MAYER | BROWN

November 10, 2021

Legal Update

US Federal Trade Commission Adopts Prescriptive Data Security Requirements and Other Updates to Its Gramm-Leach-Bliley Act Safeguards Rule

On October 27, 2021, the Federal Trade Commission ("FTC" or "Commission") issued a final rule ("Final Rule") implementing most of the revisions it proposed in 2019, with some important modifications, to its Gramm-Leach-Bliley Act[1] ("GLBA") safeguards rule ("Safeguards Rule").

Financial institutions covered by the Final Rule include finders (as discussed below), finance companies, mortgage companies, motor vehicle dealerships, payday lenders and other non-banks involved in the consumer financial services industry. The Final Rule:

- Adds provisions designed to provide covered financial institutions with more guidance on how to develop and implement specific aspects of an overall information security program, such as access controls, multi-factor authentication and encryption;
- Adds provisions designed to improve the accountability of financial institutions' information security programs, such as by requiring periodic reports to boards of directors or governing bodies;
- Exempts financial institutions that maintain customer information concerning fewer than 5,000 consumers from certain requirements;
- Expands the definition of "financial institution" to include entities engaged in activities that the Board of Governors of the Federal Reserve System ("Federal Reserve Board" or "Board") determines to be incidental to financial activities (e.g., so-called "finders" that bring together buyers and sellers of a product or service); and
- Defines several terms and provides related examples in the Safeguards Rule itself rather than incorporating them by reference from the rule implementing the GLBA privacy provisions ("Privacy Rule").[2]

The Final Rule will take effect one year after its publication in the *Federal Register*.[3]

Background

On April 4, 2019, the FTC proposed a number of revisions ("Proposed Rule") to the Safeguards Rule. In particular, the Commission proposed revisions to require financial institutions to implement specific information security controls, including those with respect to data encryption, multifactor authentication, incident response planning, board reporting and program accountability. The proposal

drew heavily from the cybersecurity regulations issued by the New York Department of Financial Services[4] ("NYDFS Cyber Regulation") in March 2017 and the insurance data security model law issued by the National Association of Insurance Commissioners ("NAIC Model Law") in October 2017.[5] Therefore, financial institutions subject to the NYDFS Cyber Regulation will be familiar with many of the requirements and likely have existing policies and procedures in place to address these requirements.

On July 13, 2020, the Commission held a workshop concerning the proposed changes and conducted panels with information security experts discussing subjects related to the Proposed Rule. The Commission received 60 comments in response to the Proposed Rule and workshop. Many comments highlighted the prescriptive nature of the Proposed Rule, noting concerns that the revisions may be too burdensome for financial institutions and other regulated entities to follow.

After reviewing the initial comments to the Proposed Rule, conducting the workshop and then reviewing the comments received following the workshop, the Commission issued its final amendments to the Safeguards Rule, which were shaped in part by the comments it received during the comment period.

The Commission received many comments suggesting that the prescriptive safeguard elements were inflexible and financially burdensome. However, the Commission dismissed these concerns, noting that the safeguard elements are goalposts that can be modified based on the institution's size and needs and a burden that is justified in order to protect customer information as required by the GLBA. The Commission noted that while large financial institutions may incur substantial costs to implement complex information security programs, there are much more affordable solutions available for financial institutions with smaller and simpler information systems. The Commission indicated that these expenses were justified because of the vital importance of protecting customer information collected, maintained and processed by financial institutions.

Overview of the Final Rule

QUALIFIED INDIVIDUAL

Where the Proposed Rule would have required a financial institution to appoint a Chief Information Security Officer ("CISO"), the Final Rule instead requires the designation of a "Qualified Individual."[6] The Qualified Individual need not be an employee of the financial institution but may be an employee of an affiliate or a service provider. This change was intended to accommodate financial institutions that may prefer to retain an outside expert. No particular level of education, experience or certification is prescribed by the Final Rule. Accordingly, a financial institution may designate any qualified individual who is appropriate for its business.

CUSTOMER INFORMATION

Several industry groups also suggested that significant portions of the Proposed Rule should not apply to all customer information but rather only to some subset of particularly "sensitive" customer information, such as account numbers or social security numbers. These commenters generally argued that the definition of "customer information" is too broad, as it will include information that the commenters felt is not particularly sensitive, such as name and address, and therefore does not justify extensive safeguards. The Commission did not agree that some portion of customer information is not entitled to the protections required by the Final Rule. The Final Rule defines "customer information" as "any record containing nonpublic personal information" about a customer that is handled or maintained by or on behalf of a financial institution.[7]

RISK ASSESSMENT

In order to tailor its information security program to address the specific risks raised by its activities, systems and customers, a financial institution must conduct a risk assessment. The Final Rule requires financial institutions to base their 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 unauthorized disclosure, misuse, alteration, destruction or other compromise of information and that assesses the sufficiency of any safeguards in place to control these risks. The risk assessment should be written and include the following: (i) criteria and categorization of identified security risks; (ii) criteria for the assessment of the confidentiality, integrity and availability of information systems and customer information; and (iii) requirements describing how the risks identified will be mitigated based on the risk assessment and how the information security program will address the risks. Additional risks assessments must be periodically performed to reexamine the internal and external risks to the security, confidentiality and integrity of customer information.

ENCRYPTION, MULTI-FACTOR AUTHENTICATION AND OTHER SAFEGUARDS

The Final Rule requires each information security program to contain certain specific safeguards while still allowing financial institutions flexibility in designing their information security programs.[8] The specific required safeguards include:

- **Access Controls:** The Final Rule requires financial institutions to implement and periodically review access controls to authenticate and permit access only to authorized users and limit authorized users' access only to customer information that they need to perform their duties and functions.
- **Encryption:** The Commission adopted the proposal that applicable financial institutions either (i) encrypt 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, secure such customer information using effective alternate compensating controls reviewed and approved by the financial institution's Qualified Individual. The Final Rule does not require any specific process or technology to perform the encryption but does require that whatever process is used be sufficiently robust to prevent the deciphering of the information in most circumstances.
- **Multi-factor Authentication:** The Final Rule adopts the proposed language that either financial institutions must (i) implement multi-factor authentication for any individual accessing customer information or (ii) implement reasonably equivalent or more secure access controls with respect to any individual accessing internal networks that contain customer information, provided that the Qualified Individual has approved such alternate controls in writing. In situations where the need for quick access outweighs the security benefits of multi-factor authentication, the Final Rule allows the use of reasonably equivalent controls if approved in writing by the financial institution's Qualified Individual.
- **User Activity Logs:** The Final Rule removes the proposal's reference to the term "audit trails" in order to clarify that logging user activity is a user monitoring process. The Final Rule instead modifies the user monitoring provision to include a requirement to monitor and log the activity of authorized users and detect unauthorized access or use of, or tampering with, customer information by users.
- **Deletion:** The Final Rule requires institutions to delete customer information two years after the last time the information is used in connection with providing a product or service to the customer unless the information is necessary for business operations or required for a legitimate business purpose or targeted disposal is not reasonably feasible due to the manner in which the information is maintained.

TESTING AND MONITORING

A financial institution must regularly test or otherwise monitor the effectiveness of the key controls, systems and procedures of its safeguards. For information systems, the monitoring and testing shall include continuous monitoring or periodic penetration testing and vulnerability assessments. Absent continuous monitoring, the Final Rule requires financial institutions to perform annual penetration testing and vulnerability assessments at least once every six months and, additionally, whenever there are material changes to their operations or business arrangements and whenever there are circumstances they know or have reason to know may have a material impact on their information security program.

The Commission agreed with commenters who pointed out the difficulty of applying certain testing requirements to physical safeguards. Although the general testing requirements such as testing the effectiveness of physical locks should apply to physical safeguards, the continuous monitoring, vulnerability assessment, and penetration testing is not as relevant to information in physical form. Accordingly, the Final Rule limits the testing requirement to safeguards on information systems.[9]

The Final Rule requires financial institutions to take steps to monitor users and their activities related to customer information in a manner adapted to the financial institution's particular operations and needs. As described above, the Final Rule also requires user activity logging.[10]

EMPLOYING APPROPRIATE PERSONNEL AND PROVIDING TRAINING

Financial institutions are required to (i) provide personnel with security awareness training that is updated to reflect the risks identified by the risk assessment, (ii) use qualified information security personnel to manage information security risks and to oversee the information security program, (iii) provide information security personnel with security updates and sufficient training to address relevant security risks and (iv) verify that key information security personnel take steps to maintain current knowledge of changing information security threats. The Proposed Rule would have required financial institutions to implement policies and procedures "to ensure that personnel are able to enact [the financial institution's] information security program." In order to clarify that updates are required only when needed by changes in the financial institution or new security threats, though, the Final Rule states that training programs need to be updated only "as necessary."[11]

SERVICE PROVIDER OVERSIGHT

The Final Rule adopted the proposed language that requires financial institutions to oversee service providers by (i) taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue, (ii) requiring service providers by contract to implement and maintain such safeguards and (iii) periodically assessing service providers based on the risk they present and the continued adequacy of their safeguards.[12] The service provider oversight provision will likely require financial institutions to review their existing service provider contracts and amend as needed to ensure that their service providers maintain appropriate safeguards for customer information consistent with the Final Rule.

PROGRAM EVALUATION

As was proposed, the Final Rule requires financial institutions to evaluate and adjust their information security programs in light of (i) the results of the required testing and monitoring, (ii) any material changes to the institution's operations or business arrangements, (iii) the results of its periodic risk assessments or (iv) any other circumstances that the institution knows or has reason to know may have a material impact on its program.[13]

INCIDENT RESPONSE PLAN

The Final Rule requires 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.[14] The incident response plan must address the following areas:

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

Unlike the NYDFS Cyber Regulation and the federal banking agencies' GLBA safeguards rule, the Final Rule does not require financial institutions to report incidents to the Commission. However, the Commission is seeking comment on a proposed rule that would make an additional change to the Safeguards Rule to require financial institutions to report certain data breaches and other security events to the Commission.[15] The public will have 60 days after the proposed rule is published in the *Federal Register* to comment.

BOARD REPORTING

The Qualified Individual must report in writing, regularly and 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, the report must be timely presented to a senior officer responsible for the institution's information security program. The report must address:

- The overall status of the information security program and the institution's compliance with the Safeguards Rule; and
- 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.[16]

SMALL BUSINESS EXEMPTION

The Commission retained the proposed exemption for financial institutions with fewer than 5,000 customers.[17] Under the current Safeguards Rule, there is no exception for smaller entities, but the Commission believed it appropriate to exempt small businesses from some of the Final Rule's requirements. While commenters indicated other, better metrics were available to determine what was a "small business" that warranted an exception, the Commission decided that the number of individuals on whom a financial institution maintains customer information is the appropriate measure of whether the exemption should apply to a particular financial institution.

DEFINITION OF "FINANCIAL INSTITUTION"

The FTC proposed, and ultimately adopted, a definition of "financial institution" modeled on the definition in the Privacy Rule.[18] The Commission also included the proposed series of examples to

provide guidance on what constitutes a financial institution under the FTC's jurisdiction. Per the Commission, the "new language was not meant to reflect a substantive change to the Safeguards Rule" but rather to be read without reference to the Privacy Rule. The FTC made "one substantive change to the definition of 'financial institution'" in order to include entities that are "significantly engaged in activities that are incidental to … 'financial activity' as defined by the Bank Holding Company Act. This change added an additional covered activity: the act of "finding."[19] The Bank Holding Company Act defines a "financial institution" as any institution "the business of which is engaging in financial activities as described in section 1843(k) of title 12."[20] That section, in turn, describes activities that are financial in nature as those that the Board has determined "to be financial in nature or incidental to such financial activity."[21] The Final Rule's definition mirrors this language.

According to the Commission, the change will not lead to a significant expansion of the Final Rule's coverage because it expands the definition only to include entities that are engaged in activity that is incidental to financial activity as determined by the Federal Reserve Board. The Board has determined only one activity to be incidental to financial activity—"acting as a finder."[22] The Board describes acting as a finder as "bringing together one or more buyers and sellers of any product or service for transactions that the parties themselves negotiate and consummate."[23] Activities within the scope of acting as a finder include "[i]dentifying potential parties, making inquiries as to interest, introducing and referring potential parties to each other, arranging contacts between and meetings of interested parties" and "[c]onveying between interested parties expressions of interest, bids, offers, orders and confirmations relating to a transaction."[24]

The Commission asserted that the scope of this language's application is limited in the context of the Safeguards Rule because the Safeguards Rule applies only to (i) transactions that are "for personal, family, or household purposes"[25] and (ii) the information of customers, which are consumers with which a financial institution has a continuing relationship,[26] criteria that significantly narrow the types of finders that will have obligations under the Final Rule.

The harmonization of the Commission's definition of financial institution with the other GLBA privacy regulations further clarifies the scope of certain state privacy laws that are slated to come into effect in 2023. Colorado[27] and Virginia[28] both enacted comprehensive privacy laws this year that include broad exemptions for entities that are "financial institutions" subject to the GLBA. This means that certain "finders" who are financial institutions for purposes of the GLBA will be exempt from requirements under these state laws. However, this approach—creating exemptions at the entity level—has not been universally adopted by states adopting privacy frameworks. California, for example, currently has a law in place (and a successor statute slated to come into effect in 2023) that only exempts information that is subject to protection under the GLBA rather than exempting financial institutions themselves.[29]

CONSOLIDATION OF DEFINITIONS

The Commission proposed and adopted the consolidation of certain terms and deleted no-longer necessary language stating that all terms in the Safeguards Rule have the same meaning as in the Privacy Rule. The Final Rule incorporates the Privacy Rule definitions of "consumer," "customer," "customer relationship," "financial product or service," "nonpublic personal information," "personally identifiable financial information," "publicly available information" and "you."[30] According to the Commission, no substantive change to these definitions is intended.

The Final Rule also added definitions for additional terms such as "authorized user,"[31] "encryption,"[32] "information system,"[33] "multi-factor authentication,"[34] "penetration testing,"[35] "personally identifiable financial information,"[36] "security event"[37] and "service provider."[38]

Many of the proposed definitions were altered with more refined and precise language, based on the comments received.

Conclusion

The Final Rule applies to a broad range of financial industry participants and reflects a marked change to the approach that federal regulators historically have taken with respect to information security. For financial institutions also covered by the NYDFS Cyber Regulation, the Safeguards Rule is 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; adopt certain technical safeguards, such as access controls, user logs, multi-factor authentication and encryptions; and amend their vendor agreements to ensure that their third-party service providers have appropriate safeguards when accessing information systems or customer information.

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

Vivek K. Mohan
+1 650 331 2054
vmohan@mayerbrown.com

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

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

Matthew Bisanz
+1 202 263 3434
mbisanz@mayerbrown.com

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

Julyana C. Dawson
+1 202 263 3211
jcdawson@mayerbrown.com

Endnotes

[1] 15 U.S.C. §§ 6801 *et seq*.

[2] 12 C.F.R. Part 1016.

[3] FTC Standards for Safeguard Rule, Published Guidance on 16 C.F.R. § 314.

[4] 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

[5] *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 more than 15 states. For an overview of the NAIC Model Law, see https://www.mayerbrown.com/en/news/2017/11/dissecting-naics-insurance-data-security-model-law

[6] 16 C.F.R. § 314.4(a).

[7] 16 C.F.R. § 314.2(d).

[8] 16 C.F.R. § 314.4(c)(1)-(8).

[9] 16 C.F.R. § 314.4(d)(1).

[10] 16 C.F.R. § 314.4(d)(2).

[11] 16 C.F.R. § 314.4(e)(1).

[12] 16 C.F.R. § 314.4 (f)(1)-(3).

[13] 16 C.F.R. § 314.4 (g).

[14] 16 C.F.R. § 314.4(h).

[15] Request for Public Comment, FTC Standards for Safeguard Customer Information, *available at* https://www.ftc.gov/system/files/documents/federal_register_notices/2021/10/p145407safeguardssnprm.pdf (last visited Nov. 9, 2021).

[16] 16 C.F.R. § 314.4(i).

[17] 16 C.F.R. § 314.6.

[18] 16 C.F.R. § 314.2(h).

[19] 12 C.F.R. § 225.86(d)(1).

[20] 15 U.S.C. § 6809(3).

[21] 15 U.S.C. § 1843(k).

[22] 12 C.F.R. § 225.86.

[23] 12 C.F.R. § 225.86(d).

[24] 12 C.F.R. § 225.86(d)(1)(i).

[25] *See* Final Rule, 16 C.F.R. 314.2(b)(1).

[26] 16 CFR 314.1; Final Rule 16 CFR 314.2(c).

[27] Colo. Rev. Stat. § 6-1-1304(2)(j)(II); Colo. Rev. Stat. § 6-1-1304(2)(q). For an overview of Colorado's New Data Privacy Law, see https://www.mayerbrown.com/-/media/files/perspectives-events/publications/2021/07/colorados-new-data-privacy-law-comparing-to-other-states-and-looking-ahead.pdf

[28] Va. Code Ann. § 59.1-572(B)(ii).

[29] California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.;* certain provisions amended by the California Privacy Rights Act, (operative Jan. 1, 2023).

[30] 16 C.F.R. § 314.1.

[31] 16 C.F.R. § 314.2(a).

[32] 16 C.F.R. § 314.2(f).

[33] 16 C.F.R. § 314.2(j).

[34] 16 C.F.R. § 314.2(k).

[35] 16 C.F.R. § 314.2(m).

[36] 16 C.F.R. § 314.2(n)(1).

[37] 16 C.F.R. § 314.2(p).

[38] 16 C.F.R. § 314.2(q).