SULLIVAN & CROMWELL LLP

S&C memo

December 20, 2021

The Federal Trade Commission's Updated Safeguards Rule: An Overview

Federal Trade Commission Strengthens Information Security Safeguards for Consumer Financial Information

SUMMARY

On December 9, 2021, the Federal Trade Commission (the "FTC") issued an updated Safeguards Rule that strengthens the information security safeguards that non-banking financial institutions regulated by the FTC are required to implement to protect their customers' financial information.[1] The current Safeguards Rule, which has been in effect since 2003, requires financial institutions to create and maintain an information security program to protect customer information.[2] When key provisions of the updated Safeguards Rule (the "Final Rule") become effective in December 2022, these financial institutions will be required to include several additional elements in their information security programs, and more businesses may be subject to its provisions. In addition, the FTC proposed new breach notification requirements that would obligate FTC-regulated financial institutions to notify the Commission within 30 days of a security incident affecting at least 1,000 consumers.[3]

Key provisions of the updated Final Rule include the following:

- **Detailed Requirements for Information Security Programs:** The Final Rule includes more detailed requirements for the development and establishment of a financial institution's information security program. These include (1) specific criteria for risk assessment, (2) a requirement to address access controls, data inventory and classification, encryption, secure development practices, authentication, information disposal procedures, change management, testing and incident response and (3) mechanisms for effective employee training and oversight of service providers.
- **Accountability for Information Security Programs:** The Final Rule requires the designation of a single "Qualified Individual" to be responsible for the information security program. It also requires periodic reports to boards of directors or equivalent governing bodies, or, if no such

boards of directors or governing bodies exist, to senior management about their institutions' information security programs.

- **Exemptions for Smaller Financial Institutions:** The Final Rule exempts financial institutions that collect information on fewer than 5,000 consumers from certain requirements, including the written risk assessment, incident response plan and annual reporting requirements.
- **Expanded Definition of "Financial Institution":** The Final Rule expands the definition of "financial institution" to include entities engaged in activities that the Federal Reserve Board determines to be incidental to financial activities. As a result, the Final Rule encompasses "finders," which are companies that bring together buyers and sellers of a product or service. Finders must therefore comply with the Final Rule's requirements to protect the sensitive consumer financial information they often collect and maintain.
- **Definitions of Terms and Related Examples:** Rather than incorporate key definitions by reference to other laws or regulations, as the current rule does, the Final Rule includes several definitions and related examples in the text of the revised rule itself. These definitions include the definition of "financial institution."

The Final Rule contains many of the substantive requirements found in the New York Department of Financial Services' Cybersecurity Regulation, which applies to many of the same financial institutions that are regulated by the FTC. The Final Rule also more closely adheres to the specific information security requirements that the FTC has imposed in enforcement orders against non-financial institutions under its authority of Section 5 of the FTC Act. Financial institutions subject to the Final Rule should closely review their information security programs, risk assessments and incident response plans and update them as necessary to comply with the specific requirements in the Final Rule.

GENERAL PROVISIONS AND APPLICABILITY

The Gramm-Leach-Bliley Act (the "GLBA") provides a framework for the regulation of financial institutions' privacy and information security practices. The FTC has promulgated each iteration of the Safeguards Rule under Subtitle A of Title V of the GLBA, which directs it and other federal financial regulators to establish standards relating to administrative, technical and physical safeguards for certain information.[4]

Covered Institutions

The Safeguards Rule applies to non-bank financial institutions that are engaged in a broad range of financial activities like lending, insuring, providing financial advisory services and dealing in securities.[5] This encompasses a diverse range of financial institutions such as mortgage brokers, money transmitters, payday lenders, automotive dealerships, retailers that directly issue consumer credit cards and tax preparers.[6]

Handling of Personal Information

Although the Final Rule defines such terms as "continuing relationship" and "customer relationship," it applies to all customer information in the possession of financial institutions regardless of whether the information pertains to individuals with whom those institutions have such relationships.[7] The Final Rule therefore requires each financial institution to safeguard any record in its control containing nonpublic

personal information about a customer of a financial institution.[8] The Final Rule provides that only authorized users in a financial institution may handle the personal information within the financial institution's control and that their authority may extend only to the information that they need to perform their duties and functions.[9]

Detailed Requirements for Written Information Security Programs

The current Safeguards Rule requires covered institutions to develop, implement and maintain a written information security program tailored to their size and complexity, the types of financial activities they engage in and the kinds of customer data they collect.[10] Although the current rule requires financial institutions to perform a risk assessment and develop and implement a plan to control the risks identified as part of its safeguards program, it provides only high-level details on what such programs should include. The new Final Rule enumerates specific elements that information security programs must incorporate going forward and adds prescriptive details for certain existing requirements.[11]

Written Risk Assessment

Under the Final Rule, a financial institution must perform a risk assessment upon which it must base its information security program. This risk assessment must identify reasonably foreseeable internal and external risks that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of customer information. It must also assess the sufficiency of any safeguards in place to control those risks. The Final Rule requires that the risk assessment be written and include:

- criteria for the evaluation and categorization of identified security risks or threats;
- criteria for the assessment of the confidentiality, integrity and availability of the institution's information systems and customer information, including the adequacy of the financial institution's existing controls in the context of the identified security risks or threats; and
- a description of how the identified risks will be mitigated or accepted and how the information security program will address those risks.

Financial institutions must also periodically perform additional risk assessments that reexamine the risks described above.[12]

Safeguards

The Final Rule identifies specific safeguards financial institutions must design and implement to control the risks identified through the risk assessment. These include, but are not limited to:

- **Access Controls:** Financial institutions must implement both technical and, where appropriate, physical controls to authenticate and limit access to customer information only to authorized users to protect against the unauthorized access to, or acquisition of, customer information. Authorized users' access must in turn be limited only to customer information that they need to perform their duties and functions. In the case of customers, such controls must limit their access to their own information. These controls must be subject to periodic review.

- **Encryption:** Financial institutions must encrypt all customer information they hold or transmit, both in transit and at rest. The Final Rule defines "encryption" as 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.[13] To the extent that encryption is infeasible, the Qualified Individual may instead review and approve effective alternative controls.
- **Multi-Factor Authentication:** Unless the Qualified Individual has approved in writing reasonably equivalent or more secure access controls, any individual accessing any information system must be verified by multi-factor authentication. The Final Rule specifies that multi-factor authentication entails verification of at least two of the following authentication factors: (1) knowledge factors, such as a password; (2) possession factors, such as a token; or (3) inherence factors, such as biometric characteristics.[14]
- **Disposal of Personal Information:** Financial institutions must securely dispose of customer information no later than two years after the last date they use the information to provide a product or service to the relevant customer. Exceptions to this maximum two-year retention requirement include when the information is necessary for legitimate business purposes, that law or regulation requires its retention, or where targeted disposal is not reasonably feasible. The Final Rule also requires that financial institutions minimize the unnecessary retention of data through periodic review of their data retention policies.[15]

Penetration Testing and Vulnerability Assessments

The Final Rule directs financial institutions to regularly test or otherwise monitor the effectiveness of their safeguards' key controls, systems and procedures. Absent effective continuous monitoring or other ongoing detection for changes in information systems that may create vulnerabilities, financial institutions must conduct both:

- **Annual penetration testing**: Penetration testing is a test methodology whereby assessors try to override an information system's security features by attempting to penetrate the databases or controls from outside or inside the systems. Each year financial institutions must undertake such tests based on relevant risks identified by the risk assessment plan.
- **Biannual vulnerability assessments:** Such assessments must include any systemic scans or reviews of information systems reasonably designed to identify publicly known security vulnerabilities in a financial institution's information systems based on the risk assessment. Financial institutions must conduct vulnerability assessments at least every six months, in addition to whenever there are material changes to operations or business arrangements and whenever there are circumstances that they have reason to know may have a material impact on their information security programs.[16]

The Final Rule also requires financial institutions to evaluate and adjust their information security programs in light of the results of the monitoring and testing detailed above.[17]

Incident Response Plan

Pursuant to the Final Rule, financial institutions must establish a written incident response plan designed to respond promptly to and recover from any security event that materially affects the confidentiality, integrity, or availability of customer information in their control. The Final Rule requires that an incident response plan address:

- the goals of the plan;

- the internal processes for responding to a security event;
- the definition of clear roles, responsibilities and levels of decision-making authority;
- external and internal communications and information sharing;
- identified 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
- following a security event, the evaluation and revision as necessary of the incident response plan.[18]

Personnel and Service Providers

The Final Rule also requires financial institutions to take certain steps to manage their personnel and their relationships with service providers. These include:

- providing security awareness training;
- utilizing qualified information security personnel;
- selecting service providers capable of maintaining the required information safeguards; and
- requiring by contract that service providers implement and maintain such safeguards.[19]

Accountability for Information Security Programs

As noted above, the Final Rule calls for the designation of a "Qualified Individual" to oversee and implement the information security program.[20] The Qualified Individual may be an employee, an affiliate or a service provider.[21] Should an affiliate or service provider fill this role, the financial institution remains responsible for compliance and must ensure that the Qualified Individual maintains the information security program under the direction and oversight of a senior member of the financial institution's personnel.[22]

The Qualified Individual must provide the financial institution's board of directors, or an equivalent governing body, with a report detailing (1) the overall status of the information security program and its compliance with the Final Rule and (2) material issues related to the information security program and recommendations for changes in the program.[23] The Qualified Individual must make this report at least annually.[24]

Exemptions for Smaller Financial Institutions

As noted, the Final Rule exempts financial institutions that collect information on fewer than 5,000 consumers from the risk assessment, incident response plan and annual reporting requirements.

Expanded Definition of "Financial Institution"

The Final Rule expands the definition of "financial institution" to include "finders" that bring together entities engaged in activities that the Federal Reserve Board determines to be incidental to financial activities. As a result, "finders," which are companies that bring together buyers and sellers of a product or service, must

comply with the Final Rule's requirements to protect the sensitive consumer financial information they often collect and maintain.

The Federal Reserve Board has previously provided several examples of services that would qualify an entity as a "finder" for purposes of the Bank Holding Company Act, which regulates bank affiliates.[25] These include (1) hosting an electronic marketplace on the finder's website; (2) hosting on its servers the website of a buyer (or seller) that provides information about the products and services it seeks to buy (or sell) and allows sellers (or buyers) to submit expressions of interest, offers and order confirmations; and (3) operating a website that allows multiple buyers and sellers to exchange information about products and services they are willing to buy or sell, locate potential counterparties for transactions, aggregate orders for goods and services with those made by other parties and enter into transactions between themselves.[26]

Definitions of Terms and Related Examples

The current Safeguards Rule contains only a few definitions and instead incorporates the definitions in the GLBA Privacy Rule. The Final Rule instead explicitly includes those definitions in the GLBA Privacy Rule in the Final Rule and adds a number of new definitions discussed above, such as encryption and multi-factor authentication.

Proposed Additional Requirement: Breach Notification

In addition to the prescriptive information security requirements in the Final Rule, the FTC also proposed a new breach notification requirement for certain "security events,"[27] which the Final Rule defines as events "resulting in unauthorized access to, or disruption or misuse of, an information system, information stored on such information system, or customer information held in physical form."[28] This aligns with the posture taken by other federal financial regulators, which require financial institutions to provide notice to affected customers following a compromise of customer information.[29] The FTC's definition of a "security event," however, is broader than the current customer notification requirement imposed by, for example, the Federal Reserve Board, which only requires notification in cases of unauthorized access to sensitive customer information.[30] With respect to regulator notification, however, the FTC's definition of a "security event" is more narrow than the recent cyber incident notification final rule issued by other federal financial regulators.[31] That rule requires regulator notification upon the occurrence of a "notification incident" that is a "computer security incident" that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, a banking organization's (i) ability to carry out banking operations, activities, or processes, or deliver banking products and services to a material portion of its customer base, in the ordinary course of business; (ii) business line(s), including associated operations, services, functions, and support, that upon failure would result in a material loss of revenue, profit, or franchise value; or (iii) operations, including associated services, functions and support, as applicable, the failure or discontinuance of which would pose a threat to the financial stability of the United States.[32] The FTC's proposed update to the Safeguards Rule would require financial institutions to notify the Commission within

30 days of a security event affecting at least 1,000 consumers.[33] The FTC solicited public comment on the proposed breach notification rule before February 7, 2022.[34]

* * *

ENDNOTES

1 Standards for Safeguarding Customer Information, Federal Trade Commission, 86 Fed. Reg. 70,272 (Dec. 9, 2021) (to be codified at 16 C.F.R. pt. 314).

2 16 C.F.R. pt. 314 (2021).

3 Standards for Safeguarding Customer Information, Supplemental Notice of Proposed Rulemaking and Request for Public Comment, Federal Trade Commission, 86 Fed. Reg. 70,062 (Dec. 9, 2021).

4 15 U.S.C. 6801(b).

5 16 C.F.R. 313.3(k)(1) (2021); 86 Fed. Reg. 70,304.

6 16 C.F.R. 313.3(k)(2) (2021); 86 Fed. Reg. 70,304.

7 86 Fed. Reg. 70,304–05.

8 86 Fed. Reg. 70,306.

9 86 Fed. Reg. 70,307.

10 16 C.F.R. 314.3(a) (2021).

11 86 Fed. Reg. 70,304–08.

12 86 Fed. Reg. at 70,307.

13 86 Fed. Reg. 70,305.

14 86 Fed. Reg. 70,306.

15 86 Fed. Reg. 70,308.

16 *Id.*

17 *Id.*

18 *Id.*

19 *Id.*

20 86 Fed. Reg. 70,307.

21 *Id.*

22 *Id.*

23 86 Fed. Reg. 70,308.

24 *Id.*

25 12 C.F.R. 225.86(d) (2021).

26 *Id.*

27 86 Fed. Reg. 70,062.

28 86 Fed. Reg. 70,307.

29 12 C.F.R. Appendix F to Part 225, Supplement A.

30 *Id.*

31 Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, Office of the Comptroller of the Currency, Federal Reserve System and Federal Deposit Insurance Corporation, 86 Fed. Reg. 66,424 (Nov. 23, 2021) (to be codified at 12 C.F.R. 53, 12 C.F.R. 225 and 12 C.F.R. 304).

32 86 Fed. Reg. 66,444.

ENDNOTES CONTINUED

[33] 86 Fed. Reg. 70,067.

[34] 86 Fed. Reg. 70,062.

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 875 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers or to any Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.