide assurance that the solution was implemented correctly, nor does it provide assurance that the controls supporting PAM are effective. Our associations urge NYDFS to provide guidance on the required controls or the risks that need to be managed supporting privileged access. If it is increased monitoring and/or review of logs for certain privileged access or privileged accounts, include them as requirements instead.

Section 500.11.b.2 requires the use of encryption to protect nonpublic information in transit and at rest. Our members rely on compensating controls in lieu of encryption at rest. Implementing encryption at rest for all nonpublic information housed within our environments (including third parties) would require significant resources and increase complexity on existing processes. We urge NYDFS to allow management to make the decision to use encryption using a risk-based protocol.

Section 500.14.b.2 requires companies to implement security measures to centralize logging and security event alerting. Centralized logging and security event alerting can be of concern if the requirement is taken literally. Some logging systems may not support centralization, and centralization may not be ideal in certain situations. We urge the Department to provide additional flexibility to this section to make it technically feasible.

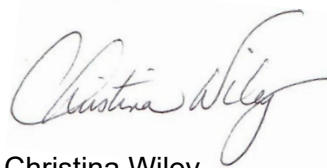
Conclusion

Once again, thank you for providing us with the opportunity to comment on proposed rules to amend 23 NYCRR Part 500. Our associations welcome the opportunity to engage with you further to develop New York's cybersecurity and data privacy standards. If you have any questions, please contact Kobie Pruitt (kpruitt@mba.org) or Christina Wiley (cwiley@nymba.org).

Sincerely,



Pete Mills
Senior Vice President
Mortgage Bankers Association



Christina Wiley
Executive Director
New York Mortgage Bankers Association