[Billing Code: 6750-01S]

FEDERAL TRADE COMMISSION

16 CFR Part 314

RIN 3084-AB35

Standards for Safeguarding Customer Information

AGENCY: Federal Trade Commission.

ACTION: Final Rule.

SUMMARY: The Federal Trade Commission ("FTC" or "Commission") is issuing a final Rule ("Final Rule") to amend the Standards for Safeguarding Customer Information ("Safeguards Rule" or "Rule"). The amended Rule contains five main modifications to the existing Rule. First, it 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, authentication, and encryption. Second, it 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. Third, it exempts financial institutions that collect less customer information from certain requirements. Fourth, it expands the definition of "financial institution" to include entities engaged in activities that the Federal Reserve Board determines to be incidental to financial activities. This change adds "finders"–companies that bring together buyers and sellers of a product or service–within the scope of the Rule. Finally, the Final Rule defines several terms and provides related examples in the Rule itself rather than incorporate them by reference from the Privacy of Consumer Financial Information Rule, 16 CFR part 313.

DATES: Certain provisions of the amendments, set forth in Section 314.5 of the Final Rule, are effective [INSERT DATE ONE YEAR AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. The remainder of the amendments are effective [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

FOR FURTHER INFORMATION CONTACT:

David Lincicum, Katherine McCarron, or Robin Wetherill, Division of Privacy and Identity Protection, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue N.W., Washington, D.C. 20580, (202) 326-2773, (202) 326-2333, or (202) 326-2220.

SUPPLEMENTARY INFORMATION:

I. Background

Congress enacted the Gramm Leach Bliley Act ("GLB" or "GLBA") in 1999.[1] The GLBA provides a framework for regulating the privacy and data security practices of a broad range of financial institutions. Among other things, the GLBA requires financial institutions to provide customers with information about the institutions' privacy practices and about their opt-out rights, and to implement security safeguards for customer information.

Subtitle A of Title V of the GLBA required the Commission and other federal agencies to establish standards for financial institutions relating to administrative, technical, and physical safeguards for certain information.[2] Pursuant to the Act's directive, the Commission promulgated the Safeguards Rule in 2002. The Safeguards Rule became effective on May 23, 2003.

[1] Pub. L. 106–102, 113 Stat. 1338 (1999).
[2] *See* 15 U.S.C. 6801(b), 6805(b)(2).

The current Safeguards Rule requires a financial institution to develop, implement, and maintain a comprehensive information security program that consists of the administrative, technical, and physical safeguards the financial institution uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.[3] The information security program must be written in one or more readily accessible parts.[4] The safeguards set forth in the program must be appropriate to the size and complexity of the financial institution, the nature and scope of its activities, and the sensitivity of any customer information at issue.[5] The safeguards must also be reasonably designed to ensure the security and confidentiality of customer information, protect against any anticipated threats or hazards to the security or integrity of the information, and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.[6]

In order to develop, implement, and maintain its information security program, a financial institution must identify 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.[7] The financial institution must then design and implement safeguards to control the risks identified through the risk assessment, and must regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and

[3] 16 CFR 314.2(c).
[4] 16 CFR 314.3(a).
[5] 16 CFR 314.3(a), (b).
[6] 16 CFR 314.3(a), (b).
[7] 16 CFR 314.4(b).

procedures.[8] The Rule also requires the financial institution to evaluate and adjust its information security program in light of the results of this testing and monitoring, any material changes in its operations or business arrangements, or any other circumstances that it knows or has reason to know may have a material impact on its information security program.[9] The financial institution must also designate an employee or employees to coordinate the information security program.[10]

Finally, the current Safeguards Rule requires financial institutions to take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for customer information and require those service providers by contract to implement and maintain such safeguards.[11]

II. Regulatory Review of the Safeguards Rule

On September 7, 2016, the Commission solicited comments on the Safeguards Rule as part of its periodic review of its rules and guides.[12] The Commission sought comment on a number of general issues, including the economic impact and benefits of the Rule; possible conflicts between the Rule and state, local, or other federal laws or regulations; and the effect on the Rule of any technological, economic, or other industry changes. The Commission received 28 comments from individuals and entities

[8] 16 CFR 314.4(c).
[9] 16 CFR 314.4(e).
[10] 16 CFR 314.4(a).
[11] 16 CFR 314.4(d).
[12] Safeguards Rule, Request for Comment, 81 FR 61632 (Sept. 7, 2016).

representing a wide range of viewpoints.[13] Most commenters agreed that there is a continuing need for the Rule and that it benefits consumers and competition.[14]

On April 4, 2019, the Commission issued a Notice of Proposed Rulemaking (NPRM) setting forth proposed amendments to the Safeguards Rule (the "Proposed Rule").[15] In response, the Commission received 49 comments from various interested parties including industry groups, consumer groups, and individual consumers.[16] 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.[17] The Commission received 11 comments following the workshop.[18] After reviewing the initial comments to the Proposed Rule, conducting the workshop, and then reviewing the comments received following the workshop, the Commission now issues final amendments to the Safeguards Rule.

III. Overview of Final Rule

As noted above, the Final Rule modifies the current Rule in five primary ways. First, the Final Rule amends the current Rule to include more detailed requirements for the development and establishment of the information security program required under

[13] The 28 public comments received prior to March 15, 2019, are posted at: https://www.ftc.gov/policy/public-comments/initiative-674.
[14] *See, e.g.*, Mortgage Bankers Association (comment 39, NPRM); National Automobile Dealers Association (Comment 40, NPRM); Data & Marketing Association (comment 38, NPRM); Electronic Transactions Association (comment 24, NPRM); State Privacy & Security Coalition (comment 26, NPRM).
[15] FTC Notice of Proposed Rulemaking, 84 FR 13158 (April 4, 2019).
[16] The 49 relevant public comments received on or after March 15, 2019, can be found at Regulations.gov. *See* FTC Seeks Comment on Proposed Amendments to Safeguards and Privacy Rules, 16 CFR Part 314, Project No. P145407, https://www.regulations.gov/docket/FTC-2019-0019/document.
[17] *See* FTC, Information Security and Financial Institutions: An FTC Workshop to Examine Safeguards Rule Tr. (July 13, 2020), https://www.ftc.gov/system/files/documents/public_events/1567141/transcript-glb-safeguards-workshop-full.pdf [hereinafter Safeguards Workshop Tr.].
[18] The 11 relevant public comments relating to the subject matter of the July 13, 2020, workshop can be found at https://www.regulations.gov/document/FTC-2020-0038-0001. This Notice cites comments using the last name of the individual submitter or the name of the organization, followed by the number based on the last two digits of the comment ID number.

the Rule. For example, while the current Rule requires financial institutions to undertake a risk assessment and develop and implement safeguards to address the identified risks, the Final Rule sets forth specific criteria for what the risk assessment must include, and requires that the risk assessment be set forth in writing. As to particular safeguards, the Final Rule requires that they address access controls, data inventory and classification, encryption, secure development practices, authentication, information disposal procedures, change management, testing, and incident response. And while the Final Rule retains the requirement from the current Rule that financial institutions provide employee training and appropriate oversight of service providers, it adds mechanisms designed to ensure that such training and oversight are effective. Although the Final Rule has more specific requirements than the current Rule, it still provides financial institutions the flexibility to design an information security program that is appropriate to the size and complexity of the financial institution, the nature and scope of its activities, and the sensitivity of any customer information at issue.

Second, the Final Rule adds requirements designed to improve accountability of financial institutions' information security programs. For example, while the current Rule allows a financial institution to designate one or more employees to be responsible for the information security program, the Final Rule requires the designation of a single Qualified Individual. The Final Rule also requires periodic reports to boards of directors or governing bodies, which will provide senior management with better awareness of their financial institutions' information security programs, making it more likely that the programs will receive the required resources and be able to protect consumer information.

Third, recognizing the impact of the additional requirements on small businesses, the Final Rule exempts financial institutions that collect information on fewer than 5,000 consumers from the requirements of a written risk assessment, incident response plan, and annual reporting to the Board of Directors.

Fourth, 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. This change brings "finders"–companies that bring together buyers and sellers of a product or service–within the scope of the Rule. Finders often collect and maintain very sensitive consumer financial information, and this change will require them to comply with the Safeguards Rule's requirements to protect that information. This change will also bring the Rule into harmony with other federal agencies' Safeguards Rules, which include activities incidental to financial activities in their definition of financial institution.

Finally, the Final Rule includes several definitions and related examples, including of "financial institution," in the Rule itself rather than incorporate them by reference from a related FTC rule, the Privacy of Consumer Financial Information Rule, 16 CFR part 313. This will make the rule more self-contained and will allow readers to understand its requirements without referencing the Privacy Rule.

IV. Section-by-Section Analysis

General Comments

The Commission received 49 comments in response to the NPRM for the Proposed Rule, from a diverse set of stakeholders, including industry groups, individual businesses, consumer advocacy groups, academics, information security experts,

government agencies, and individual consumers. It also hosted a workshop on the Proposed Rule, which included approximately 20 security experts. Some of the comments simply expressed general support[19] or general disapproval[20] of the Proposed Rule. Many, however, offered detailed responses to specific proposals in the NPRM. In general, industry groups were opposed to most or all of the Proposed Rule, and consumer advocacy groups, academics, and security experts were generally in favor of the amendments. The comments and workshop record are discussed in the following Section-by-Section analysis.

Section 314.1: Purpose and Scope.

The Purpose and Scope section of the current Rule generally states that the Rule implements the Gramm–Leach–Bliley Act and applies to the handling of customer information by financial institutions over which the FTC has jurisdiction. In its NPRM, the Commission proposed adding a definition of "financial institution" modeled on the definition included in the Commission's Privacy Rule (16 CFR part 313) and a series of examples providing guidance on what constitutes a financial institution under the Commission's jurisdiction. Other than expanding the definition of "financial institution" as discussed below, the new language was not meant to reflect a substantive change to the Safeguards Rule; rather, it was meant to allow the Rule to be read on its own, without reference to the Privacy Rule.[21] The Commission received no comments that addressed

[19] *See* Encore Capital Group (comment 25, NPRM); Justine Bykowski (comment 12, NPRM); "Peggy from Bloomington, MN" (comment 13, NPRM); "Anonymous" (comment 20, NPRM).
[20] "Jane Q. Citizen" (comment 14, NPRM).
[21] In a separate Notice, the Commission is amending the Privacy Rule to reflect changes made by the Dodd-Frank Act, limiting that Rule to certain auto dealers. Through that proceeding, the Commission is also removing examples of financial institutions from the Privacy Rule that are no longer covered under the Rule in the wake of these changes.

this section specifically, and the Commission adopts the language of the Proposed Rule in the Final Rule.[22]

Section 314.2: Definitions

The Proposed Rule added a number of definitions to section 314.2. The Proposed Rule also retained paragraph (a), which stated that terms used in the Safeguards Rule have the same meaning as set forth in the Privacy Rule.

The American Council on Education (ACE) suggested that all terms from the Privacy Rule, such as "consumer," "customer," and "customer information," be included in the Final Rule in order to make the Final Rule easier for regulated entities to understand.[23] On the other hand, HITRUST recommended that no definitions from the Privacy Rule be duplicated in the Safeguards Rule, reasoning that in the event of a need to amend the terms, it would require the amendment of two rules rather than one.[24]

The Commission is persuaded that including all terms from the Privacy Rule within the Safeguards Rule will improve clarity and ease of use. Accordingly, the Commission has determined to delete paragraph (a), since it is no longer necessary to state that all terms in the Safeguards Rule have the same meaning as in the Privacy Rule. It also adds 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" to the definitions in the Final Rule. No substantive change to these definitions is intended.

---

[22] Several commenters addressed the change to the definition of "financial institution." Those comments are addressed in the discussion of the definition of "financial institution" below.
[23] American Council on Education (comment 24, NPRM), at 7.
[24] HITRUST, (comment 18, NPRM), at 2.

Authorized User

The Proposed Rule added a definition for the term "authorized user" as paragraph (b). Proposed paragraph (b) defined an "authorized user" of an information system as "any employee, contractor, agent or other person that participates in your business operations and is authorized to access and use any of your information systems and data." This term was used in paragraph 314.4(c)(10) of the Proposed Rule, which required financial institutions to implement policies to monitor the activity of "authorized users" and detect unauthorized access to customer information.

The Commission received one comment on this proposed definition from the National Automobile Dealers Association (NADA), which suggested that the term "authorized user" was used inconsistently and was too vague.[25] NADA pointed out that while "authorized user" is a defined term, the term "authorized individual" was used in proposed paragraphs 313.4(c)(1) (addressing access controls for information systems) and (c)(3) (addressing access controls for physical data). NADA also argued that the inclusion of "other person that participates in the business operations of an entity" within the definition of "authorized user" was unclear and created ambiguity in its application.[26]

The Commission agrees with NADA's points, and, in response, modifies the Final Rule in two ways. First, the Final Rule replaces the term "authorized individual" with "authorized user" in paragraph 313.4(c)(1). As described further below, because the Final Rule combines paragraph 313.4(c)(3) with paragraph 313.4(c)(1), there is no need to make a corresponding change to that section.

[25] National Automobile Dealers Association (comment 46, NPRM), at 11-12.
[26] National Automobile Dealers Association (comment 46, NPRM), at 11-12.

Second, because the Commission agrees that the ambiguities in the definition of "authorized user" from the Proposed Rule could create confusion, it makes several changes to the definition. It deletes the phrase "other person that participates in the business operations of an entity." The Commission agrees that this phrase was vague. The Commission had intended it to cover any person the financial institution allows to access information systems or data, including, for example, "customers" of the financial institutions. For the purpose of controlling authorized access and detecting unauthorized access (which is where the definition of "authorized user" appears), financial institutions should monitor anomalous patterns of usage of their systems, not only by employees and agents, but also by customers and other persons authorized to access systems or data. To clarify this point, the Commission adds "customer or other person" to the definition of "authorized users."

The Commission intends that the definition of "authorized users" should include anyone who the financial institution authorizes to access an information system or data, regardless of whether that user actually uses the data. Thus, for clarity, the Commission has deleted the requirement that the authorized user be authorized *to use* the information system or data. Finally, the definition of authorized user should include users who can access both "information systems and data" and users authorized to access either information systems *or* data. Accordingly, for clarification purposes, the Commission modifies the definition of "authorized user" in the Final Rule as "any employee, contractor, agent, customer or other person that is authorized to access any of your information systems or data."

Security Event

In proposed paragraph (c), the Commission defined "security event" as "an event resulting in unauthorized access to, or disruption or misuse of, an information system or information stored on such information system." This term was used in provisions requiring financial institutions to establish a written incident response plan designed to respond to security events. It also appeared in the provision requiring the coordinator of a financial institution's information security program to provide an annual report to the financial institution's governing body; the required report must identify all security events that took place that year.

Commenters expressed three main concerns with this definition. The first relates to whether the term "security event" should be expanded to instances in which there is unauthorized access to, or disruption or misuse of, information in physical form, as opposed to electronic form. The Proposed Rule used the term "security event" instead of "cybersecurity event" to clarify that an information security program encompasses information in both digital and physical forms and that unauthorized access to paper files, for example, would also be a security event under the Rule. The Money Services Round Table (MSRT), however, noted that despite the use of the more general "security" in the defined term, the definition itself is limited to events involving information systems.[27] The Commission agrees that this creates a contradiction. Accordingly, the Final Rule includes the compromise of customer information in physical form in the definition of "security event."

Second, some industry groups argued that a "security event" should occur only when there is "unauthorized access" to an information system, not in cases in which there

[27] Money Services Round Table (comment 53, NPRM), at 5 n.14.

has been a "disruption or misuse" of such systems (e.g., a ransomware attack).[28] These commenters argued that the disruption or misuse of information systems is not directly related to the protection of customer information and is, therefore, outside the Commission's statutory authority.[29] The Commission disagrees. Requiring a financial institution to protect against disruption and misuse of its information system is within the Commission's authority under the GLBA, which directed the Commission to promulgate a rule that required financial institutions to "to protect against any anticipated threats or hazards to the security or integrity" of customer information. A disruption or misuse of an information system will be, in many cases, a threat to the "integrity" of customer information. In addition, disruption or misuse may also indicate the existence of a security weakness that could be exploited to gain unauthorized access to customer information. For example, an event in which ransomware placed on a system is used to encrypt customer information, rendering it useless, raises the possibility that similar software could have been used to exfiltrate customer information. Accordingly, the Final Rule retains the inclusion of "misuse or disruption" within the definition of "security event."

Third, several commenters suggested that the definition of "security event" be limited to events in which there is a risk of consumer harm or some other negative effect.[30] Similarly, some commenters argued that the definition should exclude events

[28] National Independent Automobile Dealers Association (comment 48, NPRM), at 4; National Automobile Dealers Association (comment 46, NPRM), at 12-13; Consumer Data Industry Association (comment 36, NPRM), at 3-4.
[29] National Independent Automobile Dealers Association (comment 48, NPRM), at 4; National Automobile Dealers Association (comment 46, NPRM), at 12-13.
[30] HITRUST (comment 18, NPRM), at 3; American Council on Education (comment 24, NPRM), at 7; Mortgage Bankers Association (comment 26, NPRM), at 4-5; Consumer Data Industry Association

that involve encrypted information in which the encryption key was not compromised or when there is evidence that the information accessed has not been misused.[31] The Commission declines to narrow the provision in this manner. It believes that a financial institution should still engage in its incident response procedures to determine whether the event indicates a weakness that could endanger customer information and to respond accordingly. The financial institution can then take the appropriate steps in response. Further, paragraph 314.4(h) of the Final Rule, which sets forth the requirement for an incident response plan, requires that the incident response plan be designed to respond only to security events "materially affecting the confidentiality, integrity, or availability of customer information," limiting the impact of the definition of "security event."

Accordingly, the Final Rule defines "security event" as "an event 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." The Proposed Rule placed this definition as paragraph (c), out of alphabetical order. The Final Rule adopts it as paragraph (p), placing it in alphabetical order with the other definitions in section 314.2.

Encryption

Proposed paragraph (e) defined "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." This term was used in proposed paragraph 314.4(c)(4), which generally

---

(comment 36, NPRM), at 3-4; National Automobile Dealers Association (comment 46, NPRM), at 12-13; National Independent Automobile Dealers Association (comment 48, NPRM), at 4.

[31] Mortgage Bankers Association (comment 48, NPRM), at 4-5; National Automobile Dealers Association (comment 46, NPRM), at 12-13; National Independent Automobile Dealers Association (comment 48, NPRM) at 4; American Council on Education (comment 24, NPRM), at 7.

required financial institutions to encrypt customer information. This definition was intended to define the process of encryption while not requiring any particular technology or technique for achieving the protection provided by encryption.

NADA argued that this definition should be made more flexible by adding an alternative so that it would read "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 *or securing information by another method that renders the data elements unreadable or unusable*" (emphasis added).[32] On the other hand, others argued that the Proposed Rule's definition did not sufficiently protect customer information.[33] For example, the Princeton University Center for Information Technology Policy ("Princeton Center") suggested that the Rule should be changed "to clarify that encryption must be consistent with current cryptographic standards and accompanied by appropriate safeguards for cryptographic key material."[34] Similarly, ACE argued that the definition should include "the transformation of data in accordance with industry standards."[35]

The Commission agrees that the proposed definition should be tethered to some technical standard, without being too prescriptive about what that standard is. Under the proposed definition, as well as NADA's proposed definition, financial institutions could have claimed they were "encrypting" data if they were aggregating it, scrambling it, or redacting it in a way that made it possible to re-identify the data through, for example, the application of common algorithms or programs. The Commission does not believe this

---

[32] National Automobile Dealers Association (comment 46, NPRM), at 13.
[33] American Council on Education (comment 24, NPRM), at 7; Princeton University Center for Information Technology Policy (comment 54, NPRM), at 4.
[34] Princeton University Center for Information Technology Policy (comment 54, NPRM), at 4.
[35] American Council on Education (comment 24, NPRM), at 7.

would have provided consumers with sufficient protection. The Commission also agrees with the commenters who stated that the definition should signal that encryption should be cryptographically based.

Accordingly, 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, consistent with current cryptographic standards and accompanied by appropriate safeguards for cryptographic key material." This definition 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.

Financial Institution

Incidental Activity

The Proposed Rule made one substantive change to the definition of "financial institution" that it incorporated from the Privacy Rule. The change was designed to include entities that are "significantly engaged in activities that are incidental to [] financial activity" as defined by the Bank Holding Company Act. This proposed change brought only one activity into the definition that was not covered before: the act of "finding" as defined in 12 CFR 225.86(d)(1). The proposed revision to paragraph (f) added an example of a financial institution acting as a finder by "bringing together one or more buyers and sellers of any product or service for transactions that the parties themselves negotiate and consummate." This example used the language set forth in 12 C.F.R. 225.86(d)(1), which defines "finding" as an activity that is incidental to a financial

activity under the Bank Holding Company Act. The Commission adopts this proposal without modification.

The change to the definition of "financial institution" brings it into harmony with other agencies' GLB rules.[36] The change is supported by the language of the Gramm-Leach-Bliley Act.[37] The 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."[38] 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."[39] The Final Rule's definition mirrors this language. The change will not lead to a significant expansion of the Rule coverage as 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."[40]

Several commenters who addressed this issue supported the inclusion of activities that are incidental to financial activities.[41] Other commenters expressed concern that the proposed change in the definition would expand the Rule's coverage to businesses that should not be considered financial institutions.[42] They argued that the definition of the

---

[36] *See* 12 CFR 1016.3(l) (defining "financial institution" for entities regulated by agencies other than the FTC). *See also* 17 CFR 248.3(n) (defining "financial institution" to include "any institution the business of which is… incidental to …financial activities*"* for Security and Exchange Commission's rule implementing GLBA's safeguard provisions.).
[37] 15 U.S.C. 6801 et seq.
[38] 15 U.S.C. 6809(3).
[39] 12 U.S.C. 1843(k).
[40] 12 C.F.R. § 225.86.
[41] Electronic Privacy Information Center (comment 55, NPRM), at 9; Independent Community Bankers of America (comment 35, NPRM), at 3; National Automobile Dealers Association (comment 46, NPRM), at 13-16.
[42] Association of National Advertisers (comment, Workshop), at 4-5; Internet Association (comment, Workshop*)*, at 4-5; *see also* Anonymous (comment 15, NPRM) (questioning whether any governing body

term "finder" is too broad and that companies that connect buyers and sellers in non-financial contexts would be swept inappropriately into the definition of "financial institution." The Association of National Advertisers argued that advertising agencies could be considered "finders" because they play a role in connecting buyers and sellers.[43]

In response, the Commission notes that the Federal Reserve 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."[44] The Board sets forth several activities that are within the scope of acting as a finder, such as "[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."[45]

Although this language is somewhat broad, its scope is significantly limited in the context of the Safeguards Rule. First, the Safeguards Rule applies only to transactions that are "for personal, family, or household purposes."[46] Therefore, only finding services involving consumer transactions will be covered. Second, the Safeguards Rule applies only to the information of customers, which are consumers with which a financial institution has a continuing relationship.[47] Therefore, it will not apply to finders that have only isolated interactions with consumers and that do not receive information from other financial institutions about those institutions' customers. This significantly narrows

---

would oversee any future determinations by the Federal Reserve Board that activities are incidental to financial activity).

[43] Association of National Advertisers (comment 5, Workshop), at 5.

[44] 12 CFR 225.86 (d).

[45] 12 CFR 225.86 (d)(1)(i).

[46] *See* Final Rule 16 CFR 314.2(b)(1).

[47] 16 CFR 314.1; Final Rule 16 CFR 314.2(c).

the types of finders that will have obligations under the Rule, excluding, the Commission believes, most advertising agencies and similar businesses that generally do not have continuing relationships with consumers who are using their services for personal or household purposes.

The Commission believes that entities that perform finding services for consumers with whom they have an ongoing relationship are properly considered "financial institutions" for purposes of the Rule. Accordingly, the Commission adopts the changes to the definition of "financial institution" as proposed.

Other Changes to Definition of "Financial Institutions"

Other commenters suggested modifying the definition of "financial institution"[48] in different ways. The Electronic Privacy Information Center (EPIC) argued that the definition should be expanded by treating more activities as financial activities.[49] EPIC pointed out that information shared with social media companies, retailers, apps, and devices generally is not covered under the Safeguards Rule. The Commission understands the concern that many businesses fall outside the coverage of the Safeguards Rule, despite handling sensitive consumer information, but the Commission's authority to regulate activity under the Safeguards and Privacy Rules is established by the GLBA. The Rule's application is limited to financial institutions as defined by that statute and

[48] National Pawnbrokers Association (comment 32, NPRM), at 5-6 (arguing that transaction-reporting vendors be included in definition); National Consumer Law Center and others (comment 58, NPRM), at 5 (arguing that consumer reporting agencies be included explicitly in the definition); *see also* American Escrow Association (comment, Workshop), at 2-3 (requesting that the Rule specifically set out the duties of real estate settlement operations and other businesses that handle but do not maintain sensitive information); Beverly Enterprises, LLC (comment 3, NPRM), at 3-4 (requesting that the Rule specifically set out duties related to online notarizations); Yangxue Li (comment 5, NPRM) (asking whether Rule would set forth specific guidelines for different industries); Slobadon Raybolka (comment 17, NPRM) (suggesting that companies that perform online background checks be covered by the rule); The Clearing House (comment 49, NPRM) (suggesting a separate set of more stringent rules for fintech companies).
[49] Electronic Privacy Information Center (comment 55, NPRM), at 9.

cannot be extended beyond that definition.[50] The institutions discussed by EPIC, however, are still covered by the FTC Act's prohibition against deceptive or unfair conduct, including with respect to their use and protection of consumer information.[51]

The National Federation of Independent Business (NFIB) argued that individuals and sole proprietors should be excluded from the definition of "financial institution" on the grounds that an individual cannot be an "institution."[52] When the Privacy Rule was promulgated in 2000, commenters also suggested that the definition should exclude sole proprietors.[53] The Commission noted that there was no basis to exclude sole proprietors and that "[w]hether or not a commercial enterprise is operated by a single individual is not determinative" of whether the enterprise is a financial institution. The Commission has not changed its position on this matter and declines to make this change to the definition of "financial institution."

The Final Rule adopts this definition as proposed without change.

Information Security Program

Paragraph (i) of the Final Rule adopts the existing Rule's paragraph (c) and does not alter the definition of "information security program." The Commission received no comments on this definition, and accordingly, adopts the current definition in the Final Rule.

Information System

---

[50] *See* 15 U.S.C. 6801 (requiring agencies to promulgate Rule establishing standards for financial institutions); 15 U.S.C. 6809(3) (defining "financial institutions" as an "institution the business of which is engaging in financial activities as described" in the Bank Holding Company Act).
[51] In the Matter of *Facebook, Inc.*, Docket No. C-4365 (Apr. 28, 2020); *FTC v. Wyndham Worldwide Corporation*, 799 F.3d 236 (3d Cir. 2015); FTC v. *D-Link Systems, Inc.*, Case No. 3:17-cv-00039-JD (N.D. Cal. July 2, 2019); In the Matter of *Twitter, Inc.*, Docket No. C-4316 (Mar. 11, 2011).
[52] National Federation of Independent Business (comment 16, NPRM), at 2-3.
[53] Privacy Rule, Final Rule, 65 FR 33645 (May 24, 2000) at 33656.

Proposed paragraph (h) defined "information system" as "a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems." The term "information system" was used throughout the proposed amendments to designate the systems that must be covered by the information security program.

The MSRT suggested that this definition was too narrow in some respects and too broad in others.[54] It argued that the definition of "information system" was too narrow because it did not include physical systems or employees and would exclude them from some of the provisions of the Rule. Specifically, the MSRT argued that based on this definition, the penetration tests required by paragraph 314.4(d)(2) would not be required to test "potential human vulnerabilities" such as social engineering or phishing.[55] The Commission does not agree. Penetration testing, as defined by the Final Rule, is a process through which testers "attempt to circumvent or defeat the security features of an information system."[56] One way that such security features are tested is through social engineering and phishing.[57] The fact that the testing involves employees with access to the information system, rather than just the system itself, does not exclude such tests from the definition of "penetration testing." Attempted social engineering and phishing are

[54] Money Services Round Table (comment 53, NPRM), at 5-6.
[55] *Id.* at 5.
[56] Final Rule 314.2(j).
[57] Indeed, Workshop participant Scott Wallace noted that, in conducting penetration testing, "the first thing [he does]" is generally to "prepare for the phishing campaign." Remarks of Scott Wallace, Safeguards Workshop Tr., *supra* note 17, at 131-32.

important parts of testing the security of information systems and would not be excluded by this definition.

The MSRT also argued that the definition was too broad, and was joined by other commenters in this concern.[58] These commenters shared a concern that the proposed definition would include systems that are in no way connected to customer information and would require financial institutions to include all systems in their possession, regardless of their involvement with customer information. The Commission agrees that the definition should be limited to those systems that either contain customer information or are connected to systems that contain customer information, and adds that limitation to the Final Rule. The Rule does not limit the definition to only those systems that contain customer information, because a common source of data breaches is a vulnerability in a connected system that an attacker exploits to gain access to the company's network and move within the network to obtain access to the system containing sensitive information.[59] Accordingly, the definition of "information system" in the Final Rule is modified to "a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information containing customer information or any such system connected to a system containing customer information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange

[58] Money Services Round Table (comment 53, NPRM), at 5; Consumer Data Industry Association (comment 36, NPRM), at 4; American Council on Education (comment 24, NPRM), at 7-8.
[59] *See* Remarks of Serge Jorgensen, Safeguards Workshop Tr., *supra* note 17, at 58-59 (noting that cybersecurity attacks can take advantage of systems that are connected to the systems in which sensitive information is stored); Remarks of Tom Dugas, Safeguards Workshop Tr., *supra* note 17, at 138 (noting that a vulnerability in one system can result in the exposure of information maintained in another system); *see also* Remarks of Rocio Baeza, Safeguards Workshop Tr., *supra* note 17, at 106-07 (noting the heightened importance of encryption in a context where numerous systems are connected); Remarks of James Crifasi, Safeguards Workshop Tr., *supra* note 17, at 107-08 (same).

systems, and environmental controls systems, that contains customer information or that is connected to a system that contains customer information."

Multi-factor Authentication

Proposed paragraph (i) defined "multi-factor authentication" as "authentication through verification of at least two of the following types of authentication factors: 1) knowledge factors, such as a password; 2) possession factors, such as a token; or 3) inherence factors, such as biometric characteristics." This term was used in proposed paragraph 314.4(c)(6),[60] which required financial institutions to implement multi-factor authentication for individuals accessing networks that contain customer information.

Several commenters argued that the definition should explicitly include SMS text messages as an acceptable example of a possession factor or otherwise to be explicitly allowed.[61] The Proposed Rule did not include SMS text messages as an example of a possession factor.[62] Most commenters who addressed this issue interpreted this exclusion from the examples as forbidding financial institutions from using SMS text messages as a possession factor for multi-factor authentication. That is not the effect of this exclusion, however. The language of the definition neither prohibits nor recommends use of SMS text messages. Indeed, SMS text messages are not addressed at all. In some cases, use of SMS text messages as a factor may be the best solution because of its low cost and easy

[60] Paragraph 314.4(c)(5) in the Final Rule.
[61] Electronic Transactions Association (comment 27, NPRM), at 4; U.S. Chamber of Commerce (comment 33, NPRM), at 9; CTIA (comment 34, NPRM), at 7-9; Global Privacy Alliance (comment 38, NPRM), at 9; National Automobile Dealers Association (comment 46, NPRM), at 29; National Independent Automobile Dealers Association (comment 48, NPRM), at 6.
[62] *See*, *e.g.*, NIST Special Publication 800-63B, Digital Identity Guidelines, 5.1.3.3 (restricting use of verification using the Public Switched Telephone Network (SMS or voice) as an "out-of-band" factor for multi-factor authentication).

use, if its risks do not outweigh those benefits under the circumstances.[63] In other instances, however, the use of SMS text messages may not be a reasonable solution, such as when extremely sensitive information can be obtained through the access method being controlled, or when a more secure method can be used for a comparable price. A financial institution will need to evaluate the balance of risks for its situation. If, however, the Commission were to explicitly allow use of SMS text messages, this could be considered a safe harbor that would not require the company to consider risks associated with use of SMS text as a factor in a particular use case. Accordingly, the Final Rule does not include SMS text messages in the examples of possession factors.

The final Rule adopts the proposed definition of "multi-factor authentication" without change as paragraph (k) of this section.

Penetration Testing

Proposed paragraph (j) defined "penetration testing" as a "test methodology in which assessors attempt to circumvent or defeat the security features of an information system by attempting penetration of databases or controls from outside or inside your information systems." This term was used in proposed paragraph 314.4(d)(2), which required financial institutions to continually monitor the effectiveness of their safeguards or to engage in annual penetration testing. The Commission received no comments concerning this definition. The Final Rule adopts the definition from the Proposed Rule as paragraph (m) of this section.

Personally Identifiable Financial Information

[63] *See e.g.*, Remarks of Wendy Nather, Safeguards Workshop Tr., *supra* note 17, at 231-32.

To minimize cross-referencing to the Privacy Rule, as noted above, the Commission is adding several definitions to the Final Rule. One of these definitions is "personally identifiable financial information," which is identical to the definition currently contained in the Privacy Rule. This term is included within the ambit of "customer information," in both the existing Rule and the Final Rule.

The Princeton Center suggested expanding the definition of "personally identifiable financial information" from the Privacy Rule to include "aggregate information or blind data that does not contain personal identifiers such as account numbers, names, or addresses."[64] The Princeton Center further suggested clarifying that, for information to not be considered "personally identifiable financial information," the financial institution must be required to demonstrate that the information is not "reasonably linkable" to individuals.

The Commission does not believe that this amendment is necessary. The definition of "personally identifiable financial information" is already a broad one.[65] It includes not just information associated with types of personal information such as a name or address or account number, but also information linked to a persistent identifier ("any information you collect through an Internet 'cookie' (an information collecting device from a web server")).[66] While there may be some merit to limiting the exception for aggregate information or blind data to data that cannot be reasonably linkable to an individual, for purposes of a rule that can be periodically updated to keep up with

[64] Princeton University Center for Information Technology Policy (comment 54, NPRM) at 9-10.
[65] *See* 16 CFR 313(o)(1).
[66] 16 CFR 313.3(o)(2)(i)(F).

changing technology, the current approach is more concrete and enforceable, and less subject to differences in interpretation.

Service Provider

Proposed paragraph (k) adopted the existing Rule's definition and does not alter the definition of "service provider." The Commission received no comments on this definition and adopts it as paragraph (q) of the Final Rule.

Section 314.3: Standards for safeguarding customer information

Proposed section 314.3, which required financial institutions to develop an information security program (paragraph (a)) and set forth the objectives of the Rule (paragraph (b)), was largely identical to the existing Rule. It changed only the requirement that "safeguards" be based on the elements set forth in section 314.4, by replacing "safeguards" with "information security program." The Commission received no comments on this proposal and adopts it without change in the Final Rule.

Section 314.4: Elements

Proposed section 314.4 altered the current Rule's required elements of an information security program and added several new elements.

General Comments

The Commission received many comments addressing the new elements, both in favor of the changes and opposed to them. The comments in favor of the changes generally argued that these changes would protect consumers by improving the data security of institutions that hold their information.[67] Most of the comments opposed to

[67] *See, e.g.*, New York Department of Financial Service (comment 40, NPRM), at 1 (arguing that the Proposed Rule would "further advance efforts to protect financial institutions and consumers from cybercriminals."); Princeton University Center for Information Technology Policy (comment 54, NPRM),

the proposed elements fell into several categories, objecting: 1) that the proposed changes were too prescriptive and did not allow financial institutions sufficient flexibility in managing their information security; 2) that the proposed amendments would be too expensive for financial institutions, particularly smaller institutions, to adopt; and 3) that some of the requirements should not apply to all customer information but should be limited to some subset of especially "sensitive" customer information. The Commission does not agree with these comments for the reasons discussed below, and accordingly, retains the general approach of the Proposed Rule in the Final Rule.

Flexibility

Many industry groups argued that the new proposed elements were too prescriptive, lacked flexibility, would quickly become outdated, and would force financial institutions to engage in activities that would not enhance security.[68] For example, the Electronics Transactions Association argued that the Proposed Rule would "limit the ability of industry to develop new and innovative approaches to information security."[69] Similarly, CTIA commented that the Proposed Rule would create a

---

at 1 (stating that the Proposed Rule "would significantly reduce data security risks for the customers of financial institutions."); National Consumer Law Center and others (comment 58, NPRM), at 2 (stating that requirements of Proposed Rule are "reasonable and common-sense measures that any company dealing with large amounts of consumer personal information should take.").

[68] *See, e.g.*, HITRUST (comment 18, NPRM), at 1-2; American Council on Education (comment 24, NPRM), at 2-4; Cristian Munarriz (comment 21, NPRM); Electronic Transactions Association (comment 27, NPRM), at 1-2; National Pawnbrokers Association (comment 32, NPRM), at 3; CTIA (comment 34, NPRM), at 5; Consumer Data Industry Association (comment 36, NPRM), at 2; Wisconsin Bankers Association (comment 37, NPRM), at 1-2; Global Privacy Alliance (comment 38, NPRM), at 5-6; Bank Policy Institute (comment 39, NPRM), at 2; American Financial Services Association (comment 41, NPRM), at 4; National Association of Dealer Counsel (comment 44, NPRM), at 1; ACA International, (comment 45, NPRM), at 4; National Automobile Dealers Association (comment 46, NPRM), at 11; National Independent Automobile Dealers Association (comment 48, NPRM), at 2-3; Money Services Round Table (comment 53, NPRM), at 1-4; Software & Information Industry Association (comment 56, NPRM), at 1-3; Gusto and others (comment 11, Workshop), at 2; Association of National Advertisers (comment 5, Workshop), at 1-3; Internet Association (comment 9, Workshop), at 2-3.

[69] Electronic Transactions Association (comment 27, NPRM), at 1-2.

"prescriptive core of requirements that covered businesses must follow, irrespective of whether risk assessments show they are necessary."[70]

The Commission, however, believes that the elements provide sufficient flexibility for financial institutions to adopt information security programs suited to the size, nature, and complexity of their organization and information systems. The elements for the information security programs set forth in this section are high-level principles that set forth basic issues that the programs must address, and do not prescribe how they will be addressed. For example, the requirement that the information security program be based on a risk assessment sets forth only three general items that the assessment must address: 1) criteria for evaluating risks faced by the financial institution; 2) criteria for assessing the security of its information systems; and 3) how the identified risks will be addressed. Other than meeting these basic requirements, financial institutions are free to perform their risk assessments in whatever way they choose, using whatever method or approach works best for them, as long as the method identifies reasonably foreseeable risks. The other elements are similarly flexible. The two elements that are more prescriptive, encryption and multi-factor authentication, allow financial institutions to adopt alternative solutions when necessary. Comments concerning individual elements are addressed separately in the more detailed analysis below.

Cost

Another common theme among the comments from industry groups was that the proposed information security program elements would be prohibitively expensive,

[70] CTIA (comment 34, NPRM), at 5.

especially for smaller businesses.[71] Commenters argued that the Proposed Rule would have required financial institutions to implement expensive changes to their systems and hire highly-compensated professionals to do so.[72] Industry groups were particularly concerned about the requirement that financial institutions designate a single qualified individual to coordinate their information security programs, arguing that this would require hiring professionals that were both expensive, with salaries of more than $100,000 suggested by some, and in limited supply.[73] Overall, several commenters argued that some financial institutions would be unable to afford to bring themselves into compliance with the Proposed Rule.[74]

---

[71] American Council on Education (comment 24, NPRM), at 13-14; Wisconsin Bankers Association (comment 37, NPRM), at 1-2; American Financial Services Association (comment 41, NPRM), at 4; National Association of Dealer Counsel (comment 44, NPRM), at 1; National Automobile Dealers Association (comment 46, NPRM), at 11; National Independent Automobile Dealers Association, (comment 48, NPRM), at 3; Gusto and others (comment 11, Workshop), at 2-4; National Pawnbrokers Association (comment 3, NPRM), at 2; *see also* Remarks of James Crifasi, Safeguards Workshop Tr., *supra* note 17, at 72-74 (describing study that found that compliance would be expensive for automobile dealers).

[72] *See e.g.*, Slides Accompanying Remarks of James Crifasi, FTC, "NADA Cost Study: Average Cost Per U.S. Franchised Dealership," Event Materials, Information Security and Financial Institutions: An FTC Workshop to Examine Safeguards Rule (July 13, 2020) https://www.ftc.gov/system/files/documents/public_events/1567141/slides-glb-workshop.pdf (hereinafter Safeguards Workshop Slides), at 25 (estimating an upfront cost of $293,975 per dealership, and an recurring annual cost of $276,925)*; see also* Remarks of James Crifasi, Safeguards Workshop Tr., *supra* note 17, at 72-75; Remarks of Brian McManamon, Safeguards Workshop Tr., *supra* note 17, at 78 (estimating that the average annual salary of a CISO can range from $180,000 to upwards of $400,000); Slides Accompanying Remarks of Lee Waters, "Estimated Costs of Proposed Changes," Safeguards Workshop Slides, at 26 (estimating the annual costs of a security program to include: multi-factor authentication, $50 for smart card readers, and $10 each for smart cards; a CISO, either an in-house CISO, $180,000, an in-house cybersecurity analyst, $76,000, or an outsourced cybersecurity contractor, between $120,000 and $240,000; penetration testing, average cost $4,800; and physical security, $215,000 for construction, and $10,000 to $20,000 for new or upgraded locks)*; see also* Remarks of Lee Waters, Safeguards Workshop Tr., *supra* note 17, at 75-76.

[73] *See e.g.*, Slides Accompanying Remarks of Lee Waters, "Estimated Costs of Proposed Changes," Safeguards Workshop Slides, *supra* note 72, at 26 (estimating costs of an in-house CISO to be $180,000 annually, and an in-house cybersecurity analyst to be $76,000 annually; and estimating that an outsourced cybersecurity contractor would cost between $120,000 to $240,000 annually); *see also* Remarks of Lee Waters, Safeguards Workshop Tr., *supra* note 17, at 75-76; Remarks of Brian McManamon, Safeguards Workshop Tr., *supra* note 17, at 78 (estimating that the average annual salary of a CISO can range from $180,000 to upwards of $400,000).

[74] *See* Remarks of Lee Waters, Safeguards Workshop Tr., *supra* note 17, at 119-20 (noting that when small businesses have to spend money to hire third-party vendors and security experts to comply with

The Commission recognizes that properly securing information systems can be an expensive and technically difficult task. However, the Commission believes that the additional costs imposed by the Proposed Rule are mitigated for several reasons and that, ultimately, those costs are justified in order to protect customer information as required by the GLBA.[75]

First, for almost 20 years, financial institutions have been required under the current Safeguards Rule to have information security programs in place. The current Safeguards Rule requires that financial institutions "develop, implement, and maintain a comprehensive [written] information security program that is "appropriate to [the financial institutions'] size and complexity, the nature and scope of [their] activities, and the sensitivity of any customer information at issue."[76] This comprehensive program must be coordinated by one or more individuals and based on a risk assessment.[77] As such, financial institutions that are complying with the current Rule will not be required to establish an information security program from scratch. Instead, they can compare their existing programs to the revised Rule, and address any gaps. The Commission

---

regulations, that affects consumer prices and small business profit margins); Slides Accompanying Remarks of James Crifasi, "NADA Cost Study: Average Cost Per U.S. Franchised Dealership," Safeguards Workshop Slides, *supra* note 72, at 25*; see also* Remarks of James Crifasi*, supra* note 17, at 73 (noting the requirements "start becoming a little bit unaffordable here.").

[75] The Small Business Administration's Office of Advocacy commented that it was concerned the FTC had not gathered sufficient data as to either the costs or benefits of the proposed changes for small financial institutions. Office of Advocacy, U.S. Small Business Administration (comment 28, NPRM), at 3-4. The FTC shares the Office of Advocacy's interest in ensuring that regulatory changes have an evidentiary basis. Many of the questions on which the FTC sought public comment, both in the regulatory review and in the proposed Rule context, specifically related to the costs and benefits of existing and proposed Rule requirements. Following the initial round of commenting, the Commission conducted the FTC Safeguards Workshop and solicited additional public comments with the explicit goal of gathering additional data relating to the costs and benefits of the proposed changes. *See* Public Workshop Examining Information Security for Financial Institutions and Information Related to Changes to the Safeguards Rule, 85 FR 13082 (Mar. 6, 2020). As detailed throughout this Notice, the Commission believes that there is a strong evidentiary basis for the issuance of the final Rule.

[76] 16 CFR 313.3.

[77] 16 CFR 313.4.

believes that many of the requirements set forth in the Final Rule are so fundamental to any information security program that the information security programs of many financial institutions will already include them if those programs are in compliance with the current Safeguards Rule.

Second, a number of commenters who raised concerns about the costs imposed by the Rule believed that the Proposed Rule would have required the hiring of a highly-compensated expert to serve as a Chief Information Security Officer (CISO).[78] It is correct that the Proposed Rule would have modified the current requirement of designating an "employee or employees to coordinate your information security program" by requiring the designation of a single qualified individual responsible for overseeing and implementing the security program. This individual was referred to in the Proposed Rule as a Chief Information Security Officer or "CISO." As discussed in detail below, the Final Rule does not use this term, though the concept is the same: the person designated to coordinate the information security program need only be "qualified." No particular level of education, experience, or certification is prescribed by the Rule. Accordingly, financial institutions may designate any qualified individual who is appropriate for their business. Only if the complexity or size of their information systems

[78] Several speakers at the Safeguards Workshop also raised this concern. *See e.g.*, Slides Accompanying Remarks of James Crifasi, "NADA Cost Study: Average Cost Per U.S. Franchised Dealership," in Safeguards Workshop Slides, *supra* note 72, at 25 (estimating appointing a CISO to increase program accountability would be a one-time, up-front cost of $27,500, with a recurring annual cost of $51,000); Remarks of James Crifasi, Safeguards Workshop Tr., *supra* note 17, at 72-75; Slides Accompanying Remarks of Lee Waters, "Estimated Costs of Proposed Changes," in Safeguards Workshop Slides, *supra* note 72, at 26 (estimating costs of an in-house CISO to be $180,000 annually, and an in-house cybersecurity analyst to be $76,000 annually; and estimating that an outsourced cybersecurity contractor would cost between $120,000 to $240,000 annually); *R*emarks of Lee Waters, Safeguards Workshop Tr., *supra* note 17, at 75-76; Remarks of Brian McManamon, Safeguards Workshop Tr., *supra* note 17, at 78 (estimating that the average annual salary of a CISO can range from $180,000 to upwards of $400,000).

require the services of an expert will the financial institution need to hire such an individual.[79]

Finally, the Commission believes that while large financial institutions may well 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. For example, there are very low-cost or even free vulnerability assessment programs available: "virtual CISO" services enable a third party to provide security support for many companies, splitting the cost of information security professionals among them; many applications and hardware have built-in encryption requirements;[80] and there are affordable multi-factor authentication solutions aimed at businesses of various sizes.

Considering these points, although there will undoubtedly be expenses involved for some, or even many, financial institutions to update their programs, the Commission believes these expenses are justified because of the vital importance of protecting customer information collected, maintained, and processed by financial institutions. Congress recognized the importance of securing consumers' sensitive financial information when it passed the GLBA, which required the FTC to promulgate the Safeguards Rule. The importance, as well as the difficulty, of protecting customer information has only increased in the more than twenty years since the passage of the

---

[79] *See e.g.*, Remarks of Brian McManamon, Safeguards Workshop Tr., *supra* note 17, at 89-90 (noting that the size of a financial institution and the amount and nature of the information that it holds factor into an appropriate information security program)*; see also* Slides Accompanying Remarks of Rocio Baeza, "Models for Complying to the Safeguards Rule Changes," in Safeguards Workshop Slides, *supra* note 72, at 27-28 (describing three different compliance models: in-house, outsource, and hybrid, with costs ranging from $199 per month to more than $15,000 per month); Remarks of Rocio Baeza, Safeguards Workshop Tr., *supra* note 17, at 81-83 (describing three compliance models in more detail).

[80] *See* Remarks of Brian McManamon, Safeguards Workshop Tr., *supra* note 17, at 78 (describing virtual CISO services).

GLBA. The Commission believes that the amendments to the Safeguards Rule are necessary to ensure that the purposes of the GLBA are satisfied, and so consumers can have confidence that financial institutions are providing reasonable safeguards to protect their information.

"Sensitive" 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.[81] 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 does not justify extensive safeguards.[82]

The Commission does not agree that some portion of customer information is not entitled to the protections required by the Final Rule. The Safeguards 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.[83] The Final Rule defines "nonpublic personal information" as "personally identifiable financial information," but does not include information that is "publicly available." Although this definition is broad, the Commission believes that information covered by it is rightfully considered sensitive and should be protected accordingly. The businesses regulated by

[81] *See, e.g.*, Electronic Transactions Association (comment 27, NPRM), at 2-4; CTIA (comment 34, NPRM), at 10; Global Privacy Alliance (comment 38, NPRM), at 7-8; American Financial Services Association (comment 41, NPRM), at 5; ACA International (comment 45, NPRM), at 13; Money Services Round Table (comment 53, NPRM), at 6-7.
[82] *See, e.g.*, Electronic Transactions Association (comment 27, NPRM), at 2; Global Privacy Alliance (comment 38, NPRM), at 7.
[83] 16 CFR 314.2(b).

the Safeguards Rule are not just any businesses, but are financial institutions and are responsible for handling and maintaining financial information that is both important to consumers and valuable to attackers who try to obtain the information for financial gain. Even the fact that a consumer is a customer of a particular financial institution is generally nonpublic and can be sensitive. For example, the revelation of a customer relationship between a consumer and a particular type of financial institution, such as debt collectors or payday lenders, may make those customers' information more vulnerable to compromise by facilitating social engineering or similar attacks. The nature of the relationship between customers and their financial institutions makes all nonpublic information held by the financial institution inherently sensitive and worthy of the level of protection set forth in the Rule.

Although the Commission believes that all customer information should be safeguarded by financial institutions and declines to exclude any portion of that information from protection under any of the provisions of the Rule, it notes that the Rule does contemplate that financial institutions will consider the sensitivity of particular information in designing their information security programs and safeguards. The elements required by this section are generally flexible enough to allow financial institutions to treat various pieces of information differently. For example, paragraph (c)(1) requires information security programs to include safeguards that address access control of customer information. The paragraph requires financial institutions to develop measures to ensure that only authorized users access customer information, but does not prescribe any particular measures that must be adopted. When designing these measures, a financial institution may design a system in which more sensitive information is

protected by more stringent access controls. Even in the more specific provisions of the Rule, there is flexibility to address the relative sensitivity of information. For example, in paragraph 313.4(c)(5)'s requirement that customer information be protected by multi-factor authentication, financial institutions have flexibility to implement the multi-factor authentication depending on the sensitivity of the information. The financial institution may select factors such as SMS text messages to access less sensitive information, but determine that more sensitive information should be protected by other, more secure, factors for authentication.

Third-Party Standards and Frameworks

In addition, in the NPRM, the Commission asked whether the Safeguards Rule should incorporate outside standards, such as the National Institute of Standards and Technology ("NIST") framework, either as required elements of an information security program or as a safe harbor that would treat compliance with such a standard as compliance with the Safeguards Rule. Some commenters advocated for the adoption of an outside standard into the Safeguards Rule.[84] Cisco Systems, Inc. suggested that the Safeguards Rule should be connected to NIST guidance, arguing that this would allow the Rule to evolve as NIST's guidance evolves.[85] An anonymous commenter suggested that the Rule should comply with "international standard ISO/IEC 27001."[86] The National Consumer Law Center argued that certain financial institutions with particularly sensitive customer information should be required to comply with guidelines issued by

[84] Cisco Systems, Inc. (comment 51, NPRM), at 4; National Consumer Law Center and others (comment 58), at 2; Anonymous (comment 2, Workshop).
[85] Cisco Systems, Inc. (Comment 51, NPRM), at 4.
[86] Anonymous (comment 2, Workshop). The ISO/IEC 27001 standard is an information security standard issued by the International Organization for Standardization. *See* ISO/IEC 27001 Information Security Management, ISO, https://www.iso.org/isoiec-27001-information-security.html (last accessed 15 Dec. 2020).

NIST and the Federal Financial Institutions Examination Council (FFIEC).[87] Other commenters acknowledged the value of outside standards but were opposed to the Rule requiring compliance with them.[88]

Some commenters suggested that while compliance with outside standards should not be required, compliance should serve as a "safe harbor" for compliance with the Rule.[89] On the other hand, Consumer Reports noted that while such standards can be helpful guidance, they should not be a safe harbor for compliance with the Rule because financial institutions must take steps to ensure they are responding to changing information security threats regardless of the requirements of an outside framework.[90]

The Commission declines to change the Rule to incorporate or reference a particular security standard or framework for a variety of reasons. First, it is not clear that the more detailed frameworks would apply well to financial institutions of various sizes and industries. In addition, mandating that companies follow a particular security standard or framework would reduce the flexibility built into the Rule. Similarly, the Commission declines to make compliance with an outside standard a safe harbor for the Rule. In such a scenario, the use of safe harbors would not greatly enhance regulatory stability or predictability for financial institutions because the Commission would be required to actively monitor whether those standards continued to provide equivalent protections for Safeguards compliance and modify the Rule if a standard became

---

[87] National Consumer Law Center and others (comment 58, NPRM), at 2.
[88] HITRUST (comment 18, NPRM), at 2; *see also* Consumer Reports (comment 52, NPRM), at 6-7 (discouraging the adoption of outside standards as a safe harbor for companies).
[89] Mortgage Bankers Association (comment 26, NPRM), at 2 (suggesting that Rule be modified so financial institutions that use the NIST Cybersecurity Framework would be in de facto compliance with the Rule); *see also* National Pawnbrokers Association (comment 32, NPRM), at 6-7 (advocating for the adoption of safe harbors for small financial institutions without detailing what should be required to qualify for the safe harbor).
[90] Consumer Reports (comment 52, NPRM), at 6-7.

inadequate. In addition, in investigating possible violations of the Rule, the Commission would be required to independently verify whether the financial institution had in fact complied with the outside framework, which would require substantial effort and expense on the part of the Commission and the target of the investigation.

Specific Elements

In addition to these generally applicable comments, commenters addressed many of the individual elements set forth by this section. These elements are discussed in more detail below.

Paragraph (a) – Designation of a single qualified individual

Proposed paragraph (a) changed the current requirement that institutions designate an "employee or employees to coordinate your information security program" to instead require the financial institution to designate "a qualified individual responsible for overseeing and implementing your information security program and enforcing your information security program."[91] This individual was referenced in the Proposed Rule as a Chief Information Security Officer or "CISO."

The Notice of Proposed Rulemaking for the Proposed Rule emphasized that the use of the term "CISO" was for clarity in the Proposed Rule.[92] Despite the use of the term "CISO," the Proposed Rule did not require financial institutions to actually grant that title to the designated individual. Commenters that responded to this proposal, however, generally assumed that the person designated to coordinate and oversee a financial institution's information security program would be required to have the qualifications, duties, responsibilities, and accompanying pay of a CISO as that position

[91] 314.4(a).
[92] 84 FR at 13165.

is generally understood in the information security field.[93] The position of CISO is generally limited to large companies with fairly complex information security systems, so the salary of this position is often very high.[94] Accordingly, many commenters argued that hiring a CISO would be prohibitively expensive for many financial institutions.[95] Additionally, commenters argued that the hiring of such an in-demand professional would be difficult because of a general shortage of such professionals available for hiring.[96]

By using the term "CISO," the Commission did not intend to require that all financial institutions hire a highly qualified professional with an extremely high salary, regardless of the financial institutions' size or complexity. The Proposed Rule required only that financial institutions designate a "qualified individual" to oversee and enforce their information security program, without specifying any particular level of experience, education, or compensation, or requiring any particular duties outside of overseeing the financial institution's information security program and other requirements specifically set forth in the Rule.[97] The use of the term "CISO" in the Proposed Rule, however, caused confusion about the requirements of this section. Accordingly, the Final Rule replaces the term "CISO" with "Qualified Individual" to refer to the individual designated under this section of the Rule.

---

[93] U.S. Chamber of Commerce (comment 33, NPRM), at 10; National Automobile Dealers Association (comment 46), at 17-19; National Independent Automobile Dealers Association (comment 48, NPRM), at 5; ACA International (Comment 45, NPRM), at 8.
[94] *See e.g.*, Brian McManamon, Safeguards Workshop Tr., *supra* note 17, at 78 (estimating that the average annual salary of a CISO can range from $180,000 to upwards of $400,000).
[95] National Automobile Dealers Association (comment 46, NPRM), at 17-19; National Independent Automobile Dealers Association (comment 48, NPRM), at 5; U.S. Chamber of Commerce (comment 33, NPRM), at 10; ACA International (comment 45, NPRM), at 8.
[96] National Automobile Dealers Association (comment 46, NPRM), at 18-19; U.S. Chamber of Commerce (comment 33, NPRM), at 10; ACA International (comment 45, NPRM), at 8.
[97] 84 FR at 13175.

The use of the term "Qualified Individual" is meant to clarify that the only requirement for this designated individual is that he or she be qualified to oversee and enforce the financial institution's information security program. What qualifications are necessary will depend upon the size and complexity of a financial institution's information system and the volume and sensitivity of the customer information that the financial institution possesses or processes. The Qualified Individual of a financial institution with a very small and simple information system will need less training and expertise than a Qualified Individual for a financial institution with a large, complex information system. The exact qualifications will depend on the nature of the financial institution's information system. Each financial institution will need to evaluate its own information security needs and designate an individual with appropriate qualifications to meet those needs.

The Commission believes that, in many cases, financial institutions' current coordinators, whether their own employees or third-party contractors, may be qualified for this role.[98] Because the current Safeguards Rule requires financial institutions to designate an "employee or employees to coordinate your information security program," financial institutions that are in compliance with that Rule will already have one or more information security coordinators. Although the current Rule does not expressly require that these coordinators be qualified for that position, the current Rule requires that a financial institution maintain "appropriate" safeguards, regularly test those safeguards,

[98] Remarks of James Crifasi, Safeguards Workshop Tr., *supra* note 17, at 74 (stating that car dealerships can rely on existing staff for this role); Remarks of Lee Waters, Safeguards Workshop Tr., *supra* note 17, at 78-79 (stating that any dealership with any IT staff at all would have someone who could assume the role of "qualified individual," perhaps requiring some additional research or outside help); Remarks of Rocio Baeza, Safeguards Workshop Tr., *supra* note 17, at 81-82 (stating that companies may use an existing employee for the role and "for any areas where there may be skill gaps, that can be supplemented with either certifications or some type of education.").

and evaluate and adjust the information security program in light of that testing.[99] In order to effectively comply with these ongoing requirements, a financial institution's coordinator must have some level of information security training and knowledge and, therefore, will likely be an appropriate Qualified Individual under the Final Rule. Accordingly, in many cases this amendment to the Rule will not require any additional hiring expenses.

In addition to explicitly requiring that the information security program coordinator be qualified for the role, the Commission proposed to require the designation of a single employee, as opposed to the multiple coordinators allowed by the existing Rule. Some commenters objected to this proposal on the grounds that it would interfere with financial institutions' flexibility in organizing their information security personnel.[100] For example, the Consumer Data Industry Association ("CDIA") commented that the designation of a single coordinator would interfere with financial institutions' ability to organize their program "to share responsibilities among different personnel with different strengths."[101] Similarly, ACA International argued that this requirement would prevent financial institutions from having multiple staff members share responsibilities for information security programs.[102]

---

[99] 16 C.F.R. § 314.4.

[100] National Independent Automobile Dealers Association (comment 48, NPRM), at 5; Consumer Data Industry Association (comment 36, NPRM), at 5; National Association of Dealer Counsel (comment 44, NPRM), at 2; ACA International (comment 45, NPRM), at 7-8; Money Services Round Table (comment 53, NPRM), at 10; Gusto and others (Comment 11, Workshop), at 2; *see also* Remarks of James Crifasi, Safeguards Workshop TR, *supra* note 17, at 74 (stating that "when we're talking about a small and medium business [. . .] we really need to see that 'qualified individual' be a mix of folks").

[101] Consumer Data Industry Association (comment 36, NPRM), at 5.

[102] ACA International (comment 45, NPRM), at 7-8. NPA raised similar concerns. National Pawnbrokers Association (comment 3, Workshop), at 2.

Other commenters argued that the designation of a single individual as the coordinator of the information security program provides no proven benefits over the use of multiple coordinators.[103] Similarly, NADA argued that, while the appointment of a single qualified individual might improve accountability, improving accountability does not improve security.[104] On the other hand, a group of consumer and advocacy groups including the National Consumer Law Center ("NCLC") argued that appointing a single individual as the coordinator of the information security program can increase security and prevent security events based on lack of accountability and poor coordination.[105]

The Commission retains the requirement to designate a single qualified individual, because it believes there are clear benefits to the designation of a single coordinator. Designating a single coordinator to oversee an information security program clarifies lines of reporting in enforcing the program, can avoid gaps in responsibility in managing data security, and improve communication.[106]

The Commission disagrees with the commenter who stated that improved accountability does not lead to improved security. The goal of improving accountability is to ensure that information security staff and financial institution management give the necessary attention and resources to information security. In addition, an individual that

---

[103] Consumer Data Industry Association (comment 36, NPRM), at 5; National Automobile Dealers Association (comment 46, NPRM), at 19; ACA International (comment 45, NPRM), at 8.
[104] National Automobile Dealers Association (comment 46, NPRM), at 19.
[105] National Consumer Law Center and others (comment 58, NPRM), at 3 (arguing that a clear line of reporting with a single responsible individual could have prevented the Equifax consumer data breach).
[106] Remarks of Adrienne Allen, Safeguards Workshop Tr., *supra* note 17, at 182-84 (stating that without a single responsible individual, information security staff "can fall into traps of each relying on someone else to make a hard call. . . [In a program without a single coordinator] issues can sometimes fall through the cracks."); Remarks of Michele Norin, Safeguards Workshop Tr., *supra* note 17, at 184-85 ("I think it's extremely important to have a person in front of the information security program. I think that there are so many components to understand, to manage, to keep an eye on. I think it's difficult to do that if it's part of someone else's job. And so I found that it's extremely helpful to have a person in charge of that program just from a pure basic management perspective and understanding perspective.").

has clear responsibility for the strength of a financial institution's information security program will be accountable to improve the program and ensure that it protects customer information.[107]

The major breach that occurred at national consumer reporting agency Equifax in 2017 demonstrates the importance of clear lines of reporting and accountability in management of information security programs. The U.S. House Committee on Oversight and Government Reform issued a report on the breach that identified Equifax's organization as one of the major causes of the breach.[108] The report indicated that Equifax's division of responsibility for information security between two individuals that reported to two different company officers contributed to failures of communication, oversight, and enforcement that led to millions of consumers' data being compromised.[109] Increasing accountability for individuals and organizations can directly lead to improved security for customer information.

Finally, the Commission does not believe that the requirement to designate a single Qualified Individual would prevent the approach of having multiple people responsible for different aspects of the program, as some commenters asserted. While the Qualified Individual appointed as the coordinator of the information security program would have ultimate responsibility for overseeing and managing the information security program, financial institutions may still assign particular duties and responsibilities to

---

[107] *See e.g.*, Federal Trade Commission Staff Comment on the Preliminary Draft for the NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management (Oct. 24, 2019), at12-14 (suggesting that NIST clarify that one person should be in charge of the program). https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-preliminary-draft-nist-privacy-framework/p205400nistprivacyframeworkcomment.pdf.

[108] U.S. House, Committee on Oversight and Government Reform, Majority Staff Report, The Equifax Data Breach, at 55-62, 115th Congress (Dec. 2018).

[109] *Id.*

other staff members.[110] A financial institution may organize its personnel in teams or share decision making between individuals. Moreover, the Rule does not require that this be the Qualified Individual's sole job–he or she may have other duties. The Rule requires only that one individual assume the ultimate responsibility for overseeing and enforcing the program.

Accordingly, the Final Rule requires designation of a single Qualified Individual, as proposed, but no longer uses the term "CISO."

Third-Party Coordinators

The Proposed Rule stated that the Qualified Individual would not need to be an employee of the financial institution, but could 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, that lack the resources to employ a qualified person to oversee a program, or that decide to pool resources with affiliates to share staff to manage information security. The Proposed Rule required, however, that to the extent a financial institution used a service provider or affiliate, the financial institution must still: 1) retain responsibility for compliance with the Rule; 2) designate a senior member of its personnel to be responsible for direction and oversight of the Qualified Individual; and 3) require the service provider or affiliate to maintain an information security program that protects the financial institution in accordance with the Rule.

The Commission received one comment on this aspect of the provision. NADA argued that, because a senior member of a financial institution's personnel must be responsible for the oversight of a third-party Qualified Individual, the supervising

[110] *See* Remarks of Adrienne Allen, Safeguards Workshop Tr., *supra* note 17, at 189-90 (noting that, even where there is a single point person, decision makers rarely operate "in a vacuum.").

individual would need to be an expert in information security, and the financial institution would still be required to hire an expensive employee to supervise the third-party Qualified Individual.[111] The Rule, however, does not require individuals responsible for overseeing third-party Qualified Individuals to be information security experts themselves. The senior personnel that oversees the third-party Qualified Individual is charged with supervising and monitoring the third-party so that the financial institution is aware of its data security needs and the safeguards being used to protect its information systems. This person does not need to be qualified to coordinate the information security program him or herself. Technical staff are frequently supervised by employees or officers with limited technical expertise.[112] The Rule requires only the same responsibilities that a supervisor would have in overseeing an in-house information security coordinator of a financial institution. Accordingly, the Commission adopts the proposed paragraph without modification.

Proposed paragraph (b)

The NPRM proposed amending paragraph (b) to clarify that a financial institution must base its information security program on the findings of its risk assessment by adding an explicit statement that financial institutions' "information security program [shall be based] on a risk assessment."[113] In addition, the Proposed Rule removed

[111] National Automobile Dealers Association (comment 46, NPRM), at 18.
[112] *See* Remarks of James Crifasi, Safeguards Workshop Tr., *supra* note 17, at 79-80 (stating that, in his work as a third-party information security service provider, he is often overseen by executives without technical backgrounds); *see also* Remarks of Rocio Baeza, Safeguards Workshop Tr., *supra* note 17, at 105-06 (noting distinction in how executives and technical staff may understand their organizations' use of encryption); Remarks of Karthik Rangarajan, Safeguards Workshop Tr., *supra* note 17, at 196 (discussing challenges inherent in discussing technical issues with board members who lack a technical background)and at 211 (noting that organizations can successfully manage their relationships with third-party service providers without "becom[ing] experts" in the services provided).
[113] Proposed 16 CFR 314.4(b).

existing paragraph 314.4(b)'s requirement that the risk assessment must include consideration of specific risks[114] because these specific risks are set forth elsewhere in the Proposed Rule.[115] The Commission received no comments on this paragraph and adopts paragraph (b) as proposed.

Written Risk Assessment

Paragraph (b)(1) of the Proposed Rule required that the risk assessment be written and include: 1) criteria for the evaluation and categorization of identified security risks or threats the financial institution faces; 2) criteria for the assessment of the confidentiality, integrity, and availability of the financial institution's information systems and customer information, including the adequacy of the existing controls in the context of the identified risks or threats to the financial institution; 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 financial institution's risks. Commenters raised several concerns about the Proposed Rule's provisions on risk assessment, none of which merit changes to the Proposed Rule.

First, some commenters objected to the level of specificity of the Proposed Rule, with some arguing that the requirements were too specific, and others arguing that the requirements were not specific enough. With respect to the Proposed Rule being too specific, commenters such as ACA and U.S. Chamber of Commerce argued that it removed financial institutions' flexibility in performing risk assessments.[116] The U.S. Chamber of Commerce contended that, because the criteria are too specific, a risk

[114] Proposed 16 CFR 314.4(b)(1), (b)(2), and (b)(3).
[115] *See, e.g.*, Proposed 16 CFR 314.4(c)(2), (c)(10), and (e).
[116] ACA International (comment 45, NPRM), at 12; U.S. Chamber of Commerce (comment 33, NPRM), at 10.

assessment performed using them would not be "sufficiently risk based."[117] CDIA expressed concern that it was unclear "what level of specificity is required" in the written risk assessment and if detailed risk assessments are required, they "could themselves become a roadmap for a security breach."[118]

In contrast, several other commenters recommended that the Rule set forth more specific criteria for risk assessments. Inpher suggested that the Commission add a requirement that risk assessments require financial institutions to examine "technologies that are deployed by [financial institutions'] information security systems, and evaluate the feasibility" of adopting "privacy enhancing technologies" that would better address vulnerabilities and thwart threats.[119] Inpher also recommended that the Rule require financial institutions to conduct privacy impact assessments with "specific guidelines to review internal data protection standards and adherence to fair information principles."[120] The Princeton Center suggested that the Rule require risk assessments to include threat modeling and adopt the concept of defense in depth.[121] HALOCK Security Labs recommended that the Rule specifically require "a) That risk assessments should evaluate the likelihood of magnitudes of harm that result from threats and errors, b) That risk assessments should explicitly estimate foreseeable harm to consumers as well as to the covered financial institutions, c) That risk mitigating controls are commensurate with the

[117] U.S. Chamber of Commerce (comment 33, NPRM), at 10.
[118] Consumer Data Industry Association (comment 36, NPRM), at 5.
[119] Inpher, Inc. (comment 50, NPRM), at 4.
[120] *Id.*
[121] Princeton University Center for Information Technology Policy (comment 54, NPRM), at 2.

risks they address, [and] d) That risk assessments estimate likelihoods and impacts using available data."[122]

The Commission believes that the Proposed Rule's provisions on risk assessment strike the right balance between specificity and flexibility. The amendments provide only a high-level list of criteria that the risk assessment must address. They essentially require that the financial institution identify and evaluate risks to its systems, evaluate the adequacy of its existing controls for addressing these risks, and identify how these risks can be mitigated. These are core requirements of any risk-assessment.[123] The Rule does not require any specific methodology or approach for performing the assessment. Financial institutions are free to perform the risk assessment using the method that is most suitable for their organization as long as that method meets the general requirements set forth in the Rule. [124] And while the Commission agrees that the additional requirements suggested by some commenters may be beneficial in many, or even most, risk assessments, it believes that a more flexible requirement will better allow financial institutions to find the risk assessment method that best fits their organization and will better accommodate changes in recommended approaches in the future.

---

[122] HALOCK Security Labs (comment 4, Workshop) at 2. *See* Rocio Baeza (comment 12, Workshop) at 2-3 (suggesting a detailed list of requirements for the risk assessment).

[123] *See, e.g.*, Remarks of Chris Cronin, Safeguards Workshop Tr., *supra* note 17, at 25 (stating that evaluating the likelihoods and impacts of potential security risks and evaluating existing controls is an important component of a risk assessment); Remarks of Serge Jorgensen, Safeguards Workshop Tr., *supra* note 17, at 29-30 (emphasizing the importance of risk assessments as tools for adjusting existing security measures to account for both current and future security threats); Nat. Inst. of Sci. & Tech., U.S. Dept. of Com., Special Publication 800-30 Rev. 1, Guide for Conducting Risk Assessments 1 (2012) (describing the purpose of risk assessments as the identification of and prioritization of risk in order to inform decision making and risk response).

[124] ACA International further argued that because risk assessment criteria are generally understood, they do not need to be included in the Final Rule. ACA International (comment 45, NPRM). The Commission believes that it is helpful to be clear about the criteria the risk assessment must contain, even if those criteria are commonly understood.

In response to CDIA's concern about the risk assessment providing a roadmap for bad actors, certainly, the written risk assessment will include details about a financial institution's systems that could assist an attacker if obtained by the attacker. Accordingly, the risk assessment should be protected as any other sensitive information would be. The Commission does not view this concern as a reason not to create such a document. Indeed, the concern would apply to any written document that provides information regarding a financial institution's information security procedures, from a network diagram to written security code.

Second, some commenters argued that implementing the risk-assessment provision as proposed would be too expensive and difficult for financial institutions.[125] For example, NADA argued that the contemplated risk assessment would be very costly because the criteria set out in paragraph (b)(1) are "well outside the scope of expertise of anyone but the most sophisticated IT professionals."[126] In response, although the Commission declines to modify the provision, it addresses NADA's concern in Section 314.6 by exempting financial institutions that maintain information concerning fewer than 5,000 consumers from the specific requirements of (b)(1), and from the requirement to memorialize the risk assessment in writing. For those financial institutions that do not qualify for this exemption, the Commission believes that they will be able to perform the required risk assessment in a manner that is practical and affordable for their institution.

[125] National Association of Dealer Counsel (comment 44, NPRM), at 3; National Automobile Dealers Association (comment 46, NPRM), at 20.
[126] National Automobile Dealers Association (comment 46, NPRM), at 20.

There are many resources available to financial institutions to aid in risk assessment, including service providers that can assist institutions of various sizes.[127]

While acknowledging that there will be some cost to conducting a risk assessment, the Commission believes that a properly conducted risk assessment is an essential part of a financial institution's information security program. The entire Safeguards Rule, both as it currently exists and as amended, requires that the information security program be based on a risk assessment. An information security program cannot properly guard against risks to customer information if those risks have not been identified and assessed.[128] The Commission believes that this requirement properly emphasizes the importance of robust risk assessments, while providing financial institutions sufficient flexibility in performing these assessments. Finally, the Commission notes that, because the current Rule also requires that a risk assessment be performed, financial institutions that have complied with the current Rule have already conducted a risk assessment. And, even if that risk assessment was not memorialized in writing, the work conducted for that risk assessment should be useful in performing future risk assessments.

Third, NADA objected to the requirement that the risk assessment describe how each identified risk will be "mitigated or accepted," arguing that it is not clear when it is

---

[127] *See e.g.*, Slides Accompanying Remarks of Rocio Baeza, in Safeguards Workshop Slides, *supra* note 72, at 27-28 (describing three different compliance models: in-house, outsource, and hybrid, with costs ranging from $199 per month to more than $15,000 per month); Slides Accompanying the Remarks of Brian McManamon, "Sample Pricing," in Safeguards Workshop Slides, *supra* note 72, at 29 (estimating the cost of cybersecurity services based on number of endpoints: $2K-$5K per month for 25-250 endpoints; $5K-$15K for 250-750 endpoints; $15K-$30K for 750-1,000 endpoints; and $30K-$50K for 1,500-2,500 endpoints); *see also* Remarks of Brian McManamon, Safeguards Workshop Tr., *supra* note 17, at 83-85.

[128] *See* Remarks of Chris Cronin, Safeguards Workshop Tr., *supra* note 17, at 48-49 (noting that all information security frameworks and guidelines are based on risk analysis).

appropriate to "accept a risk."[129] NADA argued that documenting a decision to accept a risk would "create a record that can be distorted and second guessed after the fact," and that "context is lost when it is written and reviewed after an incident has occurred."[130] The Rule does not require a financial institution to mitigate every risk identified, no matter how remote or insignificant. Instead, the Rule allows a financial institution to accept a risk, if its assessment of the risk reveals that the chance that it will produce a security event is very small, if the consequences of the risk are minimal, or the cost of mitigating the risk far outweighs the benefit. In those cases, the financial institution may choose to accept the risk. A financial institution that is concerned that its decision to accept a risk will later be questioned may choose to set forth whatever context or explanation it sees fit in the written assessment.

Finally, while several commenters supported the idea of conducting "periodic" risk assessments as required by the Proposed Rule,[131] NADA objected that it is unclear how often financial institutions need to conduct risk assessments under this section.[132] In order to be effective, a risk assessment must be subject to periodic reevaluation to adapt to changes in both financial institutions' information systems and changes in threats to the security of those systems. The Commission declines, however, to set forth a specific schedule for risk assessments. The Commission believes that it would not be appropriate to set forth an inflexible schedule for periodic risk assessments because each financial institution must set its own schedule based on the needs and resources of its institution.

The Final Rule adopts paragraph 314.4(b) as proposed.

---

[129] National Automobile Dealers Association (comment 46, NPRM) at 20.
[130] *Id*.
[131] Inpher, Inc. (comment 50, NPRM), at 3; Global Privacy Alliance (comment 38, NPRM), at 11.
[132] National Automobile Dealers Association (comment 46, NPRM), at 20.

Paragraph (c)

Proposed paragraph (c) retained the existing Rule's requirement for financial institutions to design and implement safeguards to control the risks identified in the risk assessment. In addition, it added more detailed requirements for what the safeguards must address (e.g., access controls, data inventory, disposal, change management, monitoring). These specific requirements represent elements of an information security program that the Commission views as essential and should be addressed by all financial institutions.[133]

As a preliminary matter, Global Privacy Alliance (GPA) argued that all of these elements should be made optional and that financial institutions should be required only to take these elements "into consideration" when designing their information security programs.[134] While the Commission agrees that it is important that the Rule allow financial institutions flexibility in designing their information security programs, these elements are such important parts of information security that each program must address them. For example, an information security program that has no access controls or does not contain any measures to monitor the activities of users on the systems cannot be said to be protecting the financial institution's systems. The Final Rule, therefore, continues

[133] NADA disagreed with the Commission's statement in the NPRM for the Proposed Rule that "most financial institutions already implement" the specific requirements in paragraph (c), stating that many financial institutions "do not currently implement some or all of these measures." National Automobile Dealers Association (comment 46, NPRM), at 20. The Commission continues to believe that most financial institutions institute some form of most of these measures, such as access control, secure disposal, and monitoring authorized users, based on its enforcement and business outreach experience. While NADA's statement that some financial institutions implement none of the measures may be true, this underlines the necessity of making these elements explicit requirements under the Rule, as these elements are necessary for a reasonable information security program for all financial institutions. Indeed, a financial institution that utilizes none of these elements and exercises no access control, no secure disposal procedures, and does not monitor users of its systems is unlikely to be in compliance with the current Rule.

[134] Global Privacy Alliance (comment 38, NPRM), at 6.

to require each information security program to contain safeguards that address these elements, with modifications described below.

Access Controls

Proposed paragraph (c)(1) required financial institutions to "place 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 and to periodically review such access controls."

Commenters suggested a number of modifications to this provision. First, GPA argued that this provision should require controls on access to information, rather than on information systems.[135] Second, several commenters suggested adding further safeguards to the "access control" requirement. For example, the Princeton Center argued that the Rule should adopt the "Principle of Least Privilege," a principle that no user should have access greater than is necessary for legitimate business purposes.[136] Reynolds and Reynolds Company (Reynolds) suggested that the Rule clarify that financial institutions must "vet, control, and monitor user access to sensitive information."[137] Consumer Reports argued that section (c)(1) should be amended to control access not just to authorized users, but to further limit access to when such access is reasonably necessary.[138] ACE argued that any requirement for physical access control allow financial institutions to determine which locations should have restricted access, rather than limiting physical access to every building and office within, say, a college

[135] Global Privacy Alliance (comment 38, NPRM), at 9-10.
[136] Princeton University Center for Information Technology Policy (comment 54, NPRM), at 4-5.
[137] Reynolds and Reynolds Company (comment 7, Workshop), at 7.
[138] Consumer Reports (comment 52, NPRM), at 7.

campus.[139] Finally, some commenters argued that the proposed language was too vague,[140] particularly as it applied to vendor-supplied services.[141]

In response to the comments, the Commission makes a number of changes to this provision in the Final Rule. First, the Commission clarifies that the Rule requires access controls, not just for information systems, but for all customer information, whether it is housed in information systems or in physical locations. To streamline the Rule, the Final Rule combines the separate physical access controls requirement found in proposed paragraph (c)(3) with this paragraph. Physical access controls will generally be most important in situations in which sensitive customer information is kept in physical form (such as hard-copy loan applications, or printed consumer reports). It may also require physical restrictions to access machines that contain customer information (e.g., locked doors and/or key card access to a computer lab).[142] The Commission declines to make any changes in response to ACE's concern that every physical location will need to be protected – as the Rule states, physical controls must be implemented to protect unauthorized access to customer information. Where no customer information exists, the Rule would not require physical controls.

---

[139] American Council on Education (comment 24, NPRM), at 10.

[140] National Automobile Dealers Association (comment 46, NPRM), at 23; National Independent Automobile Dealers Association (comment 48, NPRM), at 5; American Council on Education (comment 24, NPRM), at 10;

[141] National Independent Automobile Dealers Association (comment 48, NPRM), at 5; American Council on Education (comment 24, NPRM), at 10.

[142] NIADA suggested that instituting physical access controls would cost a dealership $215,000 because each computer would need to have its own lockable cubicle and there would need to be lockable offices for all desks. *See* Remarks of Lee Waters, Safeguards Workshop Tr., *supra* note 17, at 76. As originally promulgated, the Rule already requires that financial institutions implement "physical safeguards that are appropriate to your size and complexity." 16 CFR 314.3. The Final Rule's requirement is consistent with that longstanding requirement. If computers have technical safeguards preventing unauthorized users from accessing customer information, they usually will not need to be in a lockable area, particularly if they are not generally left unattended and are not likely to be stolen. Similarly, desks would need to be in lockable offices only if they contain accessible paper records. A lockable file cabinet may be a more economical solution.

Second, the Commission agrees with the commenters who advocated that the Rule implement the principle of least privilege. The Commission does not believe it is appropriate, for example, for larger companies to give all employees and service providers access to all customer information. Such overbroad access could create additional harm in the event of an intruder gaining access to a system by impersonating an employee or service provider. Accordingly, the Commission clarifies this in the Final Rule by adding a requirement that not only must a financial institution implement access controls, but it should also restrict access only to customer information that is needed to perform a specific function.

As to the suggestion that the Commission impose monitoring requirements for access, that requirement exists in paragraph (c)(8). And as to the suggestion that the requirement is too vague as to service providers, the Commission believes the Final Rule is clear: When a vendor accesses the financial institution's data or information systems, the financial institution must ensure that appropriate access controls are in place. Separately, under paragraph (f), the financial institution must reasonably oversee the vendor's safeguards, which would necessarily include access controls for the vendor's system.

Finally, as to the suggestion that the provision is vague generally, as discussed above, the Final Rule seeks to preserve flexibility in its provisions, both so that financial institutions can design programs that are appropriate for their systems and so that changes in technology or security practices will not render the Rule obsolete. The Commission

believes that maintaining less prescriptive requirements is the best way to achieve the goal of flexibility and protecting customer information.[143]

Accordingly, the Commission combines paragraphs (1) and (3) from the Proposed Rule into revised paragraph (1) of the Final Rule, which requires "implementing and periodically reviewing access controls on customer information, including technical and, as appropriate, physical controls to (1) authenticate and permit access only to authorized users to protect against the unauthorized acquisition of customer information and (2) limit authorized users' access only to customer information that they need to perform their duties and functions, or, in the case of customers, to access their own information."[144]

System Inventory

In the NPRM, the Commission proposed to require the financial institution to "[i]dentify and manage the data, personnel, devices, systems, and facilities that enable [the financial institution] to achieve business purposes in accordance with their relative importance to business objectives and [the financial institution's] risk strategy."[145] This requirement was designed to ensure that the financial institution inventoried the data in its possession, inventoried the systems on which that data is collected, stored, or transmitted, and had a full understanding of the relevant portions of its information

[143] NPA expressed concern about the effect of the Rule on pawnbrokers who the commenter stated are required by law to allow law enforcement access to their physical records. National Pawnbrokers Association (comment 32, NPRM), at 7. Nothing in the Rule conflicts with any such requirements. Law enforcement appropriately accessing customer information under a law that requires that access would be considered authorized use under those circumstances.
[144] As noted above, the Commission is also changing the term "authorized individuals" to "authorized users."
[145] Proposed 16 CFR 314.4(c)(2).

systems and their relative importance.[146] The Commission retains this provision in the Final Rule without modification.

Commenters raised two general objections to this provision. First, some commenters argued it was too vague and that it was not clear how such an inventory should be conducted or what systems should be included.[147] The Commission believes that the language provides effective guidance while still allowing a variety of approaches by financial institutions in identifying systems involved in their businesses. This provision requires a financial institution to identify all "data, personnel, devices, systems, and facilities" that are a part of its business and to determine their importance to the financial institution. This inventory of systems must include all systems that are a part of the business so that the financial institution can locate all customer information it controls, the systems that are connected to that information, and how they are connected. This inventory forms the basis of an information security program because a system cannot be protected if the financial institution does not understand its structure or know what data is stored in its systems.

Second, ACE suggested that the scope of this provision should be limited to systems that are "directly related to the privacy and security of 'customer information.'"[148] The Commission declines to make this change because the purpose of this provision is to allow financial institutions to obtain a clear picture of their systems and to identify where customer information is kept and how it can be accessed. An

---

[146] *See, e.g.,* Complaint at 11, *FTC v. Wyndham Worldwide Corp.*, No. CV 2:12-cv-01365-SPL (D. Ariz. June 26, 2012) (alleging that company failed to provide reasonable security by, among other things, failing to inventory computers connected to its network).
[147] National Automobile Dealers Association (comment 46, NPRM), at 23-24; American Financial Services Association (comment 41, NPRM), at 5; American Council on Education (comment 24, NPRM), at 10.
[148] American Council on Education (comment 24, NPRM), at 10.

inventory must examine all systems in order to identify all systems that contain customer information or are connected to systems that do. If a financial institution does not first examine all systems and instead limits the inventory to systems that it considers to be directly related to security, it could give an incomplete picture of the financial institution's systems and could result in some customer information or ways to connect to that information being overlooked.[149]

The Commission adopts paragraph (c)(2) of the Proposed Rule as final, without modifications.

Access to Physical Location

Proposed paragraph (c)(3) would have required that financial institutions restrict access to physical locations containing customer information only to authorized individuals. The Final Rule combines this section with proposed paragraph (c)(1) in order to eliminate redundancy and clarify that access controls must consider both electronic and physical access.

Encryption

Proposed paragraph (c)(4) required financial institutions to encrypt all customer information, both in transit over external networks and at rest. The Proposed Rule allowed financial institutions to use alternative means to protect customer information, subject to review and approval by the financial institution's Qualified Individual.

[149] Another commenter criticized proposed paragraph (c)(2) because some financial institutions "have no control" over which networks they transmit customer information. National Pawnbrokers Association (comment 32, NPRM), at 7. Paragraph (c)(2) does not require a financial system to identify all networks over which it may transmit customer information. *See also*, *infra*, this Notice's discussion of NPA's comments on paragraph 314.4(f) of the Final Rule, noting that financial institutions are generally not required to oversee other entities' service providers over which they have no control.

Several commenters supported the inclusion of an encryption requirement.[150] In fact, some suggested that the Proposed Rule did not go far enough in requiring encryption. Inpher suggested that the Rule should require encryption of customer information when in use, in addition to when in transit or at rest.[151] The Princeton Center suggested requiring encryption of data while in transit over internal networks, in addition to requiring it for external networks, noting the blurring of the distinction between internal and external networks.[152]

In contrast, others argued that encryption could be too expensive and technically challenging for some financial institutions and should not be required in all cases.[153] Indeed, GPA argued that the Rule should not require encryption at all, that financial institutions should be free to adopt other protective measures for customer information, and that the Rule should allow financial institutions to "determine the controls that are most appropriate for protecting the sensitive information that they handle."[154] Similarly, some commenters argued that financial institutions should be required to encrypt customer information only when the risk to the customer information justifies it.[155] Others suggested encryption in more limited circumstances, such as on systems "to which unauthorized individuals may have access,"[156] for sensitive data,[157] or for data in

---

[150] Inpher, Inc. (comment 50, NPRM), at 4; Princeton University Center for Information Technology Policy (comment 54, NPRM), at 3; Electronic Privacy Information Center (comment 55, NPRM), at 8; National Consumer Law Center and others (comment 58, NPRM), at 3.
[151] Inpher, Inc. (comment 50, NPRM), at 4.
[152] Princeton University Center for Information Technology Policy (comment 54, NPRM), at 3.
[153] National Pawnbrokers Association (comment 32, NPRM), at 3; U.S. Chamber of Commerce (comment 33, NPRM), at 11; CTIA (comment 34, NPRM) at 10; Wisconsin Bankers Association (comment 37, NPRM), at 2.
[154] Global Privacy Alliance (comment 38, NPRM), at 7-8.
[155] Bank Policy Institute (comment 39, NPRM), at 14; Mortgage Bankers Association (comment 26, NPRM), at 6; Global Privacy Alliance (comment 38, NPRM), at 7-8.
[156] Bank Policy Institute (comment 39, NPRM), at 14.

transit.[158] The Mortgage Bankers Association argued that encryption at rest is unnecessary because customer information at rest in a financial institution's system is sufficiently protected by controlling access to the system.[159] Two commenters stated that guidelines issued by the Federal Financial Institutions Examination Council (FFIEC) do not require most banks to encrypt data at rest, unless the institution's risk assessment indicates that such encryption is necessary.[160]

The Commission declines to modify the encryption requirement from the Proposed Rule. As to the comments that suggest that the requirement should be relaxed, the Commission notes that there are numerous free or low cost encryption solutions available to financial institutions, particularly for data in transit,[161] that make encryption a feasible solution in most situations. For data at rest, encryption is now cheaper, more

---

[157] U.S. Chamber of Commerce (comment 33, NPRM), at 11; American Financial Services Association (comment 41, NPRM), at 5; ACA International (comment 45, NPRM), at 13; CTIA (comment 34, NPRM), at 10.

[158] Mortgage Bankers Association (comment 26, NPRM), at 6; Wisconsin Bankers Association (comment 37, NPRM), at 2; American Financial Services Association (comment 41, NPRM), at 5; Ken Shaurette (comment 19, NPRM), (suggesting that the Commission consider whether "databases, applications and operating systems are prepared to fully support full encryption without significant performance impact or ability to continue to function."); National Automobile Dealers Association (comment 46, NPRM), at 25-26 (arguing that the terms "at rest" and "in transit" are unclear).

[159] Mortgage Bankers Association (comment 26, NPRM), at 6.

[160] Wisconsin Bankers Association (comment 37, NPRM), at 2 (discussing FFIEC Information Technology Booklet); American Financial Services Association (comment 41, NPRM), at 5 (discussing FFIEC Cybersecurity Assessment Tool).

[161] *See* Remarks of Matthew Green, Safeguards Workshop Tr, *supra* note 17, at 225 (noting website usage of encryption is above 80 percent; "Let's Encrypt" provides free TLS certificates; and costs have gone down to the point that if a financial institution is not using TLS encryption for data in motion, it is making an unusual decision outside the norm); Remarks of Rocio Baeza, Safeguards Workshop Tr., *supra* note 17, at 106 ("[T]he encryption of data in transit has been standard. There's no pushback with that."); *see also* National Pawnbrokers Association (comment 3, Workshop), at 2 ("[I]n states that allow us to use technology for the receipt of information from consumer customers and software to print our pawn tickets and store information, we believe our members have access through their software providers to protections that comply with the Safeguards Rule.").

flexible, and easier than ever before.[162] In many cases, widely used software and hardware have built-in encryption capabilities.[163]

In response to the argument that the Rule should not require encryption at rest because FFIEC guidelines do not require it, the Commission notes that the Safeguards Rule is very different from the guidelines issued by the FFIEC. The depository financial institutions regulated by the banking agencies are subject to regular examinations by their regulator. The guidelines created by the FFIEC are designed to be used by the examiner, as part of those examinations, to evaluate the security of the financial institution; the examiner thus has a direct role in regularly verifying that the financial institution has taken appropriate steps to protect its customer information. In contrast, the Safeguards Rule regulates covered financial institutions directly and must be usable by those entities to determine appropriate information security without any interaction between the financial institution and the Commission. The Commission does not have the ability to examine each financial institution and work with that institution to ensure that their information security is appropriate. Therefore, a requirement that institutions encrypt

---

[162] *See* Remarks of Wendy Nather, Safeguards Workshop Tr., *supra* note 17, at 267 ("we have a lot more options, a lot more technologies today than we did before that are making both of these solutions, both encryption and MFA, easier to use, more flexible, in some cases cheaper, and we should be encouraging their adoption wherever possible."); Remarks of Matthew Green, Safeguards Workshop Tr., *supra* note 17, at 265-66 ("I think that we're in a great time when we've reached the point where we can actually mandate that encryption be used. I mean, years ago -- I've been in this field for 15, you know, 20 years now, I guess. And, you know, encryption used to be this exotic thing that was very, very difficult to use, very expensive and not really feasible for securing information security systems. And we've reached the point where now it is something that's come to be and we can actually build well. So I'm really happy about that.").

[163] *See* Remarks of Randy Marchany, Safeguards Workshop Tr., *supra* note 17, at 229-30 (noting that encryption is already built into the Microsoft Office environment and that a number of Microsoft products, such as Spreadsheets, Excel, Docs, and PowerPoint, support that encryption feature). Other applications that have encryption built in include database applications; app platforms iOS and Android; and development frameworks for web applications on banking sites.

information by default is appropriate for the Safeguards Rule, as the Commission believes that encryption of customer information at rest is appropriate in most cases.

Finally, while some commenters suggested eliminating the encryption requirement for certain types of data (e.g., non-sensitive) or certain categories of data (e.g., data at rest), the Commission notes that, as discussed in more detail above, the fact that an individual is a customer of a financial institution alone may be sensitive. In any event, the Rule provides financial institutions with flexibility to adopt alternatives to encryption with the approval of the Qualified Individual.

Similarly, the Commission declines to *extend* the encryption requirement to data in use or to data transmitted over internal networks, as some commenters suggested. The Commission does not believe that the technology that would encrypt data while in use (as opposed to in transit or at rest) has been adopted widely enough at this time to justify mandating its use by all financial institutions under the FTC's jurisdiction. As to encryption of data transmitted over internal networks, the Commission acknowledges that, due to changes in network design and the growth of cloud and mobile computing, the distinction between internal and external networks is less clear than it once was. However, the Commission believes that requiring all financial institutions to encrypt all communications over internal networks would be unduly burdensome at this time. There remain significant costs and technical hurdles to encrypting transmissions on internal networks that would not be reasonable to impose on all financial institutions, especially smaller institutions with simpler systems that might realize less benefit from this approach. While the Commission encourages financial institutions to consider whether it

would be appropriate for them to encrypt the transmission of customer information over internal networks, it declines to require this for all financial institutions.[164]

Commenters pointed to three additional concerns about encryption, none of which the Commission finds persuasive. First, the Bank Policy Institute commented that the encryption requirement would in fact weaken security by blocking surveillance of the information by the financial institution and requiring the "broad distribution" of encryption keys.[165] The Commission does not believe an encryption requirement would weaken security. Encryption is almost universally recommended by security experts and included in most security standards.[166] Further, new tools have been developed to address the issue that the Bank Policy Institute has raised. Many financial institutions have monitoring tools on the edge of their networks to monitor data leaving the network. It used to be the case that these network monitoring tools could not see the content of encrypted data as it left the corporate network and was transmitted to the Internet. However, there are now tools available that can see the data as it departs the network, even if the data is encrypted.[167] Any marginal security costs of encryption are far outweighed by the benefits of rendering customer information unreadable.

Second, some commenters argued that financial institutions should be able to implement alternatives to encryption without obtaining approval from the Qualified

---

[164] The Commission believes that transmissions of customer information to remote users or to cloud service providers should be treated as external transmissions, as those transmissions are sent out of the financial institution's systems.

[165] Bank Policy Institute (comment 39, NPRM), at 13-14.

[166] *See, e.g., Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures Version 3.2.1*, PCI Security Standards Council (May 2018), https://www.pcisecuritystandards.org/document_library (last accessed 30 Nov. 2020) (Requirement 4 encrypt transmission of cardholder data across open, public networks).

[167] *See, e.g.*, *Encrypted Traffic Management*, Broadcom Inc., https://www.broadcom.com/products/cyber-security/network/encrypted-traffic-management (last accessed 30 Nov. 2020); *SSL Visibility*, F5, Inc., https://www.f5.com/solutions/application-security/ssl-visibility (last accessed 30 Nov. 2020).

Individual.[168] The New York Insurance Association expressed concern that financial institutions might feel they need to encrypt all customer information because of the risk that the alternative controls approved by the Qualified Individual would be "second guessed" in the event that unencrypted data is compromised.[169] The Commission, however, believes that this concern is a core element of information security based on risk assessment. Every aspect of an information security program is based on the judgment of the financial institution and its staff. The Qualified Individual's decision concerning alternate controls, like other decisions by the financial institution and its staff, will be subject to review in any enforcement action to determine whether the decision was appropriate. If the Qualified Individual is not required to make a formal decision, it is much more likely that a decision not to encrypt information will be made even if there is no compensating control, or even made without the Qualified Individual's knowledge.

Third, the National Pawnbrokers Association ("NPA") expressed concern that if pawnbrokers are required to encrypt customer information they may fall out of compliance with state and local regulations concerning transaction reporting.[170] NPA stated that pawnbrokers are often required by state or local law to report every pawn transaction, along with nonpublic personally identifiable consumer information, to law enforcement, and that the agencies that receive this information "prefer to take this information electronically and in unencrypted forms."[171] The Commission believes that if transmitting the information in unencrypted form is a preference of the agencies and

---

[168] Bank Policy Institute (comment 39, NPRM), at 14; New York Insurance Association (comment 31, NPRM), at 1.
[169] New York Insurance Association (comment 31, NPRM) at 1.
[170] National Pawnbrokers Association (comment 3, Workshop), at 2-3.
[171] *Id.* at 2.

not a requirement, then pawnbrokers can comply with both the Safeguards Rule and these laws by encrypting any transmissions that include customer information. If there are cases where a required transmission of customer information cannot be encrypted for technical reasons, then the pawnbroker's Qualified Individual will need to work with the law enforcement agency to implement alternative compensating controls to ensure that the customer information remains secure during these transmissions.[172]

The Final Rule adopts this paragraph as paragraph (c)(3) without revision.

Secure Development Practices

Proposed paragraph (c)(5) required financial institutions to "[a]dopt secure development practices for in-house developed applications utilized" for "transmitting, accessing, or storing customer information." In this paragraph, the Commission proposed requiring financial institutions to address the security of software they develop to handle customer information, as distinct from the security of their networks that contain customer information.[173] In addition, the Proposed Rule required "procedures for evaluating, assessing, or testing the security of externally developed applications [financial institutions] utilize to transmit, access, or store customer information." This

[172] NADA suggested that it is not clear how the encryption requirement will apply to customer information held on a service provider's system or on the systems of the subcontractors of the service provider. National Automobile Dealers Association (comment 46, NPRM), at 21-22. The Commission believes that the Final Rule lays out a financial institution's obligations in this situation: it requires that customer information be encrypted unless infeasible. Paragraph 314.4(e), in turn, requires financial institutions to require service providers to implement and maintain appropriate safeguards by contract and to periodically assess the continued adequacy of those measures. A financial institution that uses a service provider to store and process customer information must require that service provider to encrypt that information and periodically determine whether it continues to do so. If it is infeasible for the service provider to meet these requirements then the financial institution's Qualified Individual must work with the service provider to develop compensating controls or cease doing business with the service provider.

[173] *See, e.g.*, Complaint, *FTC v. D-Link Systems, Inc.*, No. 3:17-CV-00039-JD (N.D. Cal. March 20, 2017) (alleging that company failed to provide reasonable security when it failed to adequately test the software on its devices).

provision required financial institutions to take steps to verify that applications they use to handle customer information are secure.[174]

Some commenters argued that evaluating the security of externally developed software would be too expensive or impractical for some financial institutions,[175] while others raised different concerns. The American Council on Education suggested that, in cases in which a financial institution cannot obtain access to a software provider's code or technical infrastructure, then evaluating the security of its software is infeasible.[176] NADA further suggested that in order to evaluate the security of software, financial institutions would need to hire an expensive IT professional.[177]

The Commission does not agree with these assertions. Evaluating the security of software does not require access to the source code of that software or access to the provider's infrastructure. For example, a provider can supply the steps it took to ensure that the software was secure, whether it uses encryption to transmit information, and the results of any testing it conducted. In addition, there are third party services that assess software. An institution can also set up automated searches regarding vulnerabilities, patches, and updates to software listed on the financial institution's inventory. The exact nature of the evaluation required will depend on the size of the financial institution and the amount and sensitivity of customer information associated with the software. If the software will be used to handle large amounts of extremely sensitive information, then a more thorough evaluation will be warranted. Likewise, the nature of the software used

---

[174] *See, e.g.*, Complaint, *Lenovo*, FTC No. 152-3134 (January 2, 2018) (alleging that company failed to provide reasonable security by failing to properly assess and address security risks caused by third-party software).
[175] American Council on Education (comment 24, NPRM), at 11; National Automobile Dealers Association (comment 46, NPRM), at 26-27.
[176] American Council on Education (comment 24, NPRM), at 11.
[177] National Automobile Dealers Association (comment 46, NPRM), at 26-27.

will also affect the evaluation. Software that has been thoroughly tested by third parties may need little more than a review of the test results, while software that has not been widely used and tested will require closer examination.

The Commission adopts proposed paragraph (c)(5) as paragraph (c)(4) of the Final Rule.

Multi-Factor Authentication

Proposed paragraph (c)(6) required financial institutions to "implement multi-factor authentication for any individual accessing customer information" or "internal networks that contain customer information."[178] The Proposed Rule would have allowed financial institutions to adopt a method other than multi-factor authentication that offers reasonably equivalent or more secure access controls with the written permission of its Qualified Individual. In the Final Rule, the Commission retains the general requirements of proposed paragraph (c)(6) as paragraph (c)(5), with some modifications described below.

Although several commenters expressed support for including a multi-factor authentication requirement in the Final Rule,[179] others opposed such a requirement. For example, ACE argued that a blanket requirement mandating multi-factor authentication for all institutions of all sizes and complexities is not the best solution.[180] The National Independent Automobile Dealers Association (NIADA) commented that the costs of multi-factor authentication would be too high for some financial institutions because it

---

[178] Proposed 16 CFR 314.4(c)(6).
[179] Justine Bykowski (comment 12, NPRM); Princeton University Center for Information Technology Policy (comment 54, NPRM). at 6-7; Electronic Privacy Information Center (comment 55, NPRM). at 8; National Consumer Law Center and others (comment 58, NPRM), at 2; *see also* Remarks of Wendy Nather, Safeguards Workshop Tr., *supra* note 17, at 240-41 (discussing the security poverty line).
[180] American Council on Education (comment 24, NPRM), at 11-12.

would need to be built into their information systems from scratch.[181] NIADA also argued that adopting multi-factor authentication would disrupt a financial institution's activities as employees had to "jump through multiple hoops to log in."[182] Cisco Systems, Inc. argued that while multi-factor authentication is an effective safeguard, it should not be specifically required by the Rule because, while it is currently good security practice, in the future multi-factor authentication may become outdated, and that allowing financial institutions to satisfy the Rule in this way could result in inadequate protection.[183]

Other commenters did not dispute the benefits of multi-factor authentication generally, but argued that the Rule should limit the multi-factor authentication requirement. Some of these commenters stated that the Rule should only require multi-factor authentication when the financial institution's risk assessment justifies it.[184] Others argued that there should be a distinction between internal access and external access. For example, some commenters argued that the Rule should not require multi-factor authentication when a user accesses customer information from an internal network,[185] because there are other controls on internal access that make multi-factor

[181] National Independent Automobile Dealers Association (comment 48, NPRM), at 6; *see also* Ken Shaurette (comment 19, NPRM) (questioning whether multi-factor authentication is appropriate for all financial institutions).
[182] National Independent Automobile Dealers Association (comment 48, NPRM), at 6.
[183] Cisco Systems, Inc. (comment 51, NPRM), at 2-4.
[184] Bank Policy Institute (comment 39, NPRM), at 11-13; Global Privacy Alliance (comment 38, NPRM), at 8.
[185] Electronic Transactions Association (comment 27, NPRM), at 3 n.1; U.S. Chamber of Commerce (comment 33, NPRM), at 11; CTIA (comment 34, NPRM), at 11; Global Privacy Alliance (comment 38, NPRM), at 8; Bank Policy Institute (comment 39, NPRM), at 12; National Automobile Dealers Association (comment 46, NPRM), at 28; National Independent Automobile Dealers Association (comment 48, NPRM), at 6; New York Insurance Association (comment 31, NPRM), at 1.

authentication unnecessary.[186] Another commenter stated that requiring multi-factor authentication when a customer accesses their information from an external network could create problems for some institutions.[187] Finally, the Princeton Center argued that the Rule should be amended to clarify that multi-factor authentication should be required for internal and external networks.[188]

Finally, CTIA took issue with the proposed requirement that the Qualified Individual be permitted to approve "reasonably equivalent or more secure" controls if multi-factor authentication is not feasible, suggesting instead that Qualified Individuals be permitted to approve "effective alternative compensating controls."[189]

The Commission disagrees with the commenters who stated that the Rule should not include a multi-factor authentication requirement. As to costs, many affordable multi-factor authentication solutions are available in the marketplace.[190] Most financial institutions will be able to find a solution that is both affordable and workable for their

---

[186] CTIA (comment 34, NPRM), at 11; Electronic Transactions Association (comment 27, NPRM), at 3 n.1; U.S. Chamber of Commerce (comment 33, NPRM), at 11.
[187] American Council on Education (comment 24, NPRM), at 11.
[188] Princeton University Center for Information Technology Policy (comment 54, NPRM), at 6-7; *see also* Remarks of Brian McManamon, Safeguards Workshop Tr., *supra* note 17, at 102 (stating that his company TECH LOCK supports requiring multi-factor authentication for users connecting from internal networks).
[189] CTIA (comment 34, NPRM), at 11-12; *see also* Electronic Transactions Association (comment 27, NPRM) at 3 (suggesting use of the term "alternative compensating controls").
[190] *See, e.g.*, Slides Accompanying Remarks of Brian McManamon, "MFA/2FA Pricing (Duo)," in Safeguards Workshop Slides, *supra* note 72, at 30 (setting forth prices for multi-factor/two-factor services from Duo, including free services for up to ten users); Remarks of Brian McManamon, Safeguards Workshop Tr., *supra* note 17, at 102-03; Slides Accompanying Remarks of Lee Waters, "Estimated Costs of Proposed Changes," in Safeguards Workshop Slides, *supra* note 72, at 26 estimating costs of MFA to be $50 for smartcard or fingerprint readers, and $10 each per smartcard); Slides Accompanying Remarks of Wendy Nather, "Authentication Methods by Industry," in Safeguards Workshop Slides, *supra* note 72, at 37 (chart showing the use of MFA solutions such as Duo Push, phone call, mobile passcode, SMS passcode, hardware token, Yubikey passcode, and U2F token in industries such as financial services and higher education); Remarks of Wendy Nather, Safeguards Workshop Tr., *supra* note 17, at 233-34.

organization. In the cases when that it is not possible, the Rule allows financial institutions to adopt reasonably equivalent controls.[191]

As to potential disruptions that requiring multi-factor authentication may cause, the Commission notes that many organizations, both financial institutions and otherwise, currently require employees to use multi-factor authentication without major disruption.[192] Many multi-factor authentication systems are available that do not materially increase the time it takes to log into a system as compared to the use of only a password.[193] In short, multi-factor authentication is an extremely effective way to prevent unauthorized access to a financial institution's information system,[194] and its benefits generally outweigh any increased time it takes to log into a system. In those situations when the need for quick access outweighs the security benefits of multi-factor authentication, the Rule allows the use of reasonably equivalent controls.

Finally, although the Commission agrees that the Rule should not lock financial institutions into using outmoded or obsolete technologies, the basic structure of using multiple factors to identify a user is unlikely to be rendered obsolete in the near future.

---

[191] *See also* Remarks of James Crifasi, Safeguards Workshop Tr., *supra* note 17, at 103-04 (noting that even where legacy systems do not support multi-factor authentication, alternative measures can be used and "it's things that can easily be done.")

[192] *See, e.g.*, Remarks of Randy Marchany, Safeguards Workshop Tr., *supra* note 17, at 236-38 (describing how Virginia Tech implemented multi-factor authentication in 2016 for its more than 156,000 users); Slides Accompanying Remarks of Wendy Nather, "Authentication Methods by Industry," in Safeguards Workshop Slides, *supra* note 72, at 37 demonstrating the types of multi-factor authentication used by health care, financial services, higher education and the federal government); Remarks of Wendy Nather, Safeguards Workshop Tr., *supra* note 17, at 233-35.

[193] *See* Remarks of Wendy Nather, Safeguards Workshop Tr., *supra* note 17, at 234 (describing how a phone call to a landline is popular in some segments).

[194] *See, e.g.*, Remarks of Matthew Green, Safeguards Workshop Tr., *supra* note 17, at 266 (explaining that passwords are not enough of an authentication feature but when MFA is used and deployed, the defenders can win against attackers); *id*. at 239 (describing how because smart phones have modern secure hardware processors, biometric sensors and readers built in, increasingly consumers can get the security they need through the devices they already have by storing cryptographic authentication keys on the devices and then using the phone to activate them).

The Rule's definition of multi-factor authentication addresses only this principle and does not require any particular technology or technique to achieve it. This should allow it to accommodate most changes in information security practices. In the event of an unforeseen change to the information security environment that would discount the value of multi-factor authentication, the Commission will adjust the Rule accordingly.[195]

The Commission agrees with the commenter who stated that multi-factor authentication is justified both when external users, such as customers, and internal users, such as employees, access an information system. Multi-factor authentication can prevent many attacks focused on using stolen passwords from both employees and customers to access customer information. Other common attacks on information systems, such as social engineering or brute force password attacks, target employee credentials and use those credentials to get access to an information system.[196] These attacks can usually be stopped through the use of multi-factor authentication. Accordingly, the Final Rule requires multi-factor authentication whenever any individual -- employee, customer or otherwise -- accesses an information system. If a financial

---

[195] The Mortgage Bankers Association expressed concern that the Proposed Rule would not allow the use of a single-sign on process, where a user is given access to multiple applications with the use of one set of credentials. Mortgage Bankers Association (comment 26, NPRM), at 7. The Commission does not view the Rule as preventing such a system, if the user has used multi-factor authentication to access the system and the system is designed to ensure that any user of a given application has been subjected to multi-factor authentication.

[196] *See* Remarks of Pablo Molina, Safeguards Workshop Tr., *supra* note 17, at 30 (mentioning "phishing," or social engineering, as a common type of cybersecurity attack); Remarks of Lee Waters, Safeguards Workshop, *supra* note 17, at 91 (same); Remarks of Michele Norin, Safeguards Workshop Tr., *supra* note 17, at 179 (same); *see also* Cyber Div., Fed. Bureau of Investigation, *Private Industry Notification No. 20200303-001*, *Cyber Criminals Conduct Business Email Compromise through Exploitation of Cloud-Based Email Services, Costing US Businesses Over Two Billion Dollars*, (March 2020), https://www.ic3.gov/media/news/2020/200707-4.pdf, at 1-2, (last accessed 1 Dec. 2020) ("Between January 2014 and October 2019, the Internet Crime Complaint Center (IC3) received complaints totaling over $2.1 billion in actual losses from [Business Email Compromise ("BEC")] scams targeting the largest [cloud-based email] platforms. Losses from BEC scams overall have increased every year since IC3 began tracking the scam in 2013 and have been reported in all 50 states and in 177 countries.").

institution determines that it is not the best solution for its information system, it may adopt reasonably equivalent controls with the approval of the Qualified Individual.

The Commission recognizes that the language of the Proposed Rule may have created some confusion by its use of the term "internal networks" to define the systems affected by the multi-factor authentication requirement, instead of the term "information systems" as used other places in the Rule.[197] In addition, the Commission agrees with commenters that argued that separating the multi-factor authentication into two sentences created confusion.[198] Accordingly, the Commission modifies paragraph (c)(5) of the Final Rule, which was proposed as paragraph (c)(6), to require financial institutions to "[i]mplement multi-factor authentication for any individual accessing any information system, unless your Qualified Individual has approved in writing the use of reasonably equivalent or more secure access controls."

Finally, the Commission declines to adopt CTIA's proposed alternative that would allow Qualified Individuals to approve "effective alternative compensating controls," even if they are not "reasonably equivalent or more secure" than multi-factor authentication. Given the important role that multi-factor authentication has in access control, any alternative measure should provide at least as much protection as multi-factor authentication.[199]

---

[197] Consumer Data Industry Association (comment 36, NPRM), at 6-7; Cisco Systems, Inc. (comment 51, NPRM), at 3-4.
[198] Bank Policy Institute (comment 39, NPRM), at 11.
[199] NADA argued that, for financial institutions that have appointed a third party to act as their information security coordinator, this provision would require the institution to turn over decisionmaking to someone "with no stake in the business outcome." National Automobile Dealers Association (comment 46, NPRM), at 29-30. This concern misinterprets the role of the Qualified Individual. Whether the Qualified Individual is inside the company or at a third-party company, that individual will report to and be supervised by senior management of a financial institution (unless the Qualified Individual is the head of the financial institution). If a Qualified Individual recommends a safeguard that would not be practical for the business,

Audit Trails

Proposed paragraph (c)(7) required information security programs to include audit trails designed to detect and respond to security events.[200] Audit trails are chronological logs that show who has accessed an information system and what activities the user engaged in during a given period.[201]

Some commenters supported this requirement.[202] The Princeton Center noted that audit trails are "crucial to designing effective security measures that allow institutions to detect and respond to security incidents."[203] It also stated that audit trails "help understand who has accessed the system and what activities the user has engaged in."[204]

Other commenters argued that this requirement imposed unclear obligations or would not improve security.[205] For example, GPA commented that the Proposed Rule conflated the use of logs to reconstruct past events and the active use of logs to monitor user activity.[206] The American Financial Services Association argued that adding logging capabilities to some legacy systems would be expensive and difficult.[207] Another commenter argued that the increased use of cloud storage would mean that financial

---

the financial institution is not required to adopt this safeguard but can use an alternative adequate safeguard that will be functional. Indeed, when it comes to third parties, the Rule specifically requires that someone in the financial institution direct and oversee the third party.

[200] Proposed 16 CFR 314.4(c)(7).

[201] *See* Information Technology Laboratory Computer Security Resource Center, *Glossary*, National Institute of Standards and Technology, https://csrc.nist.gov/glossary/term/audit-trail (last accessed Dec. 2, 2020).

[202] Princeton University Center for Information Technology Policy (comment 54, NPRM), at 8; Electronic Privacy Information Center (comment 55, NPRM), at 8.

[203] Princeton University Center for Information Technology Policy (comment 54, NPRM), at 8.

[204] *Id.*

[205] National Automobile Dealers Association (comment 46, NPRM), at 30-31; National Independent Automobile Dealers Association (comment 48, NPRM), at 6; American Financial Services Association (comment 41, NPRM), at 6; Global Privacy Alliance (comment 38, NPRM), at 11.

[206] Global Privacy Alliance (comment 38, NPRM), at 11.

[207] American Financial Services Association (comment 41, NPRM), at 6.

institutions might not have access to any audit trails.[208] In addition, NADA argued that it did not believe maintenance of logs would increase security but would instead create records that could be sought by parties "seeking to place blame" for breaches.[209]

The Commission believes that logging user activity is a crucial component of information security because in the event of a security event it allows financial institutions to understand what was accessed and when. However, the term "audit trails" may have been unclear in this context. In order to clarify that logging user activity is a part of the user monitoring process, the Final Rule does not include paragraph (c)(7) of the Proposed Rule and instead modifies the user monitoring provision to include a requirement to log user activity.[210] By putting the "monitoring" and "logging" requirements together, the Final Rule provides greater clarity on the comment raised by the GPA: Financial institutions are expected to use logging to "monitor" active users and reconstruct past events.

Disposal Procedures

Proposed paragraph (c)(8) required financial institutions to develop procedures for the secure disposal of customer information that is no longer necessary for their business operations or other legitimate business purposes.[211] The Proposed Rule allowed the retention of information when retaining the information is required by law or where targeted disposal is not feasible.

---

[208] American Council of Education (comment 24, NPRM), at 12.
[209] National Automobile Dealers Association (comment 46, NPRM), at 30-31.
[210] *See* Final Rule, 16 CFR 314.4(c)(8).
[211] Proposed 16 CFR 314.4(c)(8).

Some commenters supported the inclusion of a disposal requirement as proposed or suggested that the disposal requirements should be strengthened.[212] Consumer Reports argued that financial institutions should be required to dispose of customer information when it is no longer needed for the business purpose for which it was gathered.[213] The Princeton Center suggested that the Rule require disposal after a set period unless the company can demonstrate a current need for the data and that financial institutions periodically review their data practices to minimize their data retention.[214]

Several other commenters opposed the disposal requirement as set forth in the Proposed Rule. Some argued that the requirement to dispose of information goes beyond the Commission's authority under the GLB Act.[215] NADA argued that the GLB Act does not "contain[] any authority to require financial institutions to delete any information" and that a requirement to have procedures to delete information for which a company has no legitimate business purpose would constitute a "new privacy regime."[216] The American Financial Services Association (AFSA) stated that the requirement was too prescriptive and that the Rule should allow financial institutions to retain information as long as that retention complies with the retention policy created by the financial institution.[217] AFSA further argued that the proposed requirement exceeds the federal banking standards, pointing to the FFIEC Cybersecurity Assessment Tool, which sets

[212] Princeton University Center for Information Technology Policy (comment 54, NPRM), at 8; Electronic Privacy Information Center (comment 55, NPRM), at 8; Consumer Reports (comment 52, NPRM), at 7.
[213] Consumer Reports (comment 52, NPRM), at 7-8.
[214] Princeton University Center for Information Technology Policy (comment 54, NPRM), at 8-9.
[215] National Automobile Dealers Association (comment 46, NPRM), at 31; National Independent Automobile Dealers Association (comment 48, NPRM), at 6.
[216] National Automobile Dealers Association (comment 46, NPRM), at 31-32.
[217] American Financial Service Association (comment 41, NPRM), at 6.

disposal of records "according to documented requirements and within expected time frames" as a baseline requirement for access and data management.[218]

Yet other commenters suggested modifying the requirement. NADA argued that if there was to be a disposal requirement, then it should be modeled after the Disposal Rule, which requires businesses to properly dispose of consumer reports, but does not have an explicit requirement to dispose of information on any particular schedule.[219] ACE suggested modifying the Proposed Rule to require disposal of information only where there is no longer any "legitimate purpose" rather than any "legitimate business purpose."[220] It argued that in some cases a financial institution may have legitimate purposes for retaining information that are not readily defined as "business" purposes, such as the retention of data by educational institutions for institutional research or student analytics.[221]

The Commission believes that requiring the disposal of customer information for which the financial information has no legitimate business purpose is within the authority granted by the GLB Act to protect the security of customer information. The disposal of records, both physical and digital, can result in exposure of customer information if not performed properly.[222] Similarly, if records are retained when they are no longer necessary, there is a risk that those records will be subject to unauthorized access. The risk of unauthorized access may be reasonable where the retention of data provides some

---

[218] *Cybersecurity Assessment Tool*, FFIEC, https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017_Cybersecurity_Maturity_June2.pdf at 37 (last visited December 3, 2020).
[219] National Automobile Dealers Association (comment 46, NPRM), at 32.
[220] American Council on Education (comment 24, NPRM), at 12.
[221] *Id.*
[222] *See, e.g.*, Complaint, *Rite Aid Corp.*, FTC No. 072-3121 (November 22, 2010) (alleging that company failed to provide reasonable data security when it failed to implement policies and procedures to dispose securely of personal information).

benefit. In situations where the information is no longer needed for a legitimate business purpose, though, the risk to the customer information becomes unreasonable because the retention is no longer benefiting the customer or financial institution. Disposing of unneeded customer information, therefore, is a vital part of protecting customer information and serves the purpose of the GLB Act.[223]

The Commission disagrees with commenters who suggested narrowing the disposal requirement or doing away with it altogether. As noted above, although no disposal requirement appears in FFIEC guidelines, those guidelines represent a different regulatory approach and are not an appropriate model for the Safeguards Rule.

Finally, as to setting retention periods or narrowing the legitimate business purposes for which financial institutions may retain customer information, the Commission recognizes that financial institutions need some flexibility. Whereas customers may want to, for example, access and transfer older data in some circumstances, in other circumstances, retaining such data would not be consistent with any legitimate business purpose. The Commission believes that the Princeton Center's recommendation that companies be required to delete information after a set period unless the information is still needed for a legitimate business purpose properly balances the needs of financial institutions with the need to protect customer information. Thus, the Commission modifies proposed paragraph (c)(6) to require the deletion of 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 required for a

[223] As to the Princeton Center's suggestion that financial institutions periodically review their disposal practices (Princeton University Center for Information Technology Policy (comment 54, NPRM), at 8-9), the Commission believes that this requirement is already encompassed in the requirement contained in paragraph 314.4(g) to periodically review their safeguards overall.

legitimate business purpose as paragraph (c)(6)(1) of the Final Rule. In addition, paragraph (c)(6)(2) of the Final Rule requires financial institutions to periodically review their policies to minimize the unnecessary retention of information.

Change Management

Proposed paragraph (c)(9) required financial institutions to adopt procedures for change management.[224] Change management procedures govern the addition, removal, or modification of elements of an information system.[225] This paragraph required financial institutions to develop procedures to assess the security of devices, networks, and other items to be added to their information system, or the effect of removing such items or otherwise modifying the information system. For example, a financial institution that adds additional servers or other machines to its information system would need to evaluate the security of the new devices and the effect of adding them to the existing network.

Some commenters supported this requirement,[226] while others stated that it was too broad and would impose unnecessary burdens on financial institutions.[227] In particular, NADA argued that financial institutions that have not made changes in their systems "for some time" should not be required to create procedures for change management.[228] ACE argued that including a change management requirement is unnecessary because such a requirement is "generally incorporated into an organization's

[224] Proposed 16 CFR 314.4(c)(9).
[225] *See, e.g.*, *Change Management*, Rutgers OIT Information Security Office, https://rusecure.rutgers.edu/content/change-management (last accessed 1 Dec. 2020).
[226] Electronic Privacy Information Center (comment 55, NPRM), at 8; National Consumer Law Center and others, (comment 58, NPRM) at 3.
[227] American Council on Education (comment 24, NPRM), at 12-13; National Automobile Dealers Association (comment 46, NPRM), at 33.
[228] National Automobile Dealers Association (comment 46, NPRM), at 32-33.

IT operations" for non-security purposes and that the security considerations of those changes will be considered as part of those procedures.[229]

Alterations to an information system or network introduce heightened risk of cybersecurity incidents;[230] thus, it is important to expressly require change management to be a part of an information security program. The Commission agrees with ACE that many financial institutions will already have change management procedures in place. If those procedures adequately consider security issues involved in the change, then they may satisfy this requirement.

As to the comment that a financial institution that has not made changes to its environment in some time should not be required to have change management processes, the Commission disagrees. Few information systems can remain unchanged for a significant period of time, given the changing technical requirements for business and security. Indeed, NADA acknowledges that financial institutions will need to "adapt[] their programs to keep up with changes in data security."[231] For this reason, all financial institutions must have procedures for when the changes occur. As with all of the requirements of the Rule, though, the exact nature of these procedures will vary depending on the size, complexity and nature of the information system. A simple system may have equally simple change management procedures.

---

[229] American Council on Education (comment 24, NPRM), at 12.
[230] *See* Remarks of Rocio Baeza, Safeguards Workshop Tr., *supra* note 17, at 95 ("[E]very time there is a change to any of these [network] environments, that is creating additional risk."); Remarks of Scott Wallace, Safeguards Workshop Tr., *supra* note 17, at 147-48 (giving an example of an incident in which network changes led to the exposure of sensitive information); Remarks of Matthew Green, Safeguards Workshop Tr., *supra* note 17, at 252 (noting that it is "a little dangerous" to make "major changes" to an information system at a time of heightened stress).
[231] National Automobile Dealers Association (comment 46, NPRM), at 33 n.96.

The Commission adopts this proposed paragraph as paragraph (c)(7) of the Final Rule without change.

System Monitoring

Proposed paragraph (c)(10) required financial institutions to implement policies and procedures designed "to monitor the activity of authorized users and detect unauthorized access or use of, or tampering with, customer information by such users."[232] The Proposed Rule required financial institutions to take steps to monitor those users and their activities related to customer information in a manner adapted to the financial institution's particular operations and needs.

NADA stated that this requirement would create unnecessary expense because it would require financial institutions to "continually monitor all authorized use" and would mean "yet more new employees or third-party IT consultants."[233] The Commission disagrees, however, noting that monitoring of system use can be automated.[234] There is no requirement that a separate staff member would be required to exclusively monitor system use.

In addition, one commenter stated that monitoring the use of paper files is impossible and should be excluded from this provision.[235] The Commission acknowledges that monitoring of paper records is qualitatively different than the monitoring of electronic records. This requirement goes hand in hand with limiting access to documents, whether electronic or paper. For example, if an institution has a file room and access to the room is limited to particular employees (e.g., the payroll office),

---

[232] Proposed 16 CFR 314.4(c)(10).
[233] National Automobile Dealer Association (comment 46, NPRM), at 33.
[234] *See* Remarks of Nicholas Weaver, Safeguards Workshop Tr., *supra* note 17, at 124-25.
[235] American Financial Services Association (comment 41, NPRM), at 6.

the institution should have measures in place to ensure that those access controls are in fact being utilized (e.g., sign in with front desk, logging of key card access, security camera).

As discussed above, this paragraph is amended to also require the logging of user activity, but is otherwise adopted as proposed as paragraph (c)(8).

Proposed paragraph (d)

Proposed paragraph (d)(1) retained the current Rule's requirement that financial institutions "[r]egularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures, including those to detect actual and attempted attacks on, or intrusions into, information systems."

Proposed paragraph (d)(2) provided further detail to this requirement by stating that the monitoring must take the form of either "continuous monitoring" or "periodic penetration testing and vulnerability assessments." The proposal explained that continuous monitoring is any system that allows real-time, ongoing monitoring of an information system's security, including monitoring for security threats, misconfigured systems, and other vulnerabilities.[236] For those who elected to engage in periodic penetration testing and vulnerability assessment, the proposal required penetration testing at least once annually (or more frequently if called for in the financial institution's risk assessment) and vulnerability assessments at least twice a year.[237]

Some commenters thought the proposal went too far in requiring continuous monitoring or penetration and vulnerability testing, while others thought the proposal did

[236] Financial institutions that choose the option of continuous monitoring would also be satisfying 314.4(c)(8).
[237] Proposed 16 CFR 314.4(d)(1) and (2).

not go far enough. On one hand, ACE argued that continuous monitoring is too burdensome and difficult for some financial institutions,[238] particularly those with "highly decentralized systems," such as colleges and universities, which could be required to monitor their entire system.[239] ACE further suggested that the Rule should not prescribe any particular testing methodology or schedule and should allow financial institutions to develop a testing approach that is appropriate for the financial institution.[240] The NPA commented that penetration and vulnerability testing would be too expensive for small pawnbrokers with small staffs and a small customer base, where their members would be "likely to notice a penetration of our records."[241] One commenter stated that the requirements for monitoring and testing were "overlapping and confusing" and suggested that the Commission avoid confusion by including continuous monitoring, penetration testing, vulnerability scanning, periodic risk assessment reviews, and logging as optional components of an information security program to be included on an as-needed basis.[242] Some commenters recommended that the testing requirement be limited to electronic data and exclude monitoring of physical data.[243] The American Financial Services Association argued that the testing of physical safeguards required by paragraph (d)(1) "would be impossible."[244] Finally, CTIA argued that, for entities that

[238] American Council on Education (comment 24, NPRM), at 13-14.
[239] American Council on Education (comment 24, NPRM), at 13.
[240] American Council on Education (comment 24, NPRM), at 14.
[241] National Pawnbrokers Association (comment 3, Workshop), at 2.
[242] Global Privacy Alliance (comment 38, NPRM), at 10-11.
[243] National Independent Automobile Dealers Association (comment 48, NPRM), at 6; American Financial Services Association (comment 41, NPRM), at 6.
[244] American Financial Services Association (comment 41, NPRM), at 6.

choose the approach of penetration and vulnerability testing, these tests should be required less regularly.[245]

On the other hand, the Princeton Center suggested that, rather than requiring either continuous monitoring or penetration testing, the Rule should require both. It noted that continuous monitoring is very effective at detecting problems with, and threats to, "off-the-shelf systems" but that penetration testing is better at "for checking the interaction between systems, proprietary systems, or subtle security issues."[246] Similarly, the MSRT was concerned that the Proposed Rule suggested that annual penetration testing alone could protect financial institutions, rather than serve as a supplement to proper monitoring.[247]

The Commission agrees with commenters who pointed out the difficulty of applying certain testing requirements to physical safeguards. Although the general testing requirement set forth in paragraph (d)(1) should apply to physical safeguards (e.g., testing effectiveness of physical locks), the continuous monitoring, vulnerability assessment, and penetration testing in (d)(2) is not relevant to information in physical form. Accordingly, the final version of (d)(2) is limited to safeguards on information systems.

The Commission also agrees that biannual vulnerability testing may not be sufficient to detect new threats. Thus, given the relative ease with which vulnerability assessments can be performed, it modifies the Final Rule to require financial institutions

---

[245] CTIA (comment 34, NPRM) at 12-13 (arguing that penetration testing should be required only once every two years and that vulnerability testing be required only once a year).
[246] Princeton University Center for Information Technology Policy (comment 54, NPRM), at 5.
[247] Money Services Round Table (comment 53, NPRM), at 9; *see also* Gusto and others (Comment 11, Workshop), at 2 (arguing that penetration testing and vulnerability assessments both have their weaknesses and financial institutions should develop a testing program that it is appropriate for them).

to perform assessments when there is an elevated risk of new vulnerabilities having been introduced into their information systems, in addition to the required biannual assessments.

Beyond these modifications, the Commission believes that the proposal struck the right balance between flexibility and protection of customer information, and adopts the proposed provision as final. For commenters concerned about costs of testing and continuous monitoring, the Commission notes that the Rule requires one, not both. Although many financial institutions may choose to use both, the Commission agrees that the costs of requiring both for all financial institutions may not be justified. [248] As to arguments that the testing required by the Rule is too frequent and will therefore be too costly, the Commission does not agree that vulnerability assessments will be costly. Indeed, there are resources for free and automated vulnerability assessments.[249] And although the Commission acknowledges that penetration testing can be a somewhat lengthy and costly process for large or complex systems,[250] a longer period between penetration tests will leave information systems vulnerable to attacks that exploit weaknesses normally revealed by penetration testing.

There are two other portions of the Final Rule that should help financial institutions concerned about the costs of monitoring and testing. First, because the Commission is limiting the definition of "information system" in the Final Rule, financial institutions will be able to limit this provision's application by segmenting their network

---

[248] The Commission believes that a system for continuous monitoring will include some form of vulnerability assessment as part of monitoring the information system.
[249] Remarks of Frederick Lee, Safeguards Workshop Tr., *supra* note 17, at 139-40.
[250] *See id.* at 129-30 (noting that the cost of a penetration test can increase significantly depending on the complexity of the system to be tested and the scope of the test).

and conducting monitoring or testing only of systems that contain customer information or that are connected to such systems. Second, this requirement does not apply to those institutions that maintain records on fewer than 5,000 individuals. Accordingly, for example, it should not apply to businesses small enough for staff to personally know a majority of customers.

Finally, the Commission does not believe the testing requirements are duplicative of other provisions of the Final Rule. The provision relating to additional risk assessments, 314.4(b)(2), requires a financial institution to reevaluate its risks and to determine if safeguards should be modified or added – it does not require testing to detect threats and technical vulnerabilities in the existing system. Paragraph 313.4(c)(8)'s requirement that financial institutions monitor users' activity in an information system is focused on one aspect of information security – detecting and preventing unauthorized access and use of the system. The requirement of this paragraph, on the other hand, is focused on testing the overall effectiveness of a financial institution's safeguards. It is broader than (c)(8)'s requirement and is necessary to ensure that financial institutions test the strength of their safeguards as a whole.

Accordingly, the Final Rule requires financial institutions to perform 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.

Proposed paragraph (e)

Proposed paragraph (e) set forth a requirement that financial institutions implement policies and procedures "to ensure that personnel are able to enact [the financial institution's] information security program." This requirement included four components: (1) general employee training; (2) use of qualified information security personnel; (3) specific training for information security personnel; and (4) verification that security personnel are taking steps to maintain current knowledge on security issues.

General Employee Training

Proposed paragraph (e)(1) required financial institutions to provide their personnel with "security awareness training that is updated to reflect risks identified by the risk assessment."[251]

While one commenter specifically supported the inclusion of this training requirement,[252] the U.S. Chamber of Commerce argued that the Rule should not have any specific training requirements at all.[253] NADA stated that the requirement that the training be "updated to reflect risks identified by the risk assessment" will require companies to develop individualized training programs to suit their financial institution and that such a process would be expensive and unnecessary because "general security awareness" is generally enough for most financial institutions.[254]

Given that the current Rule includes a similar training requirement and training remains a vital part of effective information security, the Commission declines to eliminate it. The Commission believes that the Final Rule's training requirement retains

[251] Proposed 16 CFR 314.4(e)(1).
[252] Electronic Privacy Information Center (comment 55, NPRM), at 8.
[253] U.S. Chamber of Commerce (comment 33, NPRM), at 12; *see also* American Financial Services Association (comment 41, NPRM), at 6 (stating that the Commission should acknowledge that a training program for a small financial institution will be different than a program for a larger program).
[254] National Automobile Dealers Association (comment 46, NPRM), at 34.

the same flexibility as the existing Rule and allows financial institutions to adopt a training program that is appropriate to their organization.

The Commission disagrees with NADA's concern that the requirement to update training programs would be too expensive. Without a requirement that the training program be updated based on an assessment of risks, employees may be subject to the same training year after year, which might reflect obsolete threats, as opposed to addressing current ones. The Commission interprets this provision to require only that the training program be updated as necessary based on changes in the financial institution's risk assessment. The provision also gives financial institutions the flexibility to use programs provided by a third party, if that program is appropriate for the financial institution. 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."

Information Security Personnel

Proposed paragraph (e)(2) required financial institutions to "[u]tiliz[e] qualified information security personnel," employed either by them or by affiliates or service providers, "sufficient to manage [their] information security risks and to perform or oversee the information security program."[255] This proposed provision was designed to ensure that information security personnel used by financial institutions are qualified for their positions and information security programs are sufficiently staffed.

[255] Proposed 16 CFR 314.4(e)(2).

Some commenters argued that this provision was too vague because it does not define what personnel are necessary and what "qualified" means.[256] NADA argued that hiring additional staff to meet this requirement could be prohibitively expensive.[257]

As discussed in relation to the appointment of a "Qualified Individual," the Commission believes that a more specific definition of "qualified" would not be appropriate because each financial institution has different needs and different levels of training, experience, and expertise will be appropriate for the information security staff of each institution. The term "qualified" conveys only that staff must have the abilities and expertise to perform the duties required by the information security program.[258] The Commission declines to include a more prescriptive set of qualification requirements in the Final Rule.[259]

As to the concern about expense, the Commission acknowledges that hiring employees or retaining third parties to maintain financial institutions' information security programs can be a substantial expense. But the expense is necessary to effectuate Congressional intent that financial institutions implement reasonable safeguards to protect customer information. The Rule requires only that financial institution have personnel "sufficient" to manage its risk and to maintain its information security program. A financial institution is required only to have the staff that is

---

[256] National Automobile Dealers Association (comment 46, NPRM), at 35; National Independent Automobile Dealers Association (comment 48, NPRM), at 7.
[257] National Automobile Dealers Association (comment 46, NPRM), at 35.
[258] NADA also asks whether this provision would require financial institutions to hire more personnel if they do not have enough qualified staff. *Id.* The Final Rule does require the hiring of additional personnel if existing personnel are not enough to maintain the financial institution's information security program.
[259] One commenter, on the other hand, approved of the decision not to define "qualified" in the Proposed Rule, but argued that the requirement in its totality was unclear because it did not set forth "how the Commission would hold covered entities accountable." American Council on Education (comment 24, NPRM) at 14. The Commission believes that the term "qualified" provides a clear enough requirement to allow a financial institution's compliance to be evaluated.

necessary to maintain its information security. An information security program that is not properly maintained cannot offer the protection it is designed to provide. A financial institution that does not comply with this requirement, by definition, has insufficient staffing, and thus, cannot reasonably protect customer information.

Although the expense is necessary, the level of expense is mitigated by several factors. First, existing financial institutions should already have information security personnel (either in the form of employees or third-party service providers) that are qualified to perform the duties necessary to maintain reasonable security in order to comply with the requirements of the current Rule. Depending on the skills of those employees, additional staffing may not be necessary to meet the demands of the Final Rule. Second, the required staffing will vary greatly based on the size and complexity of the information system. A financial institution with an extremely simple system may not require even a single full time employee. Finally, the Rule allows the use of service providers to meet this requirement. This can significantly reduce costs as services exist to share the expense of qualified personnel and offer information security support at significantly less than the cost of employing a single qualified employee.[260] The Commission continues to believe that utilizing qualified and sufficient information security personnel is a vital part of any information security program and accordingly, adopts proposed paragraph (e)(2) in the Final Rule without modification.

---

[260] *See e.g.*, Slides Accompanying Remarks of Rocio Baeza, "Models for Complying to the Safeguards Rule Changes," in Safeguards Workshop Slides, *supra* note 72, at 27-28 (describing three different compliance models: in-house, outsource, and hybrid, with costs ranging from $199 per month to more than $15,000 per month)*; see also* remarks of Rocio Baeza, Safeguards Workshop Tr., *supra* note 17, at 81-83; slides Accompanying Remarks of Brian McManamon, "Sample Pricing," in Safeguards Workshop Slides, *supra* note 72, at 29 (estimating the cost of cybersecurity services based on number of endpoints); Remarks of Brian McManamon, Safeguards Workshop Tr., *supra* note 17, at 83-85.

Training of Security Personnel

The Proposed Rule also required financial institutions to "[p]rovid[e] information security personnel with security updates and training sufficient to address relevant security risks."[261] This is separate from paragraph (e)(1)'s requirement to train all personnel generally.

Some commenters argued that providing ongoing training could be too costly for some financial institutions.[262] The Commission disagrees. Maintaining awareness of emerging threats and vulnerabilities is a critical aspect of information security. In order to perform their duties, security personnel must be educated on the changing nature of threats to the information systems that they maintain. There are resources that will allow smaller institutions to meet this requirement at little or no cost, such as published security updates, online courses, and educational publications.[263] For financial institutions that utilize service providers to meet information security needs, the service provider is likely to include assurances that provided personnel will be trained in current security practices. The Commission views the use of such a service provider as meeting this requirement, as the financial institution is "providing" the service as part of the price it pays to the service provider. Thus, the Final Rule adopts paragraph (e)(3) as proposed.[264]

Verification of current knowledge

Proposed paragraph (e)(4) required financial institutions to "[v]erify[ ] that key information security personnel take steps to maintain current knowledge of changing

---

[261] Proposed 16 CFR 314.4(e)(3).
[262] National Automobile Dealers Association (comment 46, NPRM), at 35.
[263] *See e.g.*, Federal Trade Commission, *Cybersecurity for Small Business*, https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity (last accessed 1 Dec. 2020); Remarks of Kiersten Todt, Safeguards Workshop Tr. at 86-88 (describing the resources of the Cyber Readiness Institute).
[264] The Clearing House suggested that the Rule should require background checks on employees. The Clearing House (Comment 49, NPRM) at 19.

information security threats and countermeasures."[265] This requirement was intended to complement the proposed requirement regarding ongoing training of data security personnel, by requiring verification that such training has taken place.

NADA argued that this requirement should not apply to smaller financial institutions, stating that that the examples set forth in the Proposed Rule would be difficult for some smaller financial institutions to perform.[266] The examples provided with the Proposed Rule were that a financial institution could: 1) offer incentives or funds for key personnel to undertake continuing education that addresses recent developments, 2) include a requirement to stay abreast of security research as part of their performance metrics, or 3) conduct an annual assessment of key personnel's knowledge of threats related to their information system. The Commission believes smaller financial institutions can take advantage of any of these methods, particularly "requiring key personnel to undertake continuing education" as part of that personnel's duties. If they outsource responsibility for data security to service providers, they can simply include these requirements in their contracts.

The Commission believes that the rapidly changing nature of information security mandates this requirement, in order that information security leadership can properly supervise the information security program. Accordingly, the Final Rule adopts proposed paragraph (e)(4) without change.

Proposed paragraph (f)

Proposed paragraphs (f)(1) and (2) retained the current Rule's requirement, found in existing paragraphs (d)(1) and (2), to oversee service providers, and added a paragraph

[265] Proposed 16 CFR 314.4(e)(4).
[266] National Automobile Dealers Association (comment 46, NPRM), at 35-36.

(f)(3), requiring that financial institutions also periodically assess service providers "based on the risk they present and the continued adequacy of their safeguards."[267] The current Rule expressly requires an assessment of service providers' safeguards only at the onboarding stage; proposed paragraph (f)(3) required financial institutions to monitor their service providers on an ongoing basis to ensure that they are maintaining adequate safeguards to protect customer information that they possess or access.[268]

Several commenters argued that it would be costly and difficult for some financial institutions to periodically assess their service providers.[269] These commenters were particularly concerned with smaller financial institutions' ability to "monitor" larger service providers.[270] The Internet Association commented that the requirement to periodically assess service providers would be too onerous for the service providers themselves, arguing that the requirement would place "service providers under constant surveillance by their financial institution clients."[271] HITRUST suggested that the Rule should state that the periodic assessment requirement may be satisfied by requiring service providers to obtain and maintain information security certifications provided by third parties and based on proper information security frameworks.[272] In contrast, Consumer Reports took issue with the Rule requiring only "assessment" of service providers, and argued that financial institutions should be required to monitor their

---

[267] Proposed 16 CFR 314.4(g).
[268] The Clearing House wrote in support of this element of the Proposed Rule, noting that it would bring the Safeguards Rule's provisions relating to service provider oversight into better alignment with security guidelines for banks. The Clearing House (comment 49, NPRM), at 14.
[269] National Automobile Dealers Association (comment 46, NPRM), at 37; National Independent Automobile Dealers Association (comment 48, NPRM), at 7; *see also* Wangyang Shen (comment 3, Privacy Rule) (noting difficulty of supervising cloud services).
[270] National Automobile Dealers Association (comment 46, NPRM), at 22; National Association of Dealer Counsel (comment 44, NPRM), at 3.
[271] Internet Association (comment 9, Workshop), at 3-4.
[272] HITRUST (comment 18, NPRM), at 3-4.

service providers for compliance.[273] Yet other commenters expressed confusion over the term "service provider," asking whether it would cover national consumer reporting agencies that smaller financial institutions would be hard-pressed to assess.[274]

The Commission retains the service provider oversight requirement from proposed paragraph (f) without modification. Some high profile breaches have been caused by service providers' security failures,[275] and the Commission views the regular assessment of the security risks of service providers as an important part of maintaining the strength of a financial institution's safeguards.

The Commission disagrees with the commenters who expressed concerns that this provision, and particularly the assessment requirement, would impose undue costs on financial institutions. The Rule would require financial institutions only to assess the risks that service providers present and evaluate whether they continue to provide the safeguards required by contract, which need not include extensive investigation of a service provider's systems. In the case of large service providers, this oversight may consist of reviewing public reports of insecure practices, changes in the services provided, or security failures in the services provided. In other circumstances, such as where a large company hires a vendor to secure sensitive customer information, certifications, reports, or even third-party audits may be appropriate. The exact steps required depend both on the size and complexity of the financial institution and the nature

[273] Consumer Reports (comment 52, NPRM) at 7.
[274] American Financial Services Association (comment 41, NPRM), at 7.
[275] For example, in 2013, attackers were reportedly able to use stolen credentials obtained from a third-party service provider to access a customer service database maintained by national retailer Target Corporation, resulting in the theft of information relating to 41 million customer payment card accounts. Kevin McCoy, *Target to pay $18.5M for 2013 data breach that affected 41 million consumers*, USA TODAY, May 23, 2017, https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/.

of the services provided by the service provider. For this reason, the Commission declines to adopt the suggestion to allow a financial institution to accept an information security certification from the service provider to satisfy the service provider oversight requirement. The fact that a company maintains an information security certification may be a significant part of assessing the adequacy of a service provider's safeguards, but the Commission declines to prescribe a one-size-fits all approach, given the variation in size and complexity of financial institutions and their service providers.

To avoid imposing undue costs on financial institutions, the Commission declines to require ongoing monitoring, rather than periodic assessment, as recommended by Consumer Reports. The Commission believes that periodic assessment strikes the right balance between protecting consumers and imposing undue costs on financial institutions. The Commission acknowledges that financial institutions may have limited bargaining power in obtaining services from large service providers and limited ability to demand access to a service provider's systems. In those cases, any sort of hands-on assessment of the provider's systems may not be possible.

As to the concern that the assessment requirement will impose undue burdens on the service providers themselves, the Commission does not believe this concern justifies a modification to the proposed requirement. First, the Rule does not require "constant surveillance" by financial institutions – they are required only to "periodically assess" the risks presented by service providers. Second, as discussed above, the supervision of service providers is a vitally important aspect of information security, and while there may be some burdens on the service providers associated with being supervised, these are necessary burdens. A financial institution must be sure that a service provider is

protecting the information of its customers and any expenses that this involves are a necessary part of fulfilling this duty.

Finally, as to concerns about potential ambiguities in the definition of service provider, the amendments preserve the definition that exists in the current Rule. Thus, entities subject to this requirement under the Final Rule will remain the same as under the existing Rule and may include consumer reporting agencies. As discussed above, even larger service providers such as national CRAs can be subjected to some form of review by financial institutions.[276]

The Commission adopts proposed paragraph (f) in the Final Rule without modification.

Proposed paragraph (g)

Paragraph (g) of the Proposed Rule retained the language of existing paragraph (e) in the current Rule, which requires financial institutions to evaluate and adjust their information security programs in light of the result of testing required by this section, material changes to their operations or business arrangements, or any other circumstances that they know or have reason to know may have a material impact on their information security program. The Commission received no comments on this paragraph and adopts the language of the Proposed Rule.

Proposed paragraph (h)

Proposed paragraph (h) required financial institutions to establish written incident response plans that addressed (1) the goals of the plan; (2) the internal processes for

[276] The National Pawnbrokers Association expressed a concern that they cannot control vendors of local law enforcement agencies to whom they are required to provide customer information. National Pawnbrokers Association (comment 32, NPRM), at 2. However, the Rule does not require that financial institutions oversee service providers employed by other entities over which they have no control.

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.

Several commenters supported the proposal to require an incident response plan.[277] The Credit Union National Association observed that an incident response plan "helps ensure that an entity is prepared in case of an incident by planning how it will respond and what is required for the response."[278] Consumer Reports noted that a rapid response to a security event can limit damage caused by the event.[279] The Princeton Center commented that "a written incident response plan is an essential component of a good security system."[280] HITRUST commented that incident response plans can help organizations "to better allocate limited resources."[281] The South Carolina Department of Consumer Affairs suggested that the provision go further by requiring that the incident response plan include a process for notifying senior information security personnel of the event.[282]

---

[277] Consumer Reports (comment 52, NPRM), at 6; Princeton University Center for Information Technology Policy (comment 54, NPRM), at 7; Electronic Privacy Information Center (comment 55, NPRM), at 8; Credit Union National Association (comment 30, NPRM), at 2; Heartland Credit Union Association (comment 42, NPRM), at 2; National Association of Federally-Insured Credit Unions (comment 43, NPRM), at 1; HITRUST (comment 18, NPRM), at 2.
[278] Credit Union National Association (comment 30, NPRM), at 2.
[279] Consumer Reports (comment 52, NPRM), at 6.
[280] Princeton University Center for Information Technology Policy (comment 54, NPRM), at 7.
[281] HITRUST (comment 18, NPRM), at 2.
[282] South Carolina Department of Consumer Affairs (comment 47, NPRM), at 2.

Other commenters opposed requiring an incident response plan or objected to particular aspects of the requirement. Some commenters suggested that requiring financial institutions to have incident response plans is outside the Commission's authority under the GLB Act.[283] NADA argued that the requirement for an incident response plan was overbroad in light of the broad definition of security event,[284] and that the requirement was vague as to what the plan should include.[285]

Other commenters argued that the requirement was too burdensome. ACE argued that "the range of security events that might occur and their potential impacts on institutional capacity to recover" make establishing an incident response plan that will allow an institution to "respond to, and recover from, *any* security event materially affecting… customer information" impossible.[286] The Mortgage Bankers Association ("MBA") suggested that "institutions of smaller sizes may not necessarily be capable of addressing all seven of the proposed goals."[287] Further, the MBA argued that an incident response plan requirement had "the potential to cripple small businesses under the pressure of repeatedly checking the boxes for potentially harmless events."[288]

Finally, some commenters raised questions about what it means for customer information to be in a financial institution's "possession" for purposes of the incident response plan requirement. ACE argued that the requirement does not adequately account for customer information held in cloud storage operated by third parties,

---

[283] National Automobile Dealer Association (comment 46, NPRM), at 38; National Independent Automobile Dealers Association (comment 48, NPRM), at 7.
[284] National Automobile Dealer Association (comment 46, NPRM), at 38.
[285] National Automobile Dealer Association (comment 46, NPRM), at 12, 38-39. NPA also asked for greater detail on what constitutes an "incident." National Pawnbroker Association (comment 32, NPRM), at 4.
[286] American Council on Education (comment 24, NPRM), at 15.
[287] Mortgage Bankers Association (comment 26, NPRM), at 4.
[288] Mortgage Bankers Association (comment 26, NPRM), at 4.

asserting that such information is not technically within the financial institution's possession.[289] ACE suggested that the provision should apply to customer information for which the financial institution is responsible, instead.[290] Relatedly, the NPA expressed concern that pawnbrokers might be subject to liability under the Proposed Rule when law enforcement agencies or their third-party vendors make public disclosures of customer information that pawnbrokers are obligated to report.[291]

The Commission retains the requirement for financial institution to develop and implement an incident response plan, with one modification described below. The Commission believes that the creation of an incident response plan is directly related to safeguarding customer information and is within its authority under the GLBA. The requirement to create an incident response plan focuses on preparing financial institutions to respond promptly and appropriately to security events, and mitigating any weaknesses in their information systems in the process. By responding quickly and promptly mitigating weaknesses, financial institutions can stop ongoing or future compromise of customer information.[292] A well-organized response to a security event can limit the number of consumers affected by an outside attacker by promptly identifying the attack and taking steps to stop the attack.

The Commission disagrees with the commenters who stated this requirement was too burdensome. The Final Rule requires that incident response plans address "security event[s] materially affecting the confidentiality, integrity, or availability of customer

[289] American Council on Education (comment 24, NPRM), at 15.
[290] *Id.*
[291] National Pawnbroker Association (comment 32, NPRM), at 4.
[292] *See* Remarks of Serge Jorgenson, Safeguards Workshop Tr., *supra* note 17, at 52 (observing that a prompt response to an incident can prevent a "threat actor running around in my environment for days, months, years, and able to access anything they want.").

information in [a financial institution's] control." Significantly, the plan must address events that "materially" affect customer information. Thus, the required incident response plan does not require a plan to address every security event that may occur. The plan need not include minute details or all possible scenarios. Instead, the Rule requires the plan to establish a system—for example, by laying out clear lines of responsibility, systems for information sharing, and methods for evaluating possible solutions—that will facilitate a financial institution's response to security events regardless of the nature of the event. A detailed approach may be appropriate for some financial institutions, such as those with especially complicated systems or personnel hierarchies, but the Rule is designed to give financial institutions the flexibility needed to develop plans that best suit their needs.[293]

Moreover, the Commission believes the requirement is clear as to what an incident response plan should include. The seven listed requirements for the incident response plans provide sufficient guidance to financial institutions designing incident response plans while giving them flexibility to design a plan suited to their organization. In addition, there are many resources for designing incident response plans available for financial institutions, as well as service providers that can assist with the design process.[294] Individual institutions can determine the exact details of the plans.

---

[293] Although the Commission agrees with the South Carolina Department of Consumer Affairs that notification of senior personnel is valuable, the requirement that the plan address "the definition of clear roles, responsibilities and levels of decision-making authority" will almost always result in communication of decision-making to senior personnel authorized to make decisions about the security response. Coupled with the requirement that the Qualified Individual report to the board or equivalent body on material events affecting security, the Commission does not see the need to make this change.

[294] *See, e.g.*, FTC, DATA BREACH RESPONSE: A GUIDE FOR BUSINESS (2019), www.ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business; NIST, GUIDE FOR CYBERSECURITY EVENT RECOVERY (2016), nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf; Orion Cassetto, *Incident Response Plan 101: How to Build One, Templates and Examples*, EXABEAM:

To address questions about whether information is in the financial institution's "possession," the Commission is revising paragraph (h) of the Final Rule to require that financial institutions develop incident response plans "designed to promptly respond to, and recover from, any security event materially affecting… customer information in your *control*." (emphasis added) Replacing the term "possession" with "control" resolves the questions raised by ACE and the NPA regarding whether financial institutions must plan for security events affecting data that has been transferred to various kinds of third parties. Where a financial institution has voluntarily opted to store its customer information in the cloud, to whatever extent the information is no longer in the "possession" of the financial institution, it is certainly within the institution's "control." By contrast, customer information that has been obtained by a third party such as a law enforcement agency, over whom a financial institution has no authority and of whose actions the financial institution has no knowledge, cannot fairly be said to be in the financial institution's control. Consequently, the financial institution need not account for possible disclosures of that information by the third party.[295]

Notification of Security Events to the Commission

The Commission also requested comment on whether the Rule should require financial institutions to report security events to the Commission. Several commenters

---

INFORMATION SECURITY BLOG (November 21, 2018), www.exabeam.com/incident-response/incident-response-plan/ (last visited December 2, 2020).

[295] NADA further argued that the incident response plan constitutes a de facto consumer notification requirement. National Automobile Dealer Association (comment 46, NPRM), at 39. Financial institutions have an independent obligation to perform notification as required by state law, whether or not they have an incident response plan in place. The fact that the Rule requires a plan that sets forth procedures for satisfying that requirement does not impose any independent notification requirement on the financial institution.

supported this requirement.[296] The Princeton University Center for Information Technology Policy noted that such a reporting requirement would "provide the Commission with valuable information about the scope of the problem and the effectiveness of security measures across different entities" and that it would "help the Commission coordinate responses to shared threats."[297] The National Association of Federally-Insured Credit Unions argued that requiring financial institutions to report security events to the Commission would provide an "appropriate incentive for covered financial companies to disclose information to consumers and relevant regulatory bodies."[298] NAFCU also suggested that notification requirements are important because they "ensure independent assessment of whether a security incident represents a threat to consumer privacy."[299]

Other commenters opposed the inclusion of a reporting requirement.[300] ACE argued that such a requirement "would simply add another layer on top of an already crowded list of federal and state law enforcement contacts and state breach reporting requirements."[301] ACE also suggested that any notification requirement should be limited to a more restricted definition of "security event" than the definition in the

[296] Consumer Reports (comment 52, NPRM), at 6; Princeton University Center for Information Technology Policy (comment 54, NPRM), at 7; Credit Union National Association (comment 30, NPRM), at 2; Heartland Credit Union Association (comment 42, NPRM), at 2; National Association of Federally-Insured Credit Unions (comment 43, NPRM), at 1-2.
[297] Princeton University Center for Information Technology Policy (comment 54, NPRM), at 7.
[298] National Association of Federally-Insured Credit Unions (comment 43, NPRM), at 1.
[299] National Association of Federally-Insured Credit Unions (comment 43, NPRM), at 1-2.
[300] National Independent Automobile Dealers Association (comment 48, NPRM), at 7; American Council on Education (comment 24, NPRM), at 15.
[301] American Council on Education (comment 24, NPRM), at 15.

Proposed Rule, so that financial institutions would only be required to report incidents that could lead to consumer harm.[302]

The Commission agrees with commenters that stated that a requirement that financial institutions report security events to the Commission would have many benefits, including allowing the Commission to identify emerging threats and assisting the Commission's enforcement of the Rule. In addition, such a requirement would be unlikely to create a significant burden on financial institutions because a security event that leads to notification to the Commission is very likely to create breach notification obligations under various state laws, and the financial institution will thus already be engaged in notifying consumers and state regulators. The addition of a notification to the FTC would not require any significant additional preparation or effort. However, because the Notice of Proposed Rulemaking did not set forth a detailed proposal for a notification requirement, the Final Rule does not include such a requirement. Instead, the Commission is issuing a Notice of Supplemental Rulemaking that proposes adding a requirement that financial institutions notify the Commission of detected security events under certain circumstances.[303]

Proposed paragraph (i)

Proposed paragraph (i) required a financial institution's CISO to "report in writing, at least annually, to [the financial institution's] board of directors or equivalent governing body" regarding the following information: (1) the overall status of the information security program and financial institution's compliance with the Safeguards Rule; and (2) material matters related to the information security program, addressing

[302] *Id.*
[303] [Cite to FR]

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.[304] For financial institutions that did not have a board of directors or equivalent, the proposal required the CISO to make the report to a senior officer responsible for the financial institution's information security program.

One commenter supported this requirement.[305] Additionally, several workshop participants emphasized the value of communication between information security leaders and corporate boards or their equivalent. For example, workshop participant Michele Norin stated that it is "important" for the topic of information security to be discussed at the level of the board or senior leadership regularly, and at least once per year.[306] Participant Adrienne Allen agreed annual reporting made sense as a requirement, but noted that for some financial institutions, particularly those with an online presence, even more frequent communication could be beneficial.[307]

ACE argued that the Proposed Rule created too much emphasis on a single annual report and should instead focus on regular reporting to the Board or equivalent.[308] It also expressed concern that the report required by the Proposed Rule would be too detailed and would not allow the Board to see "the forest for the trees,"[309] that the requirements for the report were too prescriptive, and that the requirements focused too much on

---

[304] Proposed 16 CFR 314.4(i).
[305] Rocio Baeza (comment 12, Workshop), at 3-8 (supporting requirement and providing sample report form and compliance questionnaire); *see also* The Clearing House (comment 49, NPRM), at 15-16 (arguing that Rule should require more involvement from Board and senior management).
[306] Remarks of Michele Norin, Safeguards Workshop Tr., *supra* note 17, at 194.
[307] Remarks of Adrienne Allen, Safeguards Workshop Tr., *supra* note 17, at 199-200.
[308] American Council on Education (comment 24, NPRM), at 16.
[309] *Id.*

compliance rather than security.[310] Similarly, NADA argued that the report would not improve security but would instead create "unnecessary liability exposure for the board/leadership of the entity."[311] HITRUST suggested that Qualified Individuals should be able to meet this reporting requirement by submitting a report from an information security certification program to the Board or equivalent body.[312]

The Commission adopts the proposal as final, with one modification discussed below. This provision is intended to ensure that the governing body of the financial institution is engaged with and informed about the state of the financial institution's information security program. Likewise, this will create accountability for the Qualified Individual by requiring him or her to set forth the status of the information security program for the governing body.[313] This will help financial institutions to ensure that their information security programs are being maintained appropriately and given the necessary resources. Written reports will create a record of decisions made and the information upon which they were based, which may aid future decision-making.[314]

---

[310] *Id.*

[311] National Automobile Dealer Association (comment 46, NPRM), at 41. NADA also argued that the reports by third-party Qualified Individuals might not include useful information and were "more likely to be filled with platitudes and/or efforts to 'upsell' the dealership on additional CISO services." *Id.* at 42. NADA provided no support for this claim. The Commission notes that such a report would not meet the requirements of this provision, and the financial institution would be justified in terminating their relationship with that provider or, at least, demanding a revised report that did meet those requirements.

[312] HITRUST (comment 18, NPRM), at 4.

[313] *See* Remarks of Karthik Rangarajan, Safeguards Workshop Tr., *supra* note 17, at ("If quarter over quarter, year over year, this watermark isn't reducing, then board of directors should be able to challenge us and say maybe you're not mapping your risks correctly, or vice versa if it's reducing but we're seeing more incidents, we're seeing potential breaches, things like that, then the board of directors should be able to say maybe you don't have the right risk quantification framework or the right risk management framework.").

[314] Workshop participants Adrienne Allen, Karthik Rangarajan, and Michele Norin each emphasized this point. *See* Safeguards Workshop Tr., *supra* note 17, pp. 201-09.

Management involvement in information security programs can improve the strength of those programs and help to reduce breaches.[315]

The Commission disagrees with the commenters who stated that the reporting requirement would be too prescriptive. In fact, the language only requires reporting of (1) the overall status of the information security program and its compliance with this Rule; and (2) material matters related to the information security program. The language includes examples of what material matters might include, such as risk assessments and security events, but does not require that all of them be included. The financial institution and the Qualified Individual will be responsible for determining what is material for their organization. The Commission does not believe these requirements call for overly detailed reports.[316]

Although the Commission agrees that a certification report from a Qualified Individual could be a part of the annual report and may cover many material matters, it may not suffice in all cases; thus, the Commission declines to include such a one-size-fits-all requirement.

As to the suggestion to require "regular" reporting, the Commission agrees that more regular reporting may be the best approach for many financial institutions. To this

---

[315] *See* Juhee Kwon Jackie Rees Ulmer, & Tawei Wang, *The Association Between Top Management Involvement and Compensation and Information Security Breaches*, JOURNAL OF INFORMATION SYSTEMS, Spring 2013, at 219-236 ("…the involvement of an IT executive decreases the probability of information security breach reports by about 35 percent…"); Julia L. Higgs, Robert E. Pinsker, Thomas Joseph Smith, & George Young, *The Relationship Between Board-Level Technology Committees and Reported Security Breaches*, JOURNAL OF INFORMATION SYSTEMS, Fall 2016, at 79-98 ("[A]s a technology committee becomes more established, its firm is not as likely to be breached. To obtain further evidence on the perceived value of a technology committee, this study uses a returns analysis and finds that the presence of a technology committee mitigates the negative abnormal stock returns arising from external breaches.").

[316] Indeed, workshop participants discussed a variety of strategies for meaningful communication between security personnel and senior leadership. Participants noted that the proper content, style, and cadence of reporting (beyond the minimum annual report) will vary depending on, among other things, the type of financial institution in question and the level of familiarity of leadership with the relevant technical issues. *See* Safeguards Workshop Tr., *supra* note 17, at 194-200.

end, the Commission modifies the requirement in the final rule to say "regularly, and at least annually."[317] Beyond this modification, the Final Rule adopts proposed paragraph (i) as proposed.

Board Certification

The Commission specifically sought comment on whether the Board or equivalent should be required to certify the contents of the report. The two commenters that addressed this question stated that they should not.[318] ACE noted that "governing boards generally will not have the knowledge and expertise to independently certify" the technical aspects of the report and certification might require the employment of outside auditors.[319] The Commission agrees that senior management of financial institutions will often lack the technical expertise to personally attest to its validity. In addition, the primary purpose of the required report is to encourage communication between information security personnel and senior management, not to show compliance with the Rule. Requiring the governing board to certify the contents of the report would likely transform the report into a compliance document and might reduce its efficacy as a communication between the Qualified Individual and the Board. Accordingly, the Commission declines to adopt this requirement in the Final Rule.

---

[317] NADA argued that reports required by this provision would be expensive because the Proposed Rule stated that they would need to be prepared by a "CISO," which NADA takes to mean a highly compensated expert of the type retained by the most sophisticated large institutions. National Automobile Dealer Association (comment 46, NPRM), at 41. As discussed above, however, the Rule does not require all financial institutions to retain such an expert. Instead, the report will be made by the Qualified Individual, whose expertise and compensation will vary according to the size and complexity of a financial institution's information system.

[318] National Automobile Dealer Association (comment 46, NPRM), at 41 n.126; American Council on Education (comment 24, NPRM), at 16.

[319] American Council on Education (comment 24, NPRM), at 16.

Section 314.5: Effective date

The Proposed Rule set a new effective date for some portions of the Rule. Proposed section 314.5 provided that certain elements of the information security program would not be required until six months after the publication of a final Rule, rather than immediately upon publication. The paragraphs that would have a delayed effective date were: 314.4(a), related to the appointment of a Qualified Individual; 314.4(b)(1), relating to conducting a written risk assessment; 314.4(c)(1)-(8), setting forth the new elements of the information security program; 314.4(d)(2), requiring continuous monitoring or annual penetration testing and biannual vulnerability assessment; 314.4(e), requiring training for personnel; 314.4(f)(3), requiring periodic assessment of service providers; 314.4(h), requiring a written incident response plan; and 314.4(i), requiring annual written reports from the Qualified Individual. All other requirements under the Safeguards Rule would remain in effect during this six-month period. These remaining requirements largely mirrored the requirements of the existing Rule.

All commenters that addressed this provision noted the difficulty of complying with some of the provisions of the Proposed Rule, and argued that financial institutions should be given more time to comply with them. ACE suggested that financial institutions be given one year to create a plan for compliance and two years to come into actual compliance.[320] AFSA suggested that compliance not be required for two years.[321] ACA International requested that the effective date be one year after publication of the Rule.[322]

[320] American Council on Education (comment 24, NPRM), at 4-5.
[321] American Financial Services Association (comment 41, NPRM), at 7.
[322] ACA International (comment 45, NPRM), at 10-11.

The Commission agrees that some financial institutions may need longer to modify their information security programs to comply with the new requirements in the Final Rule, especially given the current pandemic and the strains that it is placing on businesses. Accordingly, the Final Rule extends the effective date for these enumerated provisions to one year after the publication of this notice.

Proposed section 314.6: Exceptions

Proposed section 314.6 exempted financial institutions that maintain customer information concerning fewer than five thousand consumers from certain requirements of the Proposed Rule, namely 314.4(b)(1), requiring a written risk assessment; 314.4(d)(2), requiring continuous monitoring or annual penetration testing and biannual vulnerability assessment; 314.4(h), requiring a written incident response plan; and 314.4(i), requiring an annual written report by the CISO (as revised, the Qualified Individual).[323] This proposed section was designed to reduce the burden on smaller financial institutions.

The Commission sought comment on whether it was appropriate to include such an exemption, whether the specific exemptions were appropriate, whether the use of the number of customers concerning whom the financial institution retains customer information is the most effective way to determine which financial institutions should be exempted and, if so, whether five thousand customers was an appropriate number. After reviewing the comments received, the Commission retains the exemption for financial institutions with fewer than 5,000 customers as proposed.

[323] Proposed 16 CFR 314.6.

Several commenters supported the inclusion of an exemption for small financial institutions. Consumer Reports supported the exemption as proposed.[324] NPA supported the decision to base this exemption on the number of customers whose information the financial institution maintains, but questioned how the number of customers would be determined.[325] NPA asked whether the number of customers would be counted on an annual basis or include all records the financial institution maintains. It also asked if each transaction with a customer would be counted separately.[326]

Some commenters argued that the number of customers whose records a financial institution maintains was the wrong measure by which to assess whether the exemption should apply. For example, commenters suggested that the Rule should take into account businesses with revenue beneath a certain threshold,[327] the number of students enrolled at covered educational institutions,[328] or the number of individuals employed by the financial institution.[329]

Additionally, some commenters argued that the threshold for application of the exemption should be higher. ACA International suggested that the exemption should apply to all financial institutions maintaining records concerning fewer than 10,000 customers.[330] AFSA suggested a 50,000 customer threshold.[331] NADA[332] and

---

[324] Consumer Reports (comment 52, NPRM), at 6; *see also* Credit Union National Association (comment 30, NPRM), at 2 (noting that the exemption will be helpful for smaller businesses, but suggesting other changes to the Proposed Rule so that the exemption is not required).
[325] National Pawnbrokers Association (comment 32, NPRM), at 6.
[326] *Id.; see also* National Independent Automobile Dealers Association (comment 48, NPRM), at 3.
[327] ACA International (comment 45, NPRM), at 11-12.
[328] American Council on Education (comment 24, NPRM), at 5.
[329] Ahmed Aly (comment 22, NPRM).
[330] ACA International (comment 45, NPRM), at 11-12.
[331] American Financial Services Association (comment 41, NPRM), at 3-4.
[332] National Automobile Dealers Association (comment 46, NPRM), at 43-44. NADA also suggested that information about customers for which the nonpublic information has been removed should not be counted to the total. If the information is anonymized or otherwise transformed so that it is no longer reasonably

NIADA[333] argued that the threshold should be raised to 100,000 customers. Without proposing a specific alternative, NPA expressed concern that the 5,000-customer threshold may be too low, noting that pawnbrokers who accept firearms as collateral are required to keep customer records related to certain transactions for twenty years.[334]

As to the substance of the exemption, some commenters felt that it did not go far enough to relieve the burden of the rule for small financial institutions. ACA International proposed that eligible financial institutions should also be exempt from the requirement to designate a single qualified individual to oversee their information security programs.[335] The National Federation of Independent Business argued that businesses with 15 or fewer employees should be exempted from the Rule entirely and instead held only to a requirement to take "commercially reasonable steps" to safeguard customer information.[336] The Small Business Administration Office of Advocacy suggested that, in the absence of additional information regarding the impact of the proposed changes on small businesses, the Rule should "maintain the status quo" for small entities as defined by the Small Business Administration's size standards.[337]

On the other hand, other commenters opposed the inclusion of any exemption. The Independent Community Bankers of America noted that the Federal Financial Institutions Examination Council Interagency Guidelines Establishing Standards for Safeguarding Customer Information ("FFIEC Guidelines"), which detail how depository

---

linkable to a customer, that information will not count towards the exemption. NADA's example of retaining only "name, phone number, address, and VIN of the vehicle they own," would still count as customer information under the Rule.

[333] National Independent Automobile Dealers Association (comment 48, NPRM), at 3.
[334] National Pawnbrokers Association (comment 32, NPRM), at 6.
[335] ACA International (comment 45, NPRM), at 12.
[336] National Federation of Independent Business (comment 16, NPRM), at 4.
[337] Small Business Administration Office of Advocacy (comment 28, NPRM), at 6.

institutions are required to protect customer information, include no exemption for smaller institutions and suggested that the Rule should also have no exemption and apply equally to all financial institutions.[338]

Under the existing Rule, there is no exception for smaller entities. Still, the Commission continues to believe that it is appropriate to exempt small businesses from some of the revised Rule's requirements. Although the FFIEC Guidelines do not exempt small businesses from its requirements, the FFIEC Guidelines regulate only depository financial institutions that are subject to an entirely different regulatory regime, including supervision by their regulatory agencies. While the provisions from which eligible financial institutions are exempt have significant benefits for the security of customer information and other sensitive data,[339] those provisions may be less necessary in situations where the overall volume of retained data is low. This is true in part because the potential for cumulative consumer harm is less where fewer consumers' information may be exposed as the result of a security incident.[340]

---

[338] Independent Community Bankers of America (comment 35, NPRM), at 4; *see also* American Escrow (comment 6, Workshop), at 3 (arguing that even small companies may need to comply with all portions of the Rule to maintain consumer confidence); *see also* Caiting Wang (Comment 6, Privacy) (suggesting that exempted provisions should be optional for smaller businesses or that the Commission create a fund to enable small businesses to comply with these provisions).

[339] *See, e.g.,* Remarks of Brian McManamon, Safeguards Workshop Tr., *supra* note 17, at 85 (noting that continuous monitoring allows organizations to detect and quickly respond to threats); Remarks of Frederick Lee, Safeguards Workshop Tr., *supra* note 17, at 126-28 (Frederick Lee) (discussing benefits of penetration testing); Remarks of Tom Dugas, Safeguards Workshop Tr., *supra* note 17, at 143 (noting the importance of vulnerability scans); Remarks of Michele Norin, Safeguards Workshop Tr., *supra* note 17, 194-95 (asserting that annual reporting by the Qualified Individual to an organization's board or equivalent is beneficial); Remarks of Adrienne Allen, Safeguards Workshop Tr., *supra* note 17, at 201.

[340] *See* Remarks of James Crifasi, Safeguards Workshop Tr., *supra* note 17, at 91-92 (noting that companies that control large amounts of consumer data should in most instances implement the full range of data security safeguards, whereas small businesses with less data may need to focus on cybersecurity basics); *see also* Remarks of Lee Waters, Safeguards Workshop Tr., *supra* note 17, at 91 ("[T]he amount of data [that a business holds] would definitely have an influence on whether a business is even going to be attacked."); Remarks of Rocio Baeza, Safeguards Workshop Tr., *supra* note 17, at 94 (citing the volume of consumer records held by an organization as an important factor in assessing cybersecurity risk).

For similar reasons, the Commission finds that the number of individuals concerning whom a financial institution maintains customer information is the appropriate measure of whether the exemption should apply to a particular financial institution. The application of the exemption should take into account both the potential burden of compliance to financial institutions and the risk to consumers when standards are relaxed—in other words, the purpose of the exemption is to avoid imposing *undue* burden while assuring that customer information is subject to necessary protections. Even a very small financial institution, depending on its business model, may retain very large quantities of sensitive customer information.[341] Adequate security is necessary to protect such information, which may constitute an attractive target for bad actors such as identity thieves; the value of the target is correlated with the volume of information maintained.[342] While a business's revenue or number of employees may provide a measure of the burden of compliance for that business, these figures do not capture consumer risk. By contrast, the number of individuals about whom a financial institution maintains customer information is a proxy for the level of security that is necessary in light of both the risk of attack and the potential consumer harm should a security incident

[341] *See e.g.*, Remarks of James Crifasi, Safeguards Workshop Tr., *supra* note 17, at 91-92 (noting that small businesses with an enormous amount of consumer records need to follow all of the safeguards and "can't get away with just doing the basics"); *see also* ACA International (comment 45, NPRM) at 11 ("Many small financial institutions, including a number of ACA members, have objectively limited operations in terms of number of employees and revenues, but handle large volumes of consumer account data for each of their clients on whose behalf they are collecting debts.").

[342] *See e.g.*, Remarks of Rocio Baeza, Safeguards Workshop Tr., *supra* note 17, at 94 (opining that "the better indicators for cybersecurity risk are going to be two things: the volume of consumer records that a financial institution holds and also the rate of change."); Remarks of Lee Waters, Safeguards Workshop Tr., *supra* note 17, at 91 (noting that the amount of data a company holds influences whether a business is going to be attacked or not).

occur.[343] In addition, basing the exemption on the number of individuals concerning whom a financial institution maintains customer information provides an incentive to financial institutions to reduce the amount of information they retain. A financial institution may choose to dispose of information so that it holds information on few enough consumers to qualify for exemption.[344]

The Final Rule adopts this section as proposed. The Commission continues to believe that the cutoff for financial institutions maintaining information concerning 5,000 consumers appropriately balances the need for security with the burdens on smaller businesses. The requirements to which exempted financial institutions would still be required to adhere are tailored to balance the importance of adequately securing customer information against the need to limit financial burdens for small businesses. Many of these requirements were already in force as part of the existing Rule—for example, covered financial institutions were already required to design and implement a written information security program, conduct risk assessments, perform an initial assessment of their service providers, and designate one or more employees to oversee information security. For reasons discussed elsewhere in this Notice, the new requirements that apply to exempted financial institutions, such as the requirement to designate a single qualified individual to oversee information security rather than one or more individuals, will ensure that financial institutions of all sizes continue to adequately protect customer

[343] *See* Remarks of Brian McManamon, Safeguards Workshop Tr., *supra* note 17, at 89-90 (noting that the size of a financial institution and the amount and nature of the information that it holds factor into an appropriate information security program).

[344] The Commission understands this provision to count all individual consumers about which a financial institution maintains customer information, including both current and former customers. The exemption counts consumers rather than transactions so that a financial institution that had 100 transactions with a single customer would count only a single consumer.

information in an environment of increasing cybersecurity risk, while avoiding the imposition of undue burden.

IV. Paperwork Reduction Act

The Paperwork Reduction Act ("PRA"), 44 U.S.C. chapter 35, requires federal agencies to seek and obtain OMB approval before undertaking a collection of information directed to ten or more persons.[345] A "collection of information" occurs when ten or more persons are asked to report, provide, disclose, or record information in response to "identical questions."[346] Applying these standards, neither the Safeguards Rule nor the amendments constitute a "collection of information."[347] The Rule calls upon affected financial institutions to develop or strengthen their information security programs in order to provide reasonable safeguards. Under the Rule, each financial institution's safeguards will vary according to its size and complexity, the nature and scope of its activities, and the sensitivity of the information involved. For example, a financial institution with numerous employees would develop and implement employee training and management procedures beyond those that would be appropriate or reasonable for a sole proprietorship, such as an individual tax preparer or mortgage broker. Similarly, a financial institution that shares customer information with numerous service providers would need to take steps to ensure that such information remains protected, while a financial institution with no service providers would not need to address this issue. Thus, although each financial institution must summarize its compliance efforts in one or more written documents, the discretionary balancing of factors and circumstances that the Rule

[345] 44 U.S.C. 3502(3)(A)(i).
[346] *See* 44 U.S.C. 3502(3)(A).
[347] *See* Standards for Safeguarding Customer Information, 67 FR 36484, 36491 (May 23, 2002).

allows—including the myriad operational differences among businesses that it contemplated—does not require entities to answer "identical questions" and therefore does not trigger the PRA's requirements.

The amendments to the Rule do not change this analysis because they retain the existing Rule's process-based approach, allowing financial institutions to tailor their programs to reflect the financial institutions' size, complexity, and operations, and to the sensitivity and amount of customer information they collect. For example, amended paragraph 314.4(b) would require a written risk assessment, but each risk assessment will reflect the particular structure and operation of the financial institution and, though each assessment must include certain criteria, these are only general guidelines and do not consist of "identical questions." Similarly, amended paragraph 314.4(h), which requires a written incident response plan, is only an extension of the preexisting requirement of a written information security plan and would necessarily vary significantly based on factors such as the financial institution's internal procedures, which officials within the financial institution have decision-making authority, how the financial institution communicates internally and externally, and the structure of the financial institution's information systems. Likewise, the proposed requirement for Qualified Individuals to produce annual reports under proposed paragraph 314.4(i) does not consist of answers to identical questions, as the content of these reports would vary considerably between financial institutions and Qualified Individuals are given flexibility in deciding what to include in the reports.

Finally, the modification of the definition of "financial institution" to include "activities incidental to financial activities" and therefore bring finders under the scope of

the Rule do not constitute a "collection of information," and therefore do not trigger the PRA's requirements.

V. Regulatory Flexibility Act

The Regulatory Flexibility Act (RFA), as amended by the Small Business Regulatory Enforcement Fairness Act of 1996, requires an agency to either provide an Initial Regulatory Flexibility Analysis with a proposed Rule, or certify that the proposed Rule will not have a significant impact on a substantial number of small entities.[348] The Commission published an Initial Regulatory Flexibility Analysis in order to inquire into the impact of the Proposed Rule on small entities. In response, the Commission received comments that argued that the revision to the Safeguards Rule would be unduly burdensome for smaller financial institutions. The discussion below summarizes these comments and the Commission's response to them.

1. Description of the Reason for Agency Action

The Commission issues these amendments to clarify the Safeguards Rule by including a definition of "financial institution" and related examples in the Safeguards Rule rather than incorporating them from the Privacy Rule by reference. The amendments also expand the definition of "financial institution" in the Rule to include entities that are engaged in activities that are incidental to financial activities. This change would bring "finders" within the scope of the Rule. This change harmonizes the Rule with other agencies' rules and requires finders that collect consumers' sensitive financial information to comply with the Safeguards Rule's process-based approach to protect that data.

[348] 5 U.S.C. 603 *et seq*.

In addition, the amendments modify the Safeguards Rule to include more detailed requirements for the information security program required by the Rule.

2. *Issues Raised by Comments in Response to the IRFA*

As stated above, the Commission received several comments that argued that the revised Safeguards Rule would impose unduly heavy burdens on smaller businesses. The Small Business Administration's Office of Advocacy commented that it was concerned the FTC had not gathered sufficient data as to either the costs or benefits of the proposed changes for small financial institutions. The FTC shares the Office of Advocacy's interest in ensuring that regulatory changes have an evidentiary basis. Many of the questions on which the FTC sought public comment, both in the regulatory review and in the proposed rule context, specifically related to the costs and benefits of existing and proposed Rule requirements. Following the initial round of commenting, the Commission conducted the FTC Safeguards Workshop and solicited additional public comments with the explicit goal of gathering additional data relating to the costs and benefits of the proposed changes.[349] As detailed throughout this Notice, the Commission believes that there is a strong evidentiary basis for the issuance of the Final Rule.

The Office of Advocacy also argued that the Proposed Rule's requirements were unduly prescriptive and should not be enacted as they apply to small businesses until the Commission can "ascertain the quantitative impact on small entities."[350] The Office of Advocacy, along with other commenters, argued that the amendments

[349] See Public Workshop Examining Information Security for Financial Institutions and Information Related to Changes to the Safeguards Rule, 85 Fed. Reg. 13,082 (Mar. 6, 2020).
[350] Small Business Administration Office of Advocacy (comment 28, NPRM), at 6.

taken together would create a large burden on smaller financial institutions. In particular, commenters pointed to the requirements that financial institutions appoint a chief information security officer, that customer information be encrypted, that financial institutions utilize multi-factor authentication, and that financial institutions regularly update training programs. These comments and the Commission's response are discussed at length above. Most commenters did not provide any specific estimates of these expenses, but two commenters did provide a summary of their expected expenses.

As discussed in the Notice, the Commission believes that any burden imposed by the revised Rule is substantially mitigated by the fact that the Rule continues to be process-based, flexible, and based on the financial institution's size and complexity. In addition, the amendments exempt institutions that maintain information on fewer than 5,000 consumers from certain requirements that require additional written product and might pose a greater burden on smaller entities. The Commission believes that most of the entities covered by the exemption will be small businesses. Finally, the Commission believes that all financial institutions, including small businesses, that comply with the current Safeguards Rule will already be in compliance with most of the new provisions of the revised Rule as part of their current information security program.

In addition, in response to the comments concerned about the burden of the amendments, the Commission extended the effective date from six months after the publication of the Final Rule to one year after the publication to allow financial institutions additional time to come into compliance with the revised Rule. In addition, in response to comments that argued that hiring a chief information security

officer would be prohibitively expensive for small financial institutions, the Commission amended the rule to clarify that such an employee was not required for all financial institutions. The Final Rule is modified to clarify that a financial institution need only appoint an individual who is qualified to coordinate its information security program, and that those qualifications will vary based on the complexity of the program and size and nature of the financial institution. The Commission also clarified that employee training programs need to be updated only as necessary, to respond to a comment that regular updating would be difficult for smaller financial institutions.

3. Estimate of Number of Small Entities to Which the Amendments Will Apply

As previously discussed in the IRFA, determining a precise estimate of the number of small entities[351]—including newly covered entities under the modified definition of financial institution—is not readily feasible. Financial institutions already covered by the Rule as originally promulgated include lenders, financial advisors, loan brokers and servicers, collection agencies, financial advisors, tax preparers, and real estate settlement services, to the extent that they have "customer information" within the

[351] The U.S. Small Business Administration Table of Small Business Size Standards Matched to North American Industry Classification System Codes ("NAICS") are generally expressed in either millions of dollars or number of employees. A size standard is the largest that a business can be and still qualify as a small business for Federal Government programs. For the most part, size standards are the annual receipts or the average employment of a firm. Depending on the nature of the financial services an institution provides, the size standard varies. By way of example, mortgage and nonmortgage loan brokers (NAICS code 522310) are classified as small if their annual receipts are $8.0 million or less. Consumer lending institutions (NAICS code 522291) are classified as small if their annual receipts are $41.5 million or less. Commercial banking and savings institutions (NAICS codes 522110 and 522120) are classified as small if their assets are $600 million or less. Assets are determined by averaging the assets reported on businesses' four quarterly financial statements for the preceding year. The 2019 Table of Small Business Size Standards is available at https://www.sba.gov/sites/default/files/2019-08/SBA%20Table%20of%20Size%20Standards_Effective%20Aug%2019%2C%202019_Rev.pdf.

meaning of the Rule. Finders are also covered under the Final Rule. However, it is not known whether any finders are small entities, and if so, how many there are. The Commission requested comment and information on the number of "finders" that would be covered by the Rule's modified definition of "financial institution," and how many of those finders, if any, are small entities. The Commission received no comments that addressed this question.

4. Projected Reporting, Recordkeeping, and Other Compliance Requirements.

The Rule does not impose any reporting or any specific recordkeeping requirements as discussed earlier. *See supra* Section IV (Paperwork Reduction Act).

With regard to other compliance requirements, the addition of definitions and examples from the Privacy Rule is not expected to have an impact on covered financial institutions, including those that may be small entities. (The preceding section of this analysis discusses classes of covered financial institutions that may qualify as small entities.) The addition of "finders" to the definition of financial institutions imposes the obligations of the Rule on entities that engage in "finding" activity and also collect customer information.

The addition of more detailed requirements may require some financial institutions to perform additional risk assessments or monitoring, or to create additional safeguards as set forth in the Proposed Rule. These obligations may require institutions to retain employees or third-party service providers with skills in information security, but, as discussed above, the Commission believes that most financial institutions will have already complied with many parts of the Rule as part of their information security programs required under the existing Rule. There may be additional related compliance

costs (e.g., legal, new equipment or systems, modifications to policies or procedures), but, as discussed above, the Commission believes that these are limited by several factors, including the flexibility of the Rule, the existing safeguards in place to comply with the existing Rule, and the exemption for financial institutions that maintain less consumer information.

Although two commenters provided summaries of the expected expenses for some financial institutions to comply with the Rule, those estimates did not provide sufficient detail to fully evaluate whether they were accurate or representative of other financial institutions and appeared to be based, at least in part, on a misunderstanding of the requirement to appoint a Qualified Individual. The Commission believes that, for most smaller financial institutions, there are very low-cost solutions for any additional duties imposed by the Final Rule. This view is supported by the comments of several experts at the Safeguards Rule Workshop.[352]

The Commission believes that the protection of consumers' financial information is of the utmost importance and that the cost of the safeguards required to provide that protection is justified and necessary. The Commission carefully balanced the cost of these requirements with the need to protect consumer information and has made every

[352] *See, e.g.*, Remarks of Brian McManamon, Safeguards Workshop Tr., *supra* note 17, at 78 (describing virtual CISO services); Matthew Green, Safeguards Workshop Tr., *supra* note 17, at 225 (noting website usage of encryption for data in motion is above 80 percent; "Let's Encrypt" provides free TLS certificates; and costs have gone down to the point that if a financial institution is not using TLS encryption for data in motion, it is making an unusual decision outside the norm); Rocio Baeza, Safeguards Workshop Tr., *supra* note 17, at 106 ("[T]he encryption of data in transit has been standard. There's no pushback with that."); Slides Accompanying the Remarks of Lee Waters, "Information Security Programs and Smaller Businesses," in Safeguards Workshop Slides, *supra* note 72, at 26 ("Estimated Costs of Proposed Changes," estimating costs of multi-factor authentication to be $50 for smartcard or fingerprint readers, and $10 each per smartcard); Slides Accompanying Remarks of Wendy Nather, Safeguards Workshop Slides, *supra* note 72, at 37 (chart showing the use of multi-factor authentication solutions such as Duo Push, phone call, mobile passcode, SMS passcode, hardware token, Yubikey passcode, and U2F token in industries such as financial services and higher education).

effort to ensure the Final Rule retains flexibility so that financial institutions can tailor information security programs to the size and complexity of the financial institution, the nature and scope of its activities, and the sensitivity of any customer information at issue.

5. Description of Steps Taken To Minimize Significant Economic Impact, If Any, on Small Entities, Including Alternatives

The standards in the Final Rule allow a small financial institution to develop an information security program that is appropriate to its size and complexity, the nature and scope of its activities, and the sensitivity of any customer information at issue. The amendments include certain design standards (e.g., a company must implement encryption, authentication, and incident response) in the Rule, in addition to the performance standards (reasonable security) that the Rule currently uses. As discussed, while these design standards may introduce some additional burden, the Commission believes that many financial institutions' existing information security programs already meet most of these requirements. In addition, the requirements in the Final Rule, like those in the existing Rule, are designed to allow financial institutions flexibility in how and whether they should be implemented. For example, the requirement that encryption be used to protect customer information in transit and at rest may be met with effective alternative compensating controls if encryption is infeasible for a given financial institution.

In addition, the amendments exempt financial institutions that maintain relatively small amounts of customer information from certain requirements of the Final Rule. The exemptions would apply to financial institutions that maintain customer information concerning fewer than ten thousand consumers. The Commission believes that exempted

financial institutions are generally, but not exclusively, small entities. Such financial institutions are not required to perform a written risk assessment, conduct continuous monitoring or annual penetration testing and biannual vulnerability assessment, prepare a written incident response plan, or prepare an annual written report by the Qualified Individual. These exemptions are intended to reduce the burden on smaller financial institutions. The Commission believes that the obligations subject to these exemptions are the ones that are most likely to cause undue burden on smaller financial institutions.

Exempted financial institutions will still need to conduct risk assessments, design and implement a written information security program with the required elements, utilize qualified information security personnel and train employees, monitor activity of authorized users, oversee service providers, and evaluate and adjust their information security program. These are core obligations under the Rule that any financial institution that collects customer information must meet, regardless of size.

The Commission considered allowing compliance with a third-party data security standard, such as the NIST framework, to act as a safe harbor for compliance with the Rule. The Commission, however, determined that any reduction of burden created by allowing such safe harbors is offset by issues they would cause. For example, such safe harbors would require the Commission to monitor the third-party standard or standards to determine whether they continued to align with the Safeguards Rule. In addition, the Commission would still have to investigate a company's compliance with the outside standard in any enforcement action. The Commission also does not agree that compliance with an outside standard is likely to be less burdensome than complying with the Safeguards Rule itself.

VI. Other Matters

Pursuant to the Congressional Review Act (5 U.S.C. § 801 et seq.), the Office of Information and Regulatory Affairs designated this rule as not a "major rule," as defined by 5 U.S.C. § 804(2).

List of Subjects in 16 CFR Part 314

Consumer protection, Credit, Data protection, Privacy, Trade practices.

For the reasons stated above, the Federal Trade Commission amends 16 CFR Part 314 as follows:

PART 314—STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

1. The authority citation for Part 314 continues to read as follows:

Authority: 15 U.S.C. §§ 6801(b), 6805(b)(2).

2. Revise § 314.1(b) to read as follows:

§ 314.1 Purpose and scope.

* * * * *

(b) *Scope*. This part applies to the handling of customer information by all financial institutions over which the Federal Trade Commission ("FTC" or "Commission") has jurisdiction. Namely, this part applies to those "financial institutions" over which the Commission has rulemaking authority pursuant to section 501(b) of the Gramm-Leach-Bliley Act. An entity is a "financial institution" if its business is engaging in an activity that is financial in nature or incidental to such financial activities as described in section 4(k) of the Bank Holding Company Act of 1956, 12 U.S.C. 1843(k), which incorporates

by reference activities enumerated by the Federal Reserve Board in 12 CFR 225.28 and 12 CFR 225.86. The "financial institutions" subject to the Commission's enforcement authority are those that are not otherwise subject to the enforcement authority of another regulator under section 505 of the Gramm-Leach-Bliley Act, 15 U.S.C. 6805. More specifically, those entities include, but are not limited to, mortgage lenders, "pay day" lenders, finance companies, mortgage brokers, account servicers, check cashers, wire transferors, travel agencies operated in connection with financial services, collection agencies, credit counselors and other financial advisors, tax preparation firms, non-federally insured credit unions, investment advisors that are not required to register with the Securities and Exchange Commission, and entities acting as finders. They are referred to in this part as "You." This part applies to all customer information in your possession, regardless of whether such information pertains to individuals with whom you have a customer relationship, or pertains to the customers of other financial institutions that have provided such information to you.

3. Revise § 314.2 to read as follows:

§ 314.2 Definitions.

(a) *Authorized user* means any employee, contractor, agent, customer, or other person that is authorized to access any of your information systems or data.

(b)(1) *Consumer* means an individual who obtains or has obtained a financial product or service from you that is to be used primarily for personal, family, or household purposes, or that individual's legal representative.

(2) *Examples –*

(i) An individual who applies to you for credit for personal, family, or household purposes is a consumer of a financial service, regardless of whether the credit is extended.

(ii) An individual who provides nonpublic personal information to you in order to obtain a determination about whether he or she may qualify for a loan to be used primarily for personal, family, or household purposes is a consumer of a financial service, regardless of whether the loan is extended.

(iii) An individual who provides nonpublic personal information to you in connection with obtaining or seeking to obtain financial, investment, or economic advisory services is a consumer, regardless of whether you establish a continuing advisory relationship.

(iv) If you hold ownership or servicing rights to an individual's loan that is used primarily for personal, family, or household purposes, the individual is your consumer, even if you hold those rights in conjunction with one or more other institutions. (The individual is also a consumer with respect to the other financial institutions involved.) An individual who has a loan in which you have ownership or servicing rights is your consumer, even if you, or another institution with those rights, hire an agent to collect on the loan.

(v) An individual who is a consumer of another financial institution is not your consumer solely because you act as agent for, or provide processing or other services to, that financial institution.

(vi) An individual is not your consumer solely because he or she has designated you as trustee for a trust.

(vii) An individual is not your consumer solely because he or she is a beneficiary of a trust for which you are a trustee.

(viii) An individual is not your consumer solely because he or she is a participant or a beneficiary of an employee benefit plan that you sponsor or for which you act as a trustee or fiduciary.

(c) *Customer* means a consumer who has a customer relationship with you.

(d) *Customer information* means any record containing nonpublic personal information about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates.

(e)(1) *Customer relationship* means a continuing relationship between a consumer and you under which you provide one or more financial products or services to the consumer that are to be used primarily for personal, family, or household purposes.

(2) *Examples –*

(i) *Continuing Relationship.* A consumer has a continuing relationship with you if the consumer:

(A) Has a credit or investment account with you;

(B) Obtains a loan from you;

(C) Purchases an insurance product from you;

(D) Holds an investment product through you, such as when you act as a custodian for securities or for assets in an Individual Retirement Arrangement;

(E) Enters into an agreement or understanding with you whereby you undertake to arrange or broker a home mortgage loan, or credit to purchase a vehicle, for the consumer;

(F) Enters into a lease of personal property on a non-operating basis with you;

(G) Obtains financial, investment, or economic advisory services from you for a fee;

(H) Becomes your client for the purpose of obtaining tax preparation or credit counseling services from you;

(I) Obtains career counseling while seeking employment with a financial institution or the finance, accounting, or audit department of any company (or while employed by such a financial institution or department of any company);

(J) Is obligated on an account that you purchase from another financial institution, regardless of whether the account is in default when purchased, unless you do not locate the consumer or attempt to collect any amount from the consumer on the account;

(K) Obtains real estate settlement services from you; or

(L) Has a loan for which you own the servicing rights.

(ii) *No continuing relationship*. A consumer does not, however, have a continuing relationship with you if:

(A) The consumer obtains a financial product or service from you only in isolated transactions, such as using your ATM to withdraw

cash from an account at another financial institution; purchasing a money order from you; cashing a check with you; or making a wire transfer through you;

(B) You sell the consumer's loan and do not retain the rights to service that loan;

(C) You sell the consumer airline tickets, travel insurance, or traveler's checks in isolated transactions;

(D) The consumer obtains one-time personal or real property appraisal services from you; or

(E) The consumer purchases checks for a personal checking account from you.

(f) *Encryption* means 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, consistent with current cryptographic standards and accompanied by appropriate safeguards for cryptographic key material.

(g)(1) *Financial product or service* means any product or service that a financial holding company could offer by engaging in a financial activity under section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)).

(2) *Financial service* includes your evaluation or brokerage of information that you collect in connection with a request or an application from a consumer for a financial product or service.

(h)(1) *Financial institution* means any institution the business of which is engaging in an activity that is financial in nature or incidental to such financial activities as described

in section 4(k) of the Bank Holding Company Act of 1956, 12 U.S.C. 1843(k). An institution that is significantly engaged in financial activities, or significantly engaged in activities incidental to such financial activities, is a financial institution.

(2) *Examples of financial institutions*: (i) A retailer that extends credit by issuing its own credit card directly to consumers is a financial institution because extending credit is a financial activity listed in 12 CFR 225.28(b)(1) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)(4)(F)), and issuing that extension of credit through a proprietary credit card demonstrates that a retailer is significantly engaged in extending credit.

(ii) An automobile dealership that, as a usual part of its business, leases automobiles on a nonoperating basis for longer than 90 days is a financial institution with respect to its leasing business because leasing personal property on a nonoperating basis where the initial term of the lease is at least 90 days is a financial activity listed in 12 CFR 225.28(b)(3) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(F).

(iii) A personal property or real estate appraiser is a financial institution because real and personal property appraisal is a financial activity listed in 12 CFR 225.28(b)(2)(i) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(F).

(iv) A career counselor that specializes in providing career counseling services to individuals currently employed by or recently displaced from a financial organization, individuals who are seeking employment with a financial organization, or individuals who are currently employed by or seeking placement with the finance, accounting or

audit departments of any company is a financial institution because such career counseling activities are financial activities listed in 12 CFR 225.28(b)(9)(iii) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(F).

(v) A business that prints and sells checks for consumers, either as its sole business or as one of its product lines, is a financial institution because printing and selling checks is a financial activity that is listed in 12 CFR 225.28(b)(10)(ii) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(F).

(vi) A business that regularly wires money to and from consumers is a financial institution because transferring money is a financial activity referenced in section 4(k)(4)(A) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(A), and regularly providing that service demonstrates that the business is significantly engaged in that activity.

(vii) A check cashing business is a financial institution because cashing a check is exchanging money, which is a financial activity listed in section 4(k)(4)(A) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(A).

(viii) An accountant or other tax preparation service that is in the business of completing income tax returns is a financial institution because tax preparation services is a financial activity listed in 12 CFR 225.28(b)(6)(vi) and referenced in section 4(k)(4)(G) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(G).

(ix) A business that operates a travel agency in connection with financial services is a financial institution because operating a travel agency in connection with financial

services is a financial activity listed in 12 CFR 225.86(b)(2) and referenced in section 4(k)(4)(G) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(G).

(x) An entity that provides real estate settlement services is a financial institution because providing real estate settlement services is a financial activity listed in 12 CFR 225.28(b)(2)(viii) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(F).

(xi) A mortgage broker is a financial institution because brokering loans is a financial activity listed in 12 CFR 225.28(b)(1) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(F).

(xii) An investment advisory company and a credit counseling service are each financial institutions because providing financial and investment advisory services are financial activities referenced in section 4(k)(4)(C) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(C).

(xiii) A company acting as a finder in bringing together one or more buyers and sellers of any product or service for transactions that the parties themselves negotiate and consummate is a financial institution because acting as a finder is an activity that is financial in nature or incidental to a financial activity listed in 12 CFR 225.86(d)(1).

(3) *Financial institution* does not include:

(i) Any person or entity with respect to any financial activity that is subject to the jurisdiction of the Commodity Futures Trading Commission under the Commodity Exchange Act (7 U.S.C. 1 *et seq.*);

(ii) The Federal Agricultural Mortgage Corporation or any entity chartered and operating under the Farm Credit Act of 1971 (12 U.S.C. 2001 *et seq.*);

(iii) Institutions chartered by Congress specifically to engage in securitizations, secondary market sales (including sales of servicing rights) or similar transactions related to a transaction of a consumer, as long as such institutions do not sell or transfer nonpublic personal information to a nonaffiliated third party other than as permitted by sections 313.14 and 313.15; or

(iv) Entities that engage in financial activities but that are not significantly engaged in those financial activities, and entities that engage in activities incidental to financial activities but that are not significantly engaged in activities incidental to financial activities.

(4) *Examples of entities that are not significantly engaged in financial activities*.

(i) A retailer is not a financial institution if its only means of extending credit are occasional "lay away" and deferred payment plans or accepting payment by means of credit cards issued by others.

(ii) A retailer is not a financial institution merely because it accepts payment in the form of cash, checks, or credit cards that it did not issue.

(iii) A merchant is not a financial institution merely because it allows an individual to "run a tab."

(iv) A grocery store is not a financial institution merely because it allows individuals to whom it sells groceries to cash a check, or write a check for a higher amount than the grocery purchase and obtain cash in return.

(i) *Information security program* means the administrative, technical, or physical safeguards you use to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.

(j) *Information system* means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information containing customer information or connected to a system containing customer information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental controls systems that contains customer information or that is connected to a system that contains customer information.

(k) *Multi-factor authentication* means authentication through verification of at least two of the following types of authentication factors:

(1) Knowledge factors, such as a password;

(2) Possession factors, such as a token; or

(3) Inherence factors, such as biometric characteristics.

(l)(1) *Nonpublic personal information* means:

(i) Personally identifiable financial information; and

(ii) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available.

(2) *Nonpublic personal information* does not include:

(i) Publicly available information, except as included on a list described in paragraph (l)(1)(ii) of this section; or

(ii) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any personally identifiable financial information that is not publicly available.

(3) *Examples of lists* - (i) Nonpublic personal information includes any list of individuals' names and street addresses that is derived in whole or in part using personally identifiable financial information (that is not publicly available), such as account numbers.

(ii) Nonpublic personal information does not include any list of individuals' names and addresses that contains only publicly available information, is not derived, in whole or in part, using personally identifiable financial information that is not publicly available, and is not disclosed in a manner that indicates that any of the individuals on the list is a consumer of a financial institution.

(m) *Penetration testing* means a test methodology in which assessors attempt to circumvent or defeat the security features of an information system by attempting penetration of databases or controls from outside or inside your information systems.

(n) (1) *Personally identifiable financial information* means any information:

(i) A consumer provides to you to obtain a financial product or service from you;

(ii) About a consumer resulting from any transaction involving a financial product or service between you and a consumer; or

(iii) You otherwise obtain about a consumer in connection with providing a financial product or service to that consumer.

(2) *Examples* –

(i) *Information included*. Personally identifiable financial information includes:

(A) Information a consumer provides to you on an application to obtain a loan, credit card, or other financial product or service;

(B) Account balance information, payment history, overdraft history, and credit or debit card purchase information;

(C) The fact that an individual is or has been one of your customers or has obtained a financial product or service from you;

(D) Any information about your consumer if it is disclosed in a manner that indicates that the individual is or has been your consumer;

(E) Any information that a consumer provides to you or that you or your agent otherwise obtain in connection with collecting on, or servicing, a credit account;

(F) Any information you collect through an Internet "cookie" (an information collecting device from a web server); and

(G) Information from a consumer report.

(ii) *Information not included*. Personally identifiable financial information does not include:

(A) A list of names and addresses of customers of an entity that is not a financial institution; and

(B) Information that does not identify a consumer, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names, or addresses.

(o)(1) *Publicly available information* means any information that you have a reasonable basis to believe is lawfully made available to the general public from:

(i) Federal, State, or local government records;

(ii) Widely distributed media; or

(iii) Disclosures to the general public that are required to be made by Federal, State, or local law.

(2) *Reasonable basis*. You have a reasonable basis to believe that information is lawfully made available to the general public if you have taken steps to determine:

(i) That the information is of the type that is available to the general public; and

(ii) Whether an individual can direct that the information not be made available to the general public and, if so, that your consumer has not done so.

(3) *Examples* –

(i) Government records. Publicly available information in government records includes information in government real estate records and security interest filings.

(ii) Widely distributed media. Publicly available information from widely distributed media includes information from a telephone book, a television or radio program, a newspaper, or a web site that is available to the general public on an unrestricted basis. A web site is not restricted merely because an Internet service provider or a site operator requires a fee or a password, so long as access is available to the general public.

(iii) Reasonable basis –

(A) You have a reasonable basis to believe that mortgage information is lawfully made available to the general public if you have determined that the information is of the type included on the public record in the jurisdiction where the mortgage would be recorded.

(B) You have a reasonable basis to believe that an individual's telephone number is lawfully made available to the general public if you have located the telephone number in the telephone book or the consumer has informed you that the telephone number is not unlisted.

(p) *Security event* means an event 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.

(q) *Service provider* means any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a financial institution that is subject to this part.

(r) *You* includes each "financial institution" (but excludes any "other person") over which the Commission has enforcement jurisdiction pursuant to section 505(a)(7) of the Gramm-Leach-Bliley Act.

4. Revise § 314.3(a) as follows:

§ 314.3 Standards for safeguarding customer information.

(a) *Information security program*. You shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue. The information security program shall include the elements set forth in section 314.4 and shall be reasonably designed to achieve the objectives of this part, as set forth in paragraph (b) of this section.

* * * * *

5. Revise §314.4 as follows:

§ 314.4 Elements.

In order to develop, implement, and maintain your information security program, you shall:

(a) Designate a qualified individual responsible for overseeing and implementing your information security program and enforcing your information security program (for purposes of this part, "Qualified Individual"). The Qualified Individual may be employed by you, an affiliate, or a service provider. To the extent this requirement is met using a service provider or an affiliate, you shall:

(1) Retain responsibility for compliance with this part;

(2) Designate a senior member of your personnel responsible for direction and oversight of the Qualified Individual; and

(3) Require the service provider or affiliate to maintain an information security program that protects you in accordance with the requirements of this Part.

(b) Base your 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, and assesses the sufficiency of any safeguards in place to control these risks.

(1) The risk assessment shall be written and shall include:

(i) Criteria for the evaluation and categorization of identified security risks or threats you face;

(ii) Criteria for the assessment of the confidentiality, integrity, and availability of your information systems and customer information, including the adequacy of the existing controls in the context of the identified risks or threats you face; and

(iii) 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.

(2) You shall periodically perform additional risk assessments that reexamine the 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, and reassess the sufficiency of any safeguards in place to control these risks.

(c) Design and implement safeguards to control the risks you identity through risk assessment, including by:

(1) Implementing and periodically reviewing access controls, including technical and, as appropriate, physical controls to (1) authenticate and permit access only to authorized users to protect against the unauthorized acquisition of customer information and (2) limit authorized users' access only to customer information that they need to perform their duties and functions, or, in the case of customers, to access their own information;

(2) Identify and manage the data, personnel, devices, systems, and facilities that enable you to achieve business purposes in accordance with their relative importance to business objectives and your risk strategy;

(3) Protect by encryption all customer information held or transmitted by you both in transit over external networks and at rest. To the extent you determine that encryption of customer information, either in transit over external networks or at rest, is infeasible, you may instead secure such customer information using effective alternative compensating controls reviewed and approved by your Qualified Individual;

(4) Adopt secure development practices for in-house developed applications utilized by you for transmitting, accessing, or storing customer information and procedures for evaluating, assessing, or testing the security of externally developed applications you utilize to transmit, access, or store customer information;

(5) Implement multi-factor authentication for any individual accessing any information system, unless your Qualified Individual has approved in writing the use of reasonably equivalent or more secure access controls;

(6) (i) Develop, implement, and maintain procedures for the secure disposal of customer information in any format no later than two years after the last date the information is used in connection with the provision of a product or service to the customer to which it relates, unless such information is necessary for business operations or for other legitimate business purposes, 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; and

(ii) Periodically review your data retention policy to minimize the unnecessary retention of data;

(7) Adopt procedures for change management; and

(8) Implement policies, procedures and controls designed to monitor and log the activity of authorized users and detect unauthorized access or use of, or tampering with, customer information by such users.

(d) (1) Regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures, including those to detect actual and attempted attacks on, or intrusions into, information systems.

(2) For information systems, the monitoring and testing shall include continuous monitoring or periodic penetration testing and vulnerability assessments. Absent

effective continuous monitoring or other systems to detect, on an ongoing basis, changes in information systems that may create vulnerabilities, you shall conduct:

i. Annual penetration testing of your information systems determined each given year based on relevant identified risks in accordance with the risk assessment; and

ii. Vulnerability assessments, including any systemic scans or reviews of information systems reasonably designed to identify publicly known security vulnerabilities in your information systems based on the risk assessment, at least every six months; and whenever there are material changes to your operations or business arrangements; and whenever there are circumstances you know or have reason to know may have a material impact on your information security program.

(e) Implement policies and procedures to ensure that personnel are able to enact your information security program by:

(1) Providing your personnel with security awareness training that is updated as necessary to reflect risks identified by the risk assessment;

(2) Utilizing qualified information security personnel employed by you or an affiliate or service provider sufficient to manage your 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.

(f) 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 your service providers by contract to implement and maintain such safeguards; and

(3) Periodically assessing your service providers based on the risk they present and the continued adequacy of their safeguards.

(g) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (d) of this section; any material changes to your operations or business arrangements; the results of risk assessments performed under paragraph (b)(2) of this section; or any other circumstances that you know or have reason to know may have a material impact on your information security program.

(h) 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 your control. Such incident response plan shall 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.

(i) Require your Qualified Individual to report in writing, regularly and at least annually, to your board of directors or equivalent governing body. If no such board of directors or equivalent governing body exists, such report shall be timely presented to a senior officer responsible for your information security program. The report shall include the following information:

(1) The overall status of the information security program and your compliance with this 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.

6. Revise § 314.5 to read as follows:

§ 314.5 Effective date.

Sections 314.4(a), 314.4(b)(1), 314.4(c)(1)-(8), 314.4(d)(2), 314.4(e), 314.4(f)(3), 314.4(h), and 314.4(i) are effective as of [INSERT DATE ONE YEAR AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

7. Add § 314.6, to read as follows:

§ 314.6 Exceptions.

Sections 314.4(b)(1), 314.4(d)(2), 314.4(h), and 314.4(i) do not apply to financial institutions that maintain customer information concerning fewer than five thousand consumers.

By direction of the Commission.

April Tabor,

Secretary of the Commission.