MAYER | BROWN

March 22, 2019

Legal Update

US Federal Trade Commission Proposes Prescriptive Data Security Requirements and Other Updates to Its Gramm-Leach-Bliley Act Regulations

On March 5, 2019, the Federal Trade Commission (the "FTC" or the "Commission") proposed a number of revisions to its Gramm-Leach-Bliley Act[1] ("GLBA") regulations. Most significantly, the Commission departs from its current non-prescriptive approach to data security by proposing to revise the Safeguards Rule[2] to require financial institutions to implement specific information security controls, including with respect to data encryption, multi-factor authentication, incident response planning, board reporting and program accountability. The proposal draws heavily in this regard from the cybersecurity regulations issued by the New York Department of Financial Services ("NYDFS Cyber Regulation") in March 2017[3] and the insurance data security model law issued by the National Association of Insurance Commissioners ("NAIC Model Law") in October 2017.[4] Finance companies and other non-bank lenders who are licensed in New York will need to comply with both the NYDFS Cyber Regulation and the FTC's Safeguards Rule. Because the NYDFS Cyber Regulation imposes additional requirements and has provisions similar to those of the FTC proposal but broader in scope, financial institutions complying with the NYDFS Cyber Regulation should be well-prepared if the proposed changes are adopted by the Commission.[5]

Two commissioners issued a dissenting statement on the Safeguards Rule proposal.[6]

The FTC also proposes several amendments to its GLBA Privacy Rule,[7] which requires financial institutions to inform consumers about their privacy practices and to give consumers an opportunity to opt out of the sharing of personal information with certain nonaffiliated third parties. In particular, the proposal would update the Privacy Rule to reflect a statutory exemption to the annual privacy notice requirement that was enacted by Congress in 2015. It also would streamline the Privacy Rule to focus on motor vehicle dealers (the only type of financial institution over which the Commission continues to have Privacy Rule rulemaking authority).

Finally, in order to harmonize the FTC regulations with those promulgated by the Bureau of Consumer Financial Protection (the "CFPB"), the Securities and Exchange Commission (the "SEC") and the federal banking agencies, the Commission also

proposes to expand the definition of "financial institution," both in the Safeguards Rule and the Privacy Rule, to include so-called "finders" (i.e., those who charge a fee to connect lenders with loan applicants) and other entities engaged in activities that are incidental to financial activities.

Interested parties must submit written comments to the Commission within 60 days after the proposals' publication in the *Federal Register*.

Safeguards Rule

The proposal would make four main modifications to the existing Safeguards Rule. First, it would provide covered financial institutions with more guidance on how to develop and implement specific aspects of an overall information security program, including with respect to access controls, authentication, encryption, incident response, and accountability. Second, it would exempt small businesses from certain requirements. Third, it would expand the definition of "financial institution" to include finders. Finally, it would incorporate the definition of "financial institution" and related examples into the Safeguards Rule itself, instead of by cross-reference to the Privacy Rule.

INFORMATION SECURITY CONTROLS AND PROGRAM ACCOUNTABILITY

The existing Safeguards Rule largely is non-prescriptive, in that it allows financial institutions to tailor their information programs to the size and scope of their operations and to the sensitivity and amount of customer information they collect. In its proposal, the FTC indicates that, while it generally intends to preserve this flexibility, it believes that mandating more specific requirements with respect to certain controls will benefit financial institutions by providing them with more guidance and certainty.

Chief Information Security Officer

Under the proposed rule, a financial institution would be required to designate a qualified individual responsible for overseeing, implementing and enforcing its information security program (a "Chief Information Security Officer" or "CISO"). The CISO may be employed by the financial institution, an affiliate, or a service provider. To the extent, however, that the CISO is employed by a service provider or an affiliate the financial institution would be required to: (i) retain responsibility for compliance with the Safeguards Rule; (ii) designate a senior member of its personnel responsible for direction and oversight of the CISO; and (iii) require the service provider or affiliate to maintain an information security program that protects the financial institution in accordance with the requirements of the Safeguards Rule.

Risk Assessment

A financial institution also would be required to base its information security program on a risk assessment that identifies reasonably foreseeable internal and external risks to the security, confidentiality and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information. This process also must assess the sufficiency of any safeguards in place to control these risks. The risk assessment must be in writing and include:

1. Criteria for the evaluation and categorization of identified security risks or threats faced by the institution;
2. Criteria for the assessment of the confidentiality, integrity and availability of the institution's information systems and customer information, including the adequacy of the existing controls in the context of the identified risks or threats; and

3. Requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the information security program will address the risks.

A financial institution would be required periodically to perform additional risk assessments to reexamine the reasonably foreseeable internal and external data security risks and to reassess the sufficiency of any safeguards in place to control such risks.

Performing a risk assessment is also a key element of the NYDFS Cyber Regulation and the NAIC Model Law. The risk assessment enables a financial institution to tailor its information security program to reflect the actual risks faced by the institution rather than those risks faced by the industry.

Encryption, Multi-factor Authentication and Other Safeguards

The proposal also would require a financial institution to design and implement particular safeguards to control the risks that it identifies through its risk assessment process, including:

1. Placing 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;
2. Periodically reviewing such access controls;
3. Identifying and managing the data, personnel, devices, systems and facilities that enable the institution to achieve business purposes in accordance with their relative importance to business objectives and risk strategy;
4. Restricting access at physical locations containing customer information only to authorized individuals;
5. Either: (i) encrypting all customer information held or transmitted by the institution, whether in transit over external networks or at rest; or (ii) to the extent that such encryption is not feasible, securing such customer information using effective alternate compensating controls reviewed and approved by the CISO;
6. Adopting secure development practices with respect to self-developed applications for transmitting, accessing or storing customer information;
7. Adopting procedures for evaluating, assessing or testing the security of any such applications which are externally developed;
8. Either: (i) implementing multi-factor authentication for any individual accessing customer information; or (ii) implementing reasonably equivalent or more secure access controls with respect to any individual accessing internal networks that contain customer information, provided that the CISO has approved such alternate controls in writing;[8]
9. Including audit trails within the information security program designed to detect and respond to security events;
10. Developing, implementing and maintaining procedures for the secure disposal of customer information in any format that is no longer necessary for business operations or for other legitimate business purposes, except where such information is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained;
11. Adopting change management procedures; and

12. Implementing policies, procedures and controls designed to monitor the activity of authorized users and to detect unauthorized access or use of, or tampering with, customer information by such users.

Testing and Monitoring

The proposal would require a financial institution to regularly test or otherwise monitor the effectiveness of key information security controls, systems and procedures, including those to detect actual and attempted attacks on, or intrusions into, information systems. Absent effective continuous monitoring or other systems to detect, on an ongoing basis, changes in information systems that may create vulnerabilities, a financial institution would be required to conduct:

1. Annual penetration testing of its information systems determined each given year based on relevant identified risks in accordance with the risk assessment; and
2. Biannual vulnerability assessments, including any systemic scans or reviews of information systems reasonably designed to identify publicly known security vulnerabilities based on the risk assessment.

Program Implementation

Financial institutions would be required to implement policies and procedures to ensure that their personnel are able to enact the information security program, including by:

1. Providing personnel with security awareness training that is updated to reflect risks identified by the risk assessment;
2. Using qualified information security personnel (whether employed by the financial institution or by an affiliate or service provider) sufficient to manage the institution's information security risks and to perform or oversee the information security program;
3. Providing information security personnel with security updates and training sufficient to address relevant security risks; and
4. Verifying that key information security personnel take steps to maintain current knowledge of changing information security threats and countermeasures.

Service Provider Oversight

The proposal contemplates that financial institutions would be required to oversee service providers, by:

1. Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue;
2. Requiring service providers by contract to implement and maintain such safeguards; and
3. Periodically assessing service providers based on the risk they present and the continued adequacy of their safeguards.

Program Evaluation

A financial institution would be required to evaluate and adjust its information security programs in light of the results of the required testing and monitoring, any material changes to its operations or business arrangements; the results of its periodic risk assessments or any other circumstances that the institution knows or has reason to know may have a material impact on the program.

Incident Response Plan

The proposal would require each financial institution to establish a written incident response plan designed to promptly respond to, and recover from, any security event

materially affecting the confidentiality, integrity or availability of customer information in its possession. The incident response plan would be required to address the following areas:

1. The goals of the incident response plan;
2. The internal processes for responding to a security event;
3. The definition of clear roles, responsibilities and levels of decision-making authority;
4. External and internal communications and information sharing;
5. Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;
6. Documentation and reporting regarding security events and related incident response activities; and
7. The evaluation and revision, as necessary, of the incident response plan following a security event.

Board Reporting

The CISO would be required to report in writing, at least annually, to the financial institution's board of directors or equivalent governing body. If no such board of directors or equivalent governing body exists, such report would be required to be timely presented to a senior officer responsible for the institution's information security program. The report would be required to address:

1. The overall status of the information security program and the institution's compliance with the Safeguards Rule; and
2. Material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management's responses thereto, and recommendations for changes in the information security program.

SMALL BUSINESS EXEMPTIONS

The FTC proposes to exempt small business from certain of the Safeguard Rule's requirements. Specifically, financial institutions that maintain customer information concerning fewer than 5,000 consumers would not be required to comply with:

1. Section 314.4(b)(1), regarding the contents of the written risk assessment;
2. Section 314.4(d)(2), regarding continuous monitoring or periodic penetration testing and vulnerability assessments;
3. Section 314.4(h), regarding the written incident response plan; or
4. Section 314.4(i), regarding the requirement for the CISO to report in writing, at least annually, to the institution's board of directors or equivalent governing body.

While the NYDFS Cyber Regulation and the NAIC Model Law have exemptions, these typically apply based on the number of employees or gross revenue rather than the number of customers.

DEFINITION OF "FINANCIAL INSTITUTION"

When it first promulgated the Privacy Rule in 2000, the FTC determined that companies engaged in activities that are "incidental to financial activities" would not be considered "financial institutions." The FTC also decided that activities that were determined to be financial in nature after the enactment of the GLBA would not automatically be covered by its GLBA rules; rather, the Commission would have to take additional action to include them. The result was that – unlike the equivalent

regulations promulgated by the CFPB and the other federal agencies with GLBA rulemaking authority – the FTC version of the Privacy Rule (and by extension, the Safeguards Rule), does not consider a loan "finder" to be a financial institution.

The FTC now proposes to harmonize the Safeguards Rule and Privacy Rule with the other agencies' GLBA regulations by amending the definition of "financial institution" to include "incidental" activities and activities determined to be financial or incidental after 1999. This change would bring "finders" within the scope of the two rules. (The proposed change would not bring any other activities under the coverage of the rules at this time, because the Federal Reserve Board has not determined any activity other than finding to be financial in nature, or incidental to such activity, since the enactment of the GLBA.)

CONSOLIDATION OF DEFINITIONS

Currently, the definition of "financial institution" in the Privacy Rule—which governs the scope of the Safeguards Rule—applies to all financial institutions within FTC jurisdiction, despite the fact that most types of financial institution are now subject to the privacy rules promulgated by the CFPB, the SEC, and the federal banking agencies. The FTC notes in its proposed rule that this creates a confusing situation where the Privacy Rule, on its face, appears to cover types of "financial institution" that no longer are subject to the rule.

To resolve this confusion, the FTC proposes to revise the Privacy Rule to make its limited scope more clear, and to transfer the broader definition of "financial institution" and its accompanying examples from the Privacy Rule to the Safeguards Rule. This modification is intended only to increase clarity – it would have no substantive effect on the scope of the rules or their enforcement.

Privacy Rule

The FTC proposes to make three types of change to the Privacy Rule: (i) technical changes to correspond to the reduced scope of the rule pursuant to the Dodd-Frank Wall Street Reform and Consumer Protection Act[9] (the "Dodd-Frank Act") (e.g., removing references inapplicable to motor vehicle dealers); (ii) modifications to the annual privacy notice requirements to reflect the changes made to the GLBA by the Fixing America's Surface Transportation Act[10] (the "FAST Act") in 2015; and (iii) as discussed above, modifications to the scope and definition of "financial institution" to include "finders" and other entities engaged in activities that are incidental to financial activities.

TECHNICAL CHANGES

The Dodd-Frank Act amended the FTC's rulemaking authority under the GLBA such that the Privacy Rule only applies to motor vehicle dealers. The FTC proposes to delete references in the Privacy Rule to entities other than motor vehicle dealers, so as to avoid confusion as to the existing, narrower scope of the Privacy Rule.

Specifically, the proposed amendments narrow the description of the scope of the Privacy Rule to those financial institutions that are predominantly engaged in the sale and servicing of motor vehicles or the leasing and servicing of motor vehicles, excluding those dealers that directly extend credit to consumers and do not routinely assign the extensions of credit to an unaffiliated third party. The amendments also would remove the reference to "other persons" from the section of the Privacy Rule that describes its scope, because even though the FTC continues to have enforcement authority over "other persons" covered by the CFPB's Regulation P, the Commission no longer has

Privacy Rule rulemaking authority with respect to such persons.

ANNUAL PRIVACY NOTICE

On December 4, 2015, President Obama signed the FAST Act, which contains a provision that modified the GLBA annual privacy notice requirement. The FAST Act provision states that a financial institution is not required to provide an annual privacy notice if it: (i) only shares nonpublic personal information with nonaffiliated third parties in a manner that does not require an opt-out right be provided to customers (e.g., if the institution discloses nonpublic personal information to a service provider or for fraud detection and prevention purposes); and (ii) has not changed its policies and practices with respect to disclosing nonpublic personal information since it last provided a privacy notice to its customers.

In order to incorporate this exemption into the Privacy Rule, the Commission proposes to revise the regulation to indicate that a financial institution is not required to deliver an annual privacy notice if it:

1. Provides nonpublic personal information to nonaffiliated third parties only in accordance with one or more opt-out exceptions; and
2. Has not changed its policies and practices with regard to the disclosure of nonpublic personal information from those disclosed to the customer in the institution's most recent GLBA privacy notice.

If a financial institution takes advantage of this exemption and subsequently changes its policies or practices in such a way that it no longer qualifies for the exemption, and Section 313.8 of the Privacy Rule requires the institution to provide a revised privacy notice, the institution would be required to provide an annual privacy notice in accordance with the standard timing requirements, treating the revised privacy notice as an initial privacy notice. If the institution no longer qualifies for the exemption because the institution has changed its policies or practices in such a way that Section 313.8 does not require a revised privacy notice, the institution would be required to provide an annual privacy notice within 100 days of the change in its policies or practices.

DEFINITION OF "FINANCIAL INSTITUTION"

As discussed above, the current versions of the Safeguards Rule and Privacy Rule do not cover "finders" or other entities engaged in activities that are incidental to financial activities. As with the Safeguards Rule, the Commission proposes to expand the definition of "financial institution" in the Privacy Rule to harmonize with the equivalent regulations promulgated by the CFPB, the SEC and the federal banking regulators.

Conclusion

While the proposed Privacy Rule updates are non-controversial, the proposed revisions to the Safeguards Rule would apply to a broad range of financial industry participants and reflect a marked change in the approach that federal regulators historically have taken with respect to information security. For financial institutions also covered by the NYDFS Cyber Regulation, the proposed revisions to the Safeguards Rule are very similar and should not require any significant changes to existing cybersecurity policies and procedures. Other financial institutions likely will need to revisit their existing information security policies and procedures if the proposed revisions eventually are adopted by the Commission. Financial institutions and their service providers should provide the Commission with comments on the proposals, particularly with respect to any implementation concerns they may have. Mayer Brown would be happy to

assist your company in preparing any comments you wish to submit to the FTC.

For more information about the topics raised in this Legal Update, please contact any of the following lawyers.

David A. Tallman
+1 713 238 2696
dtallman@mayerbrown.com

Jeffrey P. Taft
+1 202 263 3293
jtaft@mayerbrown.com

Stephen Lilley
+1 202 263 3865
slilley@mayerbrown.com

Endnotes

[1] 15 U.S.C. §§6801 *et seq.*

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

[3] 23 NYCRR 500. The NYDFS Cyber Final Regulation applies to any person operating under or required to operate under a license, registration, charter, certificate, permit ,accreditation or similar authorization under the New York Banking, Insurance or Financial Services Laws. For an overview of the NYDFS Cyber Regulation, see https://www.mayerbrown.com/en/perspectives-events/publications/2017/03/cybersecurity-ny-adopts-final-regulations-for-bank.

[4] *See* NAIC, Insurance Data Security Model Law, *available at* https://www.naic.org/store/free/MDL-668.pdf (*last accessed* Mar. 12, 2019). The NAIC Model Law requires every insurance licensee in a state (unless they qualify for an exemption) to maintain a written cybersecurity policy and implement a risk-based cybersecurity program. To date, the NAIC Model Law has been adopted in Michigan, Ohio and South Carolina. For an overview of the NAIC Model Law, see https://www.mayerbrown.com/en/news/2017/11/dissecting-naics-insurance-data-security-model-law.

[5] One of the key differences between the NYDFS Cyber Regulation and the proposed changes to the Safeguards Rule is the information covered. The NYDFS Cyber Regulation covers nonpublic information, which includes confidential information of the covered entity and not just customer information. Because GLBA and its implementing regulations only covers nonpublic personally identifiable information, the scope of the Safeguards Rule is narrower.

[6] Dissenting Statement of Commissioner Noah Joshua Phillips and Commissioner Christine S. Wilson, Regulatory Review of Safeguards Rule, Matter No. P145407 (March 5, 2019), *available at* https://www.ftc.gov/system/files/documents/public_statements/1466705/reg_review_of_safeguards_rule_cmr_phillips_wilson_dissent.pdf.

[7] 16 C.F.R. Part 313.

[8] The NYDFS Cyber Regulation does not limit the use of multi-factor authentication to accessing consumer information but rather applies it more broadly to cover nonpublic confidential information and information systems.

[9] P.L. No. 111-203.

[10] P.L. No. 114-94.

Mayer Brown is a distinctively global law firm, uniquely positioned to advise the world's leading companies and financial institutions on their most complex deals and disputes. With extensive reach across four continents, we are the only integrated law firm in the world with approximately 200 lawyers in each of the world's three largest financial centers—New York, London and Hong Kong—the backbone of the global economy. We have deep experience in high-stakes litigation and complex transactions across industry sectors, including our signature strength, the global financial services industry. Our diverse teams of lawyers are recognized by our clients as strategic partners with deep commercial instincts and a commitment to creatively anticipating their needs and delivering excellence in everything we do. Our "one-firm" culture—seamless and integrated across all practices and regions—ensures that our clients receive the best of our knowledge and experience.

Please visit mayerbrown.com for comprehensive contact information for all Mayer Brown offices.