[Billing Code: 6750-01S]

FEDERAL TRADE COMMISSION

16 CFR Part 314

RIN 3084-AB35

Standards for Safeguarding Customer Information

AGENCY: Federal Trade Commission.

ACTION: Notice of proposed rulemaking; request for public comment.

SUMMARY: The Federal Trade Commission ("FTC" or "Commission") requests public comment on its proposal to amend the Standards for Safeguarding Customer Information ("Safeguards Rule" or "Rule"). The proposal 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 small businesses 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. Such a change would add "finders"–companies that bring together buyers and sellers of a product or service–within the scope of the Rule. Finally, the Commission proposes to include the definition of "financial institution" and related examples in the Rule itself rather than incorporate them

by reference from a related FTC rule, the Privacy of Consumer Financial Information Rule.

DATES: Written comments must be received on or before [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*].

ADDRESSES: Interested parties may file a comment online or on paper by following the Request for Comment part of the **SUPPLEMENTARY INFORMATION** section below. Write "Safeguards Rule, 16 CFR Part 314, Project No. P145407," on your comment and file your comment online at https://www.regulations.gov by following the instructions on the web-based form. If you prefer to file your comment on paper, mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue, N.W., Suite CC-5610 (Annex B), Washington, D.C. 20580, or deliver your comment to the following address: Federal Trade Commission, Office of the Secretary, Constitution Center, 400 7th Street S.W., 5th Floor, Suite 5610 (Annex B), Washington, D.C. 20024.

FOR FURTHER INFORMATION CONTACT:

David Lincicum or Allison M. Lefrak, 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 or (202) 326-2804.

SUPPLEMENTARY INFORMATION:

I. Background

The Gramm Leach Bliley Act ("GLB" or "GLBA") was enacted in 1999.[1] The GLBA provides a framework for regulating the privacy and data security practices of a

[1] Pub. L. 106–102, 113 Stat. 1338 (1999).

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.

The 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

[2] *See* 15 U.S.C. 6801(b), 6805(b)(2).
[3] 16 CFR 314.2(c).
[4] 16 CFR 314.3(a).
[5] 16 CFR 314.3(a), (b).

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, including in the areas of: (1) employee training and management; (2) information systems, including network and software design, as well as information processing, storage, transmission, and disposal; and (3) detecting, preventing, and responding to attacks, intrusions, or other systems failures.[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 procedures.[8] The financial institution is also required to evaluate and adjust its information security program in light of the results of this testing and monitoring, as well as 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 Safeguards Rule requires financial institutions to take reasonable steps to select and retain service providers that are capable of maintaining appropriate

[6] 16 CFR 314.3(a), (b).
[7] 16 CFR 314.4(b).
[8] 16 CFR 314.4(c).
[9] 16 CFR 314.4(e).
[10] 16 CFR 314.4(a).

safeguards for customer information and require those service providers by contract to implement and maintain such safeguards.[11]

When the Commission issued the Rule in 2002, it opted to provide general requirements and guidance for the required information security program, without providing detailed descriptions of what the information security program should contain.[12] It took this approach in order to provide financial institutions with the flexibility to shape the information security programs to their particular business and to allow the programs to adapt to changes in technology and threats to the security and integrity of customer information.[13] While the Commission believes the proposed amendments continue to provide companies with flexibility, they also attempt to provide more detailed guidance as to what an appropriate information security program entails.

II. Regulatory Review of the Safeguards Rule

On August 29, 2016, the Commission solicited comments on the Safeguards Rule as part of its periodic review of its rules and guides.[14] 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 representing a wide range of viewpoints.[15] Most commenters agreed that there is a continuing need for the

[11] 16 CFR 314.4(d).
[12] *See* Standards for Safeguarding Customer Information, Final Rule, 67 FR 36484 (May 23, 2002).
[13] *Id.*
[14] Safeguards Rule, Request for Comment, 81 FR 61632 (Sept. 7, 2016).
[15] The comments are posted at: https://www.ftc.gov/policy/public-comments/initiative-674. The Commission has assigned each comment a number appearing after the name of the commenter and the date of submission. This notice cites comments using the last name of the individual submitter or the name of the organization, followed by the number assigned by the Commission.

Rule and that it benefits consumers and competition.[16] The Commission also generally asked commenters to weigh in on: (1) whether the Commission should add more specific requirements for information security programs to the Rule; (2) whether the Rule should require the inclusion of an incident response plan; (3) whether the Rule should reference or incorporate any other information security standards or framework, such as the National Institute of Standards and Technology's Cybersecurity Framework or the Payment Card Industry Data Security Standard; (4) whether the Rule should contain its own definition of "financial institution" rather than incorporate the definition set forth in the Privacy Rule; and (5) whether the definition of "financial institution" should be expanded.

1. Whether the Safeguards Rule should include more specific requirements for information security programs.

Several commenters urged the Commission not to add more specific and prescriptive requirements for information security programs.[17] These commenters stated that financial institutions are familiar with the Rule in its current form and have established practices and policies in reliance on it;[18] that preserving the Rule's flexible guidelines for information security plans enables financial institutions to adapt quickly to

[16] *See, e.g.*, Mortgage Bankers Association (Comment #39); National Automobile Dealers Association (Comment #40); Data & Marketing Association (Comment #38); Electronic Transactions Association (Comment #24); State Privacy & Security Coalition (Comment #26).
[17] *See, e.g.*, American Financial Services Association (Comment #42); Securities Industry and Financial Markets Association (Comment #25); State Privacy & Security Coalition (Comment #26); EDUCAUSE (Comment #17); Mortgage Bankers Association (Comment #39).
[18] National Automobile Dealers Association (Comment #40).

the rapidly changing cybersecurity landscape;[19] and that additional prescriptive requirements for information security plans would negatively impact innovation.[20]

Some commenters asserted that a more prescriptive regulatory approach for information security programs in the Rule would not necessarily make institutions more secure and cautioned that regulation that adopts a checklist approach to information security plans risks creating complacency among companies.[21] A few commenters proposed that rather than amending the Rule to add more specific and prescriptive requirements for information security plans, the Commission should promote self-regulation as an appropriate tool to effectively promote information security.[22]

On the other hand, some commenters recommended that the FTC strengthen the Rule by including more detailed security requirements.[23] The Clearing House Association LLC ("The Clearing House"), a banking association and payments company that is owned by the largest commercial banks, argued that the Rule's requirements, at least with respect to large financial technology ("Fintech") companies, should be more akin to the rules applicable to banks under the Federal Financial Institutions Examination Council ("FFIEC") Interagency Guidelines. Among other things, these guidelines specify elements that financial institutions should include in a risk assessment; areas a financial institution must consider—such as access controls, encryption, and incident

[19] *See, e.g.*, American Financial Services Association (Comment #42); Securities Industry and Financial Markets Association (Comment #25); State Privacy & Security Coalition (Comment #26); EDUCAUSE (Comment #17); Mortgage Bankers Association (Comment #39).
[20] *See, e.g.*, Data & Marketing Association (Comment #38); Electronic Transactions Association (Comment #24).
[21] *See e.g.*, Software & Information Industry Association (Comment #23); Electronic Transactions Association (Comment #24).
[22] Data & Marketing Association (Comment #38); Electronic Transactions Association (Comment #24); State Privacy & Security Coalition (Comment #26).
[23] The Clearing House Association LLC (Comment #35); Electronic Privacy Information Center (Comment #30).

response—in developing security controls; and provisions that financial institutions must include in contracts with service providers. The Electronic Privacy Information Center ("EPIC") recommended that certain practices set forth in the FTC's Safeguards Rule Guidance, such as employee background checks, authentication requirements, and encryption, should be mandatory.[24]

Having considered these comments, the Commission proposes to amend the Rule to include more specific security requirements. While the Commission agrees with those commenters that argued that the flexibility of the current Safeguards Rule is a strength that allows the Rule to adapt to changing technology and threats, the Commission believes that more specific requirements will benefit financial institutions by providing them more guidance and certainty in developing their information security programs, while largely preserving that flexibility. The Commission agrees that a checklist approach is not appropriate, which is why the proposed amendments retain the existing Rule's process-based approach, allowing companies to tailor their programs to their size and to the sensitivity and amount of customer information they collect. As to the commenters that stated that the current Rule works well and that companies have already developed compliance programs under it, the Commission does not believe the proposed new requirements would require an overhaul of existing compliance programs. Because the new requirements build on existing requirements, they will help companies benchmark and improve their current compliance programs, rather than having to start

[24] Electronic Privacy Information Center (Comment #30), *citing Financial Institutions and Customer Information: Complying with the Safeguards Rule*, FED. TRADE COMM'N (Apr. 2006), https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying [hereinafter "Safeguards Rule Guidance"]. EPIC also urged the Commission to apply the Rule to all types of businesses, not just financial institutions, but the GLBA provides statutory authority only for requirements applicable to financial institutions.

from scratch. Finally, the Commission recognizes that some of the financial institutions to which the Safeguards Rule applies—such as tax preparers or mortgage brokers—may be very small businesses with few customers. Accordingly, the proposed amendment would exempt smaller financial institutions from certain requirements of the amended Rule.

The Commission also agrees that very specific requirements for information security programs could become outdated and require frequent amendments. Accordingly, the proposed amendments provide more detailed requirements as to the issues and threats that must be addressed by the information security program, but do not require specific solutions to those problems. Instead, the proposed amendments retain the process-based approach of the Rule, while providing a more detailed map of what information security plans must address. As discussed in detail below, information security programs under the proposed amendments would still be based on risk assessments performed by the covered financial institutions and would be developed to address the specific risks and needs of the financial institution. The Commission continues to believe that a flexible, non-prescriptive Rule enables covered organizations to use it to respond to the changing landscape of security threats, to allow for innovation in security practices, and to accommodate technological changes and advances. The proposed amendments are designed to preserve that flexibility while doing more to ensure that financial institutions develop information security plans that are appropriate, reasonable, and designed to protect customer information.[25] Although the Commission

[25] The Commission agrees with the Electronic Transactions Association (Comment #24) about the importance of self-regulation in this area and continues to work with industry groups to promote industry-specific guidance and training on security.

believes the proposed approach is sufficiently flexible, it seeks comment on whether the approach creates unintended consequences for businesses, may be more stringent than necessary to achieve the objective, and/or unnecessarily modifies language without creating a material benefit to security.

2. Whether the Rule Should Require the Inclusion of an Incident Response Plan

The Commission sought comment on whether the Rule should require an incident response plan. Several commenters were opposed to adding such a requirement. Some of these commenters noted that states already require companies to notify consumers of a breach and that companies effectively must have some sort of incident response plan in place to meet this requirement, so there would be no need to add this requirement to the Rule.[26] Some commenters argued that such a requirement would be burdensome for many businesses.[27] Others stated that there is no need to add such a requirement because, for many financial institutions, in order to satisfy the Rule's current requirement to have a reasonable information security program, a financial institution would necessarily be required to have an incident response plan.[28] On the other hand, The Clearing House noted that an incident response program is "a crucial element of data security hygiene in the increasingly dangerous threat environment" and urged that the Commission impose

[26] *See, e.g.*, Securities Industry and Financial Markets Association (Comment #25); National Automobile Dealers Association (Comment #40).
[27] *See, e.g.*, National Automobile Dealers Association (Comment #40); Securities Industry and Financial Markets Association (Comment #25);
[28] *See, e.g.*, Consumer Data Industry Association (Comment #36); EDUCAUSE (Comment #17); MasterCard Worldwide (Comment #14).

this requirement on FTC-regulated financial institutions, especially since this is already a requirement for banks under the FFIEC Interagency Guidelines.[29]

The Commission agrees that the current Rule already requires many financial institutions to develop an incident response plan as part of their information security program. However, the Commission believes there is value to making such a requirement explicit. Accordingly, the Commission proposes an amendment to the Rule to require covered financial institutions to develop an incident response plan as part of their information security program, as described in greater detail below. The Commission does not agree that a process-based requirement that financial institutions plan for an incident encourages a "check the box" approach. Nor does the Commission agree that such an obligation is generally burdensome, particularly for businesses operating nationwide, given that many institutions already must develop a response plan to comply with state law.[30]

The proposed amendment lists several general areas that the plan would need to address, as discussed in greater detail below. The Commission seeks comment about the potential costs and benefits of this proposal. In particular, the Commission is interested in any data, research or case studies that the Commission could use to analyze what commenters advocate. The proposed amendment is designed to ensure that covered financial institutions are prepared in the event of a cybersecurity event, while still giving them ample flexibility to adapt the plan to the needs and resources of their business.

3. Whether the Safeguards Rule should reference or incorporate any other information security standards or framework, such as the National

[29] The Clearing House (Comment #35).
[30] *See e.g.*, n.26.

Institute of Standards and Technology's Cybersecurity Framework or the Payment Card Industry Data Security Standard.

The Commission sought comment on whether the Rule should reference or incorporate any other information security standards or frameworks, such as the National Institute of Standards and Technology's ("NIST") Cybersecurity Framework (the "Framework") or the Payment Card Industry Data Security Standard ("PCIDSS").

The majority of commenters advocated against referring to or incorporating any other information security standard or framework, such as the NIST Framework or PCIDSS, into the Rule.[31] Some commenters argued that the FTC should not adopt the NIST Framework as a binding set of obligations because it would lead to a "check the box" security mandate, and would add a layer of complexity to an already complex regulatory environment where institutions have to comply with numerous preexisting federal and state requirements.[32] The Electronic Transactions Association ("ETA") argued that the Framework is "not designed to replace an organization's cybersecurity risk management" and that it is not intended to be a standard or checklist.[33]

A few commenters wrote in support of incorporating a reference to the NIST Framework in the Rule, while not requiring compliance with the Framework.[34] For example, the Financial Services Roundtable/BITS ("FSR/BITS") argued that incorporating the NIST Framework in the Rule as an informative reference would help to address "the growing thicket of cybersecurity compliance obligations that are spreading

[31] *See, e.g.*, U.S. Chamber of Commerce, Center for Capital Markets Competitiveness (Comment #22); Retail Industry Leaders Association (Comment #18); Electronic Transactions Association (Comment #24); EDUCAUSE (Comment #17).
[32] EDUCAUSE (Comment #17).
[33] Electronic Transactions Association (Comment #24).
[34] *See, e.g.*, Financial Services Roundtable/BITS (Comment #21); Software & Information Industry Association (Comment #23).

across the financial services sector."[35] FSR/BITS recommended further that the Commission modify the Rule so that financial institutions that use the NIST Framework would be found in *de facto* compliance with the Rule.[36]

With respect to the PCIDSS, numerous commenters opposed the Rule's reference or incorporation of PCIDSS.[37] Commenters argued such an amendment has the possibility of undermining the Rule's flexibility by imposing a "one-size-fits-all" approach.[38] MasterCard Worldwide, a co-founder and developer of PCIDSS, opposed this amendment to the Rule, highlighting that the PCIDSS was created by major card networks for participants in the card industry.[39] Whereas the PCIDSS may be appropriate for payment card issuers and acquirers, MasterCard argued, it would not necessarily apply well to other financial institutions.[40] Other comments agreed that incorporating PCIDSS would be inappropriate.[41] No commenters wrote in support of referencing or incorporating the PCIDSS into the Rule. Having considered these comments, the Commission declines to propose changing the Rule to incorporate or reference a particular security standard or framework. As noted above, for a variety of reasons, including questions about the applicability of the particular standards at issue to all financial institutions, the majority of commenters opposed referencing or

---

[35] Financial Services Roundtable/BITS (Comment #21).
[36] *Id.*
[37] *See, e.g.*, Electronic Transactions Association (Comment #24);MasterCard Worldwide (Comment #14); Retail Industry Leaders Association (Comment #18).
[38] Electronic Transactions Association (Comment #24); EDUCAUSE (Comment #17).
[39] MasterCard Worldwide (Comment #14).
[40] *Id.*
[41] *See* Securities Industry and Financial Markets Association (Comment #25) (arguing that there is insufficient overlap between payment card industry and covered financial institutions to justify adopting PCIDSS); Retail Industry Leaders Association (Comment #18) (arguing that adopting PCIDSS would not be an effective basis for a regulation); National Retail Federation (Comment #29) (noting that PCIDSS is a proprietary information security standard controlled by a single industry); State Privacy & Security Coalition (Comment #26) (arguing that adopting PCIDSS would amount to outsourcing federal rulemaking authority).

incorporating any specific information security standard or framework into the Rule. Mandating that companies follow a particular security standard or framework would reduce the flexibility built into the current Rule. This proposal does not amend the Rule to allow compliance with such standards to serve as a safe harbor against Commission enforcement, as some commenters sought. The Commission seeks additional comment on how such a program could remain up to date and respond rapidly to changes in the security environment, and the workability of monitoring changing standards and adapting a safe harbor rule as needed.

4. *Whether the Safeguards Rule should contain its own definition of "financial institution" rather than incorporate the definition set forth in the Privacy Rule.*

The Commission also asked whether the Rule should be revised to incorporate a definition of "financial institution" and related examples in the Rule itself, rather than incorporate by reference definitions and examples set forth in the Privacy Rule.[42]

The term "financial institution" is defined in the Privacy Rule, and that term is incorporated by reference in the Safeguards Rule.[43] Under the Dodd-Frank Act,[44] the majority of the Commission's rulemaking authority for the Privacy Rule was transferred to the Consumer Financial Protection Bureau, with the exception of rulemaking authority pertaining to certain motor vehicle dealers.[45] Accordingly, the Commission's Privacy Rule now applies only to certain motor vehicle dealers. The Safeguards Rule, however, still applies to all financial institutions within the FTC's general enforcement

[42] Privacy of Consumer Financial Information Rule ("Privacy Rule"), 16 CFR pt. 313.
[43] 16 CFR 313.3(k); 16 CFR 314.2(a).
[44] Pub. L. 111-203, 124 Stat. 1376 (2010).
[45] 15 U.S.C. 6804(a)(1)(C).

jurisdiction.[46] Thus, currently, the definition of "financial institution" in the Privacy Rule—which governs the scope of the Safeguards Rule—applies to all financial institutions within the Commission's jurisdiction, despite the fact that most types of financial institutions are no longer subject to the Privacy Rule. This creates a confusing situation where the Privacy Rule, on its face, appears to cover types of "financial institutions" that the Privacy Rule no longer covers.

To address this issue, the Commission proposes incorporating the definition of "financial institution" and the accompanying examples from the Privacy Rule into the Safeguards Rule.[47] None of the commenters voiced a view one way or the other on this issue. The Commission notes that this modification would have no substantive effect on the scope of the Rule or its enforcement.[48] This change will only increase the clarity of the Rule.

> *5. Whether, if the Safeguards Rule is amended to include its own definition of "financial institution," that definition should be expanded to also include (1) entities that are significantly engaged in activities that the Federal Reserve Board has found to be incidental to financial activities and/or (2) activities that have been found to be closely related to banking or incidental to financial activities by regulation or order in effect after the enactment of the GLBA.*

Finally, the Commission asked about the scope of the definition of "financial institution." When promulgating the Privacy Rule in 2000, the Commission determined that companies engaged in activities that are "incidental to financial activities" would not be considered "financial institutions."[49] The Commission was the only agency to adopt

---

[46] 15 U.S.C. 6804(a)(1)(A).
[47] The Commission is releasing a NPRM that proposes parallel revisions to the Privacy Rule concurrently with this NRPM.
[48] Separately, as noted below, the Commission proposes to revise the definition of "financial institution" to cover finders.
[49] *See* 16 CFR 313.3(k); *see also* 65 FR 33646, 33654 (May 24, 2000).

this restrictive definition in its Privacy Rule, while the other agencies included incidental activities.[50] In addition, the Commission decided that activities that were determined to be financial in nature after the enactment of the GLBA would not be automatically included in its Privacy Rule; rather, the Commission would have to take additional action to include them.[51] The effect of these two decisions was to limit the activities covered by the Commission's rules to those set out in 12 CFR 225.28 as it existed in 2000, and to exclude any activities later determined by the Federal Reserve Board to be financial activities or incidental to those activities.[52] The definition from the Privacy Rule was incorporated into the Safeguards Rule.[53] Thus, in the Request for Comment,[54] the Commission sought comment on whether it should more closely align with other agencies and amend the Safeguards Rule to include "incidental" activities and activities determined to be financial or incidental after 1999.

In 2000, the Federal Reserve Board determined that acting as a "finder" is an activity that is "incidental to a financial activity."[55] The Federal Reserve Board defined "finding" as bringing together buyers and sellers of products or services for transactions that the buyers and sellers themselves negotiate and consummate.

The majority of commenters who addressed the definition of "financial institutions" urged the Commission not to amend the definition to include more than those businesses that conduct traditional financial activities or to include activities

[50] The Commission also added the requirement that an entity must be "significantly engaged" in the financial activity to be considered a financial institution under the Privacy Rule. 16 CFR 313.3(k). The Commission is not proposing to change this requirement.
[51] 65 FR 33646, 33654 n.23 (May 24, 2000).
[52] *Id*.
[53] 16 CFR 314.2(a).
[54] 81 FR 61632 (Sept. 7, 2016).
[55] *See* 65 FR 80735 (Dec. 22, 2000); 12 CFR 225.86(d)(1).

determined to be financial in nature or incidental after the enactment of the GLBA.[56] For example, the Software & Information Industry Association ("SIIA") commented that the Rule already has an impact beyond financial institutions themselves in encouraging entities that receive customer information from financial institutions to take measures to secure that data, even though they may not be legally obligated to do so under the Rule.[57] Per SIIA, this is because they are either contractually bound by partnerships with financial institutions, or compete for business on the ability to meet high security requirements.[58] The Securities Industry and Financial Markets Association ("SIFMA") also opposed this amendment, claiming that the securities industry makes a proactive, regular effort to familiarize itself with other regulatory frameworks' definitions in order to satisfy the Rule's "reasonable" standard.[59] Thus, the Rule already implicitly requires their industry, SIFMA argues, "to understand the Privacy Act, Federal Reserve Board guidance, and the [GLBA's] impact. Creating new, or modifying existing, definitions in the Rule would eliminate the Rule's flexibility in this regard."[60]

In opposition to an expansion of the definition of financial institutions that might include incidental participants in financial transactions, the National Association of Convenience Stores ("NACS") noted that some incidental participants—such as its members—do not store customer-identifying information, nor do they have continuing information-based relationships with consumers that would justify development and

[56] *See, e.g.*, National Association of Convenience Stores (Comment #28); Software & Information Industry Association (Comment #23); Securities Industry and Financial Markets Association (Comment #25).
[57] Software & Information Industry Association (Comment #23). *But see* National Automobile Dealers Association (Comment #40) (supporting more specific requirements for service providers' security).
[58] Software & Information Industry Association (Comment #23).
[59] Securities Industry and Financial Markets Association (Comment #25).
[60] *Id.*

maintenance of a comprehensive security program.[61] Further, according to NACS, its members do not handle some of the most sensitive personal information such as Social Security numbers and driver's license numbers that are more commonly associated with identity theft.[62] Financial institutions, by contrast, do handle such sensitive personal consumer information.[63]

On the other hand, EPIC advocated that the Commission expand the scope of the Rule to include "all organizations and companies that collect consumer data," such as educational institutions and commercial businesses that process student and consumer information.[64] In underscoring the importance of doing so, EPIC noted that such organizations frequently collect the same sensitive information as traditional financial institutions and are subject to the same security threats.[65]

Having considered these comments, the Commission proposes amending the definition of "financial institution" to include "incidental" activities and activities determined to be financial or incidental after 1999. This change would bring "finders" within the scope of the Rule. The Commission recognizes that commenters generally opposed revising the definition, but notes that commenters' concerns generally related to issues not presented by the proposed change *(e.g.*, bringing such entities as convenience stores or securities firms within the Rule's ambit).

The Commission is not proposing such a broad expansion, however. The only effect of this proposed amendment would be to cause finders, whose activities often

---

[61] National Association of Convenience Stores (Comment #28).
[62] *Id.*
[63] *Id.*
[64] Electronic Privacy Information Center (Comment #30).
[65] *Id.*

involve collection of financially sensitive personal information, to be covered by the Rule. This modification would ensure that finders adequately protect that information. Because they collect, maintain, and store sensitive consumer information, it is important for them to be subject to requirements to safeguard it. If this sensitive information were to get into the wrong hands, consumers could suffer identity theft, fraud, and other harms.

The Commission's proposed change would not bring any other activities under the coverage of the Rule because the Federal Reserve Board has not determined any activity other than finding to be financial in nature, or incidental to such activity, since the enactment of the GLBA. Further, it would harmonize the Commission's Rule with other regulators' Safeguards Rules—which already cover institutions engaged in activities incidental to financial activities—as well as Regulation P, which applies to all other financial institutions that are not covered by the Privacy Rule.[66] This harmonization will create a more consistent regulatory landscape that will help to treat businesses the same regardless of which agency is regulating them. Accordingly, the Commission's proposed amendment to section 314.1(b) indicates that the Rule's scope includes companies that engage in activities that are financial in nature or incidental to such financial activities. Likewise, the proposed definition of "financial institution" in proposed section 314.2(e)(1) also includes companies engaged in activities that are incidental to financial activities.

In connection with this proposal, the Commission requests comment on the impact of expanding the definition of "financial institutions" to include finders.

[66] As noted above, however, unlike other agencies' equivalent rules, the FTC Safeguards Rule limits financial institutions to those "significantly engaged" in the financial activity. The Commission is proposing to retain this limitation and extend it to activity incidental to financial activity.

Specifically, the Commission seeks information on (1) the number of finders in the marketplace that would be included in this definition; and (2) the costs and benefits, including the costs and benefits to finders and consumers, of this proposal.

III. Section-by-Section Analysis

As discussed above, the Commission proposes to amend the Safeguards Rule to include more detailed requirements for the development and establishment of the information security program required under the Rule. These amendments are based primarily on the cybersecurity regulations issued by the New York Department of Financial Services, 23 NYCRR 500 ("Cybersecurity Regulations"), and the insurance data security model law issued by the National Association of Insurance Commissioners ("Model Law").[67] The Cybersecurity Regulations were issued in February 2017 after two rounds of public comment. The Model Law was issued in October 2017. The Commission believes that both the Cybersecurity Regulations and the Model Law maintain the balance between providing detailed guidance and avoiding overly prescriptive requirements for information security programs. The proposed amendments do not adopt either law wholesale, instead taking portions from each and adapting others for the purposes of the Safeguards Rule.[68]

The Commission is interested in receiving data, research, case studies, or other evidence related to business efforts to comply with the Cybersecurity Regulations or state

[67] National Association of Insurance Commissioners, Insurance Data Security Model Law (2017), www.naic.org/store/free/MDL-668.pdf. South Carolina has enacted legislation based on the Model Law. 2017 S.C. Act No. 171, R. 184, H 4655.

[68] At the time the Commission issued its request for comments, neither the Cybersecurity Regulations nor the Model Law had been implemented, so the Commission did not seek comment on the more detailed approaches they adopted. The Commission is doing so through this NPRM.

laws mirroring the Model Law. The Commission is also interested in receiving comments on the extent to which the proposal would preempt existing state laws. Section 507(a) of the GLBA, 15 U.S.C. § 6807(a), preserves a state "statute, regulation, order, or interpretation" that is not "inconsistent" with the privacy and security provisions of the GLBA. The Commission is interested in hearing about the effect of the proposal on companies' compliance with state and federal law. Finally, in light of the proposed amendments and the existence of several cybersecurity frameworks that require processes similar to the Proposed Rule, the Commission additionally requests comments on the potential for safe harbors against Commission enforcement of the Safeguards Rule, including evidence on the efficacy and utility of safe harbors in other contexts and perspectives on the viability of a safe harbor in the present context, especially as safe harbors relate to small business.

In addition to the amendments related to the requirements for information security programs, the Commission proposes amendments to the definition of "financial institution" and the addition of examples previously contained in the Privacy Rule, as discussed above. It also adds to the definition of "financial institution" entities that engage in activities incidental to financial activities. The following is a section-by-section analysis of the proposed amendments. The Commission seeks comments on the proposed amendments in general but also seeks comment on specific questions as set forth in the analysis below.

Proposed amendments to section 314.1: Purpose and Scope.

The proposed amendment would add language from section 313.1(b) of the Privacy Rule, relating to the scope of the Rule and definition of financial institution, to

section 314.1(b) of the Safeguards Rule. This addition would set forth the scope of the Safeguards Rule, which previously applied to the same entities as the Privacy Rule until the Dodd-Frank Act limited the scope of the Privacy Rule only to certain automobile dealers. As noted above, the Commission is proposing in a concurrent NPRM to amend the Privacy Rule to reflect the narrower scope of that regulation[69] and, in turn, proposes to amend the Safeguards Rule to clarify that it retains its original scope. Section 314.1(b) states that the Safeguards Rule applies to the handling of customer information by all financial institutions over which the Commission has jurisdiction. The proposed amendment sets forth the general definition of "financial institution" and provides examples of financial institutions under the Commission's jurisdiction, such as finance companies and mortgage brokers. The added language is taken largely from the existing Privacy Rule. The new language is not meant to change the scope of the Safeguards Rule, other than to reflect the proposed addition of "finders" to the Rule's scope, as discussed below.

Proposed amendment to section 314.2: Definitions

The proposed amendments to section 314.2 add definitions to terms introduced in the proposed amended Rule. The proposed amendments do not alter or remove any definitions in the existing Rule. Existing definitions are interspersed with new definitions in alphabetical order. The Commission is interested in hearing whether these updated definitions reflect current practices, or whether they need to be adjusted to avoid unintended consequences, modified or eliminated for smaller firms, or narrowed to avoid undue burden. Proposed paragraph (a), which states that terms used in the Safeguards

[69] A notice of proposed rulemaking relating to the Privacy Rule is published elsewhere in this issue of the *Federal Register*.

Rule have the same meaning as set forth in the Privacy Rule, would be unchanged from the existing Rule. This provision will apply to terms defined in the Privacy Rule but not in the Safeguards Rule, such as "customer" and "nonpublic personal information."

Proposed paragraph (b) would define an "authorized user" of an information system as any employee, contractor, agent or other person that participates in the business operations of an entity and is authorized to access and use any of that financial institution's information systems and data.[70] This term is used in proposed section 314.4(c)(10), which requires financial institutions to implement policies to monitor the activity of authorized users and detect unauthorized access to customer information.

Proposed paragraph (c) would define a "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."[71] This term is used in proposed provisions requiring financial institutions to establish written incident response plans designed to respond to security events and to implement audit trails to detect and respond to security events. It also appears in a proposed provision requiring a financial institution's chief information security officer to provide an annual report to the financial institution's governing body, which must identify all security events that took place that year.

---

[70] This definition is substantively identical to the definition found in 23 NYCRR 500.01(b).

[71] This definition is based on the definition found in the Model Law, Section 3(D). The proposed amendment adopts the term "security event" in place of the Model Law's term "cybersecurity event" to clarify that an information security program encompasses information in both digital and paper form and that unauthorized access to paper files would also be a security event under the Rule. For this reason, throughout the proposed amendment, the Commission has proposed to replace the term "cybersecurity" from the Cybersecurity Regulations and Model Law with either "information security" or simply "security." In addition, the proposed definition does not include the Model Law's exemption for the acquisition of encrypted information or events where the covered entity determines that the information accessed by an unauthorized person has not been used or released and has been returned or destroyed. In both instances, the Commission believes that a financial institution should still engage in its incident response procedures to address the failures in its information security that allowed such events to occur.

Proposed paragraph (d) is the existing Rule's paragraph (b) and would not alter the definition of "customer information."

Proposed paragraph (e) would define "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 is used in proposed section 314.4(c)(4), which generally requires financial institutions to encrypt customer information, with certain exceptions. This definition is adopted from the Model Law[72] and is intended to define the process of encryption while not requiring any particular technology or technique for achieving the protection provided by encryption. The Commission seeks comment on this definition.

As discussed above, proposed paragraph (f) would incorporate the definition of "financial institution" from the Privacy Rule. The Commission is proposing one substantive change to the definition of "financial institution" to include entities that are "significantly engaged in activities that are incidental" to financial activities as defined by the Bank Holding Company Act. As discussed above, this change would bring 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) would add 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 uses the language set forth in 12 CFR 225.86(d)(1), which defines finding as an activity that is incidental to a financial activity under the Bank Holding Company Act.

[72] Model Law, Section 3(F).

Proposed paragraph (g) is the existing Rule's paragraph (c) and would not alter the definition of "information security program."

Proposed paragraph (h) would define "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."[73] The term "information system" is used throughout the proposed amendments to designate the systems that must be covered by the information security program. This definition is designed to cover the systems, including hardware, software, and networks that financial institutions use to maintain, process, access and store customer information. It is meant to be a broad definition that covers any system that, if compromised, could result in unauthorized access to customer information.

Proposed paragraph (i) would define "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 is used in proposed section 314.4(c)(6), which requires financial institutions to implement multi-factor authentication for individuals accessing internal networks that contain customer information. This definition comes from the Cybersecurity Regulations[74] and is

[73] This definition is identical to the definition in 23 NYCRR 500.1(e).

[74] 23 NYCRR 500.01(f). The proposed amendment deviates from the language of the Cybersecurity Regulations in that it does not include text messages as an example of a possession factor. As NIST has noted, SMS text messages are vulnerable to compromise and may not be an appropriate means of verifying identity. *See, e.g.*, NIST Special Publication 800-63B, Digital Identity Guidelines, 5.1.3.3 (restricting use

designed to conform to current understanding of what constitutes multi-factor authentication while still allowing financial institutions considerable flexibility in designing systems to protect their networks.[75] Under this definition, a system of multi-factor authentication would need to verify at least two of the three types of factors, but has considerable flexibility in how to implement each factor. For example, under the knowledge factor, financial institutions are not limited to requiring passwords for access to systems, but might also use biographical information, or other knowledge that should be limited to the authorized user. The possession factor, could include verifying that a recognized device is accessing the system, or the transmission of a one-time code to a device on file with the financial institution. For the inherence factors, fingerprints, retina scans, or voice prints can be used. The Commission seeks comment on whether this definition is sufficiently flexible, while still requiring the elements of meaningful multi-factor authentication.

Proposed paragraph (j) would define "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."[76] This term is used in proposed section 314.4(d)(2), which requires financial institutions to continually monitor the effectiveness of their safeguards or to engage in annual penetration testing. The primary example of penetration testing is where a security expert uses common techniques in an attempt to breach the security of a

---

of verification using the Public Switched Telephone Network (SMS or voice) as an "out-of-band" factor for multifactor authentication).

[75] *See* NIST, Glossary, "Multifactor Authentication," https://csrc.nist.gov/glossary/term/Multi_Factor_Authentication.

[76] This definition is substantively identical to the definition found in 23 NYCRR 500.01(h).

financial institution's information system. As set forth in the proposed definition, this includes attempts where the penetration tester is acting as an outsider who must penetrate the system without any initial access to the system, and attempts where the tester acts as someone with limited access to the system—such as a contractor or employee—and tries to access information that such an insider is not authorized to access. The Commission believes that there is currently a commonly understood definition of these services and that this definition provides sufficient guidance to understand the requirements of the proposed amendments.

Proposed paragraph (k) is the existing Rule's paragraph (d) and would not alter the definition of "service provider."

Proposed amendment to section 314.3: Standards for safeguarding customer information

Current section 314.3 requires financial institutions to develop an information security program (subsection (a)) and sets forth the objectives of the Rule (subsection (b)). Proposed section 314.3 retains the current requirements of section 314.3 under subsection (a) and the existing statement of objectives under subsection (b). It would, however, change the requirement that "safeguards" be based on the elements set forth in section 314.4, by replacing "safeguards" with "information security program." This change is proposed to clarify that the elements set forth in section 314.4 are parts of the information security plan.

Proposed amendments to section 314.4: Elements

The proposed amendments to section 314.4 would alter existing required elements of an information security program and adds several new elements. Although the Commission believes the proposed approach is sufficiently flexible, it seeks comment on

whether it creates unintended consequences for businesses, may be more stringent than necessary to achieve the objective, and/or unnecessarily modifies the current rule without creating a material benefit to security.

Proposed paragraph (a)

Amended paragraph (a) would expand 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 financial institution's security program and enforcing its information security program.[77] This individual is referenced in the Rule as a Chief Information Security Officer or "CISO." This title is for clarity in the proposed Rule; financial institutions would not be required to actually grant that title to the designated individual. The proposed amendment would no longer allow financial institutions to designate more than one employee to coordinate the information security program. The Commission is interested in hearing about the potential costs and benefits of this proposal. In particular, the Commission is interested in any data, research or case studies that the Commission could use to analyze whether this is the best approach. This proposed change is intended to ensure that a single individual is accountable for overseeing the entire information security program and to lessen the possibility that there will be gaps in responsibility between individuals. The Commission believes that requiring a single responsible individual will increase accountability for the security of financial institutions' information systems.

[77] Proposed 16 CFR 314.4(a). This amendment is based on 23 NYCRR 500.04(a) and is functionally identical.

Under the proposed amendment, the CISO need not be an employee of the financial institution, but can be an employee of an affiliate or a service provider. This proposed change is meant to accommodate financial institutions that may prefer to retain an outside expert, lack the resources to employ their own information security staff qualified to oversee a program, or decide to pool resources with affiliates to share staff to manage information security. To the extent a financial institution meets this requirement by using a service provider or affiliate, however, the proposed amendment would require that the financial institution 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 CISO; and 3) require the service provider or affiliate to maintain an information security program that protects the financial institution in accordance with the Rule. These proposed amendments are designed to ensure that, even when the financial institution outsources the CISO function, the financial institution retains responsibility for its own information security.

Proposed paragraph (b)

The proposed amendments to paragraph (b) clarify that a financial institution must base its information security program on the findings of its risk assessment by changing the first sentence of existing paragraph (b) to read that financial institutions' "information security program shall be based on a risk assessment. . . ."[78] This is intended to emphasize this requirement, which is already required under the existing Rule.[79] In addition, the proposed amendment removes existing section 314.4(b)'s

[78] Proposed 16 CFR 314.4(b).
[79] 16 CFR 314.4(b).

requirement that the risk assessment must include consideration of specific risks[80] because these specific risks are set forth elsewhere in the proposed amendments.[81]

Proposed section 314.4(b)(1) would require that the risk assessments be written and based on criteria for evaluating the risks the institutions face based on their particular information systems and the customer information they hold.[82] In addition, revised paragraph (b)(1) would require that the risk assessment describe how the financial institution will mitigate or accept any identified risks and how the financial institution's information security program will address those risks.[83] The Commission is proposing these requirements in order to encourage financial institutions to perform thorough and complete risk assessments. The proposed amendment would allow financial institutions to develop their own criteria suited to their needs, but generally the criteria should address the sensitivity and value of customer information collected, maintained or transmitted by the financial institution and possible vectors through which the security, confidentiality, and integrity of that information could be threatened.

The proposed amendment to section 314.4(b) would also add a requirement that financial institutions "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

[80] 16 CFR 314.4(b)(1), (b)(2), and (b)(3).
[81] *See*, *e.g.*, Proposed 16 CFR 314.4(c)(2), (c)(10), and (e).
[82] Proposed 16 CFR 314.4(b)(1). This proposed amendment is based on 23 NYCRR 500.09(b). Proposed 16 CFR 314.4(b)(1) retains the requirement from the Cybersecurity Regulations that the risk assessment be written, but deviates from the Cybersecurity Regulations in that it does not require that the criteria for the risk assessment be written.
[83] Proposed 16 CFR 314.4(b)(1)(iii).

sufficiency of any safeguards in place to control these risks."[84] The Commission believes that 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 proposed amendment would not set forth a prescriptive schedule for the periodic risk assessment, but would require financial institutions to set their own schedule based on the needs and resources of their institution.

Proposed paragraph (c)

Proposed paragraph (c) retains the existing Rule's requirement for financial institutions to design and implement safeguards to control the risks identified in the risk assessment. It also adds more detailed requirements for what these safeguards must include. The Commission believes that most financial institutions already implement such measures as part of their comprehensive information security programs under the existing Rule. The proposed amendment simply makes these requirements explicit in order to clarify the Rule and ensure that financial institutions understand their obligations under the Rule.

Amended paragraph (c)(1) would require financial institutions to place access controls on information systems, designed to authenticate users and permit access only to authorized individuals in order to protect customer information from unauthorized acquisition.[85] The Commission views this as a fundamental requirement of all

[84] Proposed 16 CFR 314.4(b)(2).

[85] Proposed 16 CFR 314.4(c)(1). This proposed amendment is based primarily on the Model Law, Section 4(D)(2)(a), though it adds the Cybersecurity Regulations' requirement that such controls be periodically reviewed. 23 NYCRR 500.07. The proposed amendments use the Model Law, as opposed to the Cybersecurity Regulations, where, as here, the format is more easily integrated into the current Rule.

information security programs,[86] which certainly would have been a part of any program that met the requirements of the existing Rule.

Proposed paragraph (c)(2) would require financial institutions 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."[87] This requirement is designed to ensure that the financial institution inventories the data in its possession, inventories the systems on which that data is collected, stored or transmitted, and has a full understanding of the relevant portions of its information systems and their relative importance.[88] For example, it would require a company to understand which devices and networks contain customer information, who has access to them, and how those systems are connected to each other and to external networks.

Proposed paragraph (c)(3) would require that financial institutions restrict access to physical locations containing customer information only to authorized individuals.[89] This element would require financial institutions to protect physical locations, as opposed to networks, that contain customer information and is designed to address the threat to physical copies of records.[90] This would require financial institutions to protect paper

---

[86] *See, e.g.*, Complaint, *Uber Technologies, Inc.*, No. 152 3054 (October 26, 2018) (alleging that company failed to implement reasonable access controls).
[87] Proposed 16 CFR 314.4(c)(2). This proposed amendment is based on the Model Law, Section 4(D)(2)(b), and is functionally identical to it.
[88] *See, e.g.*, Complaint, *FTC v. Wyndham Worldwide Corp.*, No. CV 12-1365-PHX-PGR (D. Ariz. August 8, 2012) (alleging that company failed to provide reasonable security by, among other things, failing to inventory computers connected to its network).
[89] Proposed 16 CFR 314.4(c)(3). This proposed amendment is based on Model Law, Section 4(D)(2)(c) and is functionally identical to it.
[90] *See, e.g.*, Complaint, *FTC v. LifeLock, Inc.*, No. 2:10-cv-00530-MHM (D. Ariz. March 9, 2010) (alleging that company failed to provide reasonable security where it received customers' personal information by facsimile in an open and easily accessible area).

files and control access to areas in which such files are stored. This may include restricting access to work areas where personnel are using hard copies of customer information or requiring physical locks on filing cabinets containing customer information and similar protections. It would also include policies for securing physical devices that contain personal information, such as laptops, tablets, phones, and thumb drives.

Proposed paragraph (c)(4) would generally require financial institutions to encrypt all customer information, both in transit and at rest.[91] The Commission believes that in most circumstances encryption is an appropriate and important way to protect customer information from unauthorized use and access.[92] Recognizing that companies may need flexibility in certain unforeseen circumstances, the proposed amendment does, however, permit financial institutions to use alternative means to protect customer information, subject to review and approval by the CISO. This is similar to the approach taken by the Health Insurance Portability and Accountability Act Security Rule, which permits a covered entity to use an alternative to encryption if it determines that encryption is not reasonable and documents an equivalent alternative measure.[93] The Commission seeks comment on this approach.

Proposed paragraph (c)(5) would establish a requirement that financial institutions "[a]dopt secure development practices for in-house developed applications utilized" for

---

[91] Proposed 16 CFR 314.4(c)(4). This proposed amendment is based on both 23 NYCRR 500.15 and Model Law Section 4(D)(2)(d). It takes the general format from the Model Law but integrates the requirement that any alternative measures must be approved by the CISO from the Cybersecurity Regulations.
[92] *See, e.g.*, Complaint, *Uber Technologies, Inc.*, FTC No. 152 3054 (October 26, 2018) (alleging that company failed to provide reasonable security when it stored sensitive personal information in plain text rather than encrypting it).
[93] *See* 45 CFR 164.306(d)(3); *id.* 164.312(a)(2)(iv) (making encryption an addressable specification).

"transmitting, accessing, or storing customer information."[94] This proposed amendment is designed to ensure that financial institutions address the security of software they develop to handle customer information, as distinct from the security of their networks that contain customer information.[95] Financial institutions would be required to adopt practices designed to develop applications that do not subject customer information to unacceptable risk of unauthorized access. In addition, this amendment would require financial institutions to develop "procedures for evaluating, assessing, or testing the security of externally developed applications [they] utilize to transmit, access, or store customer information." This proposed provision is designed to ensure that financial institutions take steps to verify that applications they use to handle customer information are secure.[96] Under this amendment, financial institutions would be required to take reasonable steps to assure themselves that applications they use to handle customer information are secure and will not expose customer information.

Amended paragraph (c)(6) would require financial institutions to "implement multi-factor authentication for any individual accessing customer information" or "internal networks that contain customer information."[97] The Commission views multi-factor authentication as a minimum standard to allowing access to customer information

[94] Proposed 16 CFR 314.4(c)(5).
[95] *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).
[96] *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).
[97] Proposed 16 CFR 314.4(c)(6). This proposed amendment is based on 23 NYCRR 500.12, although it has been limited to requiring multifactor authentication only for accessing customer information.

for most financial institutions.[98] As discussed above, the Commission believes that the definition of multi-factor authentication is sufficiently flexible to allow most financial institutions to develop a system that is suited to their needs. Currently used forms of multifactor authentication, such as requiring both a password and the receipt of a one-time passcode on a registered device, would meet this proposed requirement. To the extent that a financial institution finds that a method other than multi-factor authentication offers reasonably equivalent or more secure access controls, the institution may adopt that method with the written permission of its CISO. The Commission seeks comment on this approach.

Amended paragraph (c)(7) would require information systems under the Rule to include audit trails designed to detect and respond to security events.[99] Audit trails are chronological logs that show who has accessed an information system and what activities the user engaged in during a given period.[100] The proposed Rule does not require any specific type of audit trail, nor does it require that every transaction be recorded in its entirety. However, the audit trail must be designed to allow the financial institution to detect when the system has been compromised or when an attempt to compromise has been made. It must also provide sufficient information for the financial institution to reasonably respond to the event. The proposed amendment does not require that the audit trails be retained for any particular period, but the Commission believes that in order to

---

[98] *See, e.g.*, Federal Financial Institutions Examinations Council, "Authentication in an Electronic Banking Environment," (August 8, 2001) ("In general, multi-factor authentication should be used on higher risk systems."); *see also* Complaint, *TaxSlayer*, FTC No. 1623063 (November 8, 2017) (alleging that company failed to provide reasonable security when it used single factor authentication).

[99] Proposed 16 CFR 314.4(c)(7). This proposed amendment is based on Model Law, Section 4(D)(2)(i), but removes the requirement that the audit trail be able to reconstruct material financial transactions. The proposed amendment requires only that the audit trail be designed to detect and respond to security events.

[100] *See* Computer Security Resource Center, Glossary, "Audit Trail," https://csrc.nist.gov/glossary/term/audit-trail.

allow the financial institution to detect and respond to security events, the audit trails will usually have to be maintained for some reasonable length of time. Financial institutions would need to determine the appropriate retention period for their operations. The Commission seeks comment on whether this requirement needs to be modified or eliminated for smaller firms, or narrowed to avoid undue burden.

Amended paragraph (c)(8) would require financial institutions to develop procedures for the secure disposal of customer information in any format that is no longer necessary for their business operations or other legitimate business purposes.[101] The proposed amendment allows the retention of information when retaining the information is required by law or where targeted disposal is not feasible due to the manner in which the information is maintained, such as when the information is on paper records that cannot be destroyed without also destroying other information which is still necessary for business operations. The disposal of records, both physical and digital, can result in exposure of customer information if not performed properly.[102] Similarly, if records are retained when they are no longer necessary, there is a risk that those records will be subject to unauthorized access. This amendment would require financial institutions to reduce both of those risks by designing procedures to dispose of records that are no longer necessary and to do so securely and in a timely manner. The proposed amendment does not define "legitimate business purposes," as the Commission feels that the wide

[101] Proposed 16 CFR 314.4(c)(8). This proposed amendment is based on Model Law, Section D(2)(k), but adds additional language from 23 NYCRR 500.13, which requires disposal of information that is no longer necessary for business operation or other legitimate business purposes, but provides an exception where disposal is not feasible.

[102] *See, e.g., 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).

array of business models of financial institutions under its jurisdiction defies any such attempt.

The Commission seeks comment on whether the Rule should define legitimate business purposes to exclude certain uses of customer information, require the destruction of certain types of data after a fixed period, or require financial institutions to affirmatively demonstrate a current need for customer information that is retained. The Commission also seeks comment on whether the proposed amendment should include a requirement to develop procedures to limit the collection of customer information that is not necessary for business operation or other legitimate business purposes.

Proposed paragraph (c)(9) would require financial institutions to adopt procedures for change management.[103] Change management procedures govern the addition, removal, or modification of elements of an information system.[104] Under the proposed amendment, financial institutions would need 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 acquired a new subsidiary and wished to combine the new subsidiary's network with its own would be required to assess the security of the new network and the effect of adding it to the existing network. Although the Commission believes the proposed approach is sufficiently balanced, it seeks comment on whether the proposal may be more stringent than necessary to achieve the objective, or unnecessarily modifies the current rule without creating a material benefit to security.

---

[103] Proposed 16 CFR 314.4(c)(9). This proposed amendment is unique to this proposal and is not based on the Cybersecurity Regulations or the Model Law.

[104] *See, e.g.*, Rutgers Information Security, Change Management, https://rusecure.rutgers.edu/content/change-management.

Proposed paragraph (c)(10) would require 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."[105] In addition to threats posed by outside actors, authorized users such as employees and contractors can pose a substantial risk to the security of customer information.[106] This amendment would require 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. The monitoring should allow financial institutions to identify inappropriate use of customer information by authorized users, such as transferring large amounts of data or accessing information for which the user has no legitimate use. This requirement is separate from the requirement to maintain "audit trails," which would require logging of unusual events.

Proposed paragraph (d)

Proposed paragraph (d)(1) would retain 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."[107] The Commission

[105] Proposed 16 CFR 314.4(c)(10). This proposed amendment is based on 23 NYCRR 500.14(a) and is functionally identical.
[106] *See, e.g.*, Complaint, *U.S. v. ChoicePoint Inc.*, No. 1:06-cv-00198-GET (N.D. Ga. January 30, 2006) (alleging that company failed to provide reasonable security when it failed to monitor the activities of authorized users).
[107] Proposed 16 CFR 314.4(d). This language is based on the current rule's requirement for regular testing, 16 CFR 314.4(c), but adds the requirement for either continuous monitoring or regular penetration testing and vulnerability assessments from 23 NYCRR 500.05.

views testing and monitoring as an integral part of any information security program.[108] Proposed paragraph (d)(2) provides further guidance noting that the monitoring should take the form of either "continuous monitoring" or "periodic penetration testing and vulnerability assessments." 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.[109] The Commission seeks comment on whether these required enhancements are appropriate, as well as information about the potential costs or unintended consequences of this proposal.

If a financial institution does not adopt effective continuous monitoring, under the proposed amendments it would be required to engage in periodic penetration testing and vulnerability assessment consisting of no less than annual penetration testing based on the financial institution's risk assessment and biannual vulnerability assessments designed to detect publicly known vulnerabilities.[110] These tests may be performed directly by the financial institution or by third-party assessors, as long as they are designed to assess the systems that contain or can be used to access customer information and are performed effectively. The schedule of this required testing aligns with the requirements of the Cybersecurity Regulations. The Commission seeks comment on whether this schedule of penetration testing and vulnerability assessment is appropriate or whether the Rule should require these tasks to be performed more or less frequently. In particular, the

[108] *See, e.g., U.S. v. VTech Electronics Limited*, No. 1:18-cv-00114 (N.D. Ill. Jan. 8, 2018) (alleging that company failed to provide reasonable information security when it failed to monitor its network and failed to perform vulnerability and penetration testing).
[109] Financial institutions that choose the option of continuous monitoring would also be satisfying 314.4(c)(10).
[110] Proposed 16 CFR 314.4(d)(1) and (2).

Commission is interested in any data, research or case studies that the Commission could use to analyze what commenters advocate.

Proposed paragraph (e)

Proposed paragraph (e) would require financial institutions to implement policies and procedures "to ensure that personnel are able to enact [the financial institution's] information security program" through various forms of training and education.[111] Training of employees is a critical part of information security, as employees will be the ones enforcing and implementing any information security program.[112] First, financial institutions would be required to provide their personnel with "security awareness training that is updated to reflect risks identified by the risk assessment."[113] This requirement would apply to all personnel that have the ability to handle, access, or dispose of customer information. The training would be designed to inform personnel of the risks to customer information and the financial institution's policies and procedures to minimize those risks.[114]

Second, financial institutions would be required to "[u]tiliz[e] qualified information security personnel," employed either by them or by affiliates or service providers, "to manage [their] information security risks and to perform or oversee the

---

[111] Proposed 16 CFR 314.4(e).

[112] *See, e.g.*, Complaint, *Lenovo*, FTC No. 152-3134 (January 2, 2018) (alleging that company failed to provide reasonable security by failing to provide adequate data security training for employees responsible for testing third-party software); Complaint, *HTC America Inc.*, FTC No. 122 3049 (July 2, 2013) (alleging that company failed to implement adequate privacy and security guidance or training for its engineering staff).

[113] Proposed 16 CFR 314.4(e)(1). This proposed amendment is based on 23 NYCRR 500.14(b) and is functionally identical.

[114] The Commission offers educational material on data security that can aid financial institutions in developing training materials for their employees. *See, e.g.*, FTC Business Center, Data Security, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security.

information security program."[115] This amendment is designed to ensure that information security personnel used by financial institutions are qualified for their positions and that sufficient personnel are used.

Third, financial institutions would be required to "[p]rovid[e] information security personnel with security updates and training sufficient to address relevant security risks."[116] Maintaining awareness of emerging threats and vulnerabilities is a critical aspect of information security that the Commission believes was already a part of any information security program that complies with the existing Safeguards Rule. This amendment formalizes the requirement that financial institutions provide information security personnel with ongoing training to stay abreast of such developments. It is separate from the requirement to train all personnel generally, reflected in paragraph (e)(1).

Fourth, financial institutions would be required to "[v]erify[ ] that key information security personnel take steps to maintain current knowledge of changing cybersecurity threats and countermeasures."[117] For example, a financial institution could offer incentives or funds for key personnel to undertake continuing education that addresses recent developments, include a requirement to stay abreast of security research as part of their performance metrics, or conduct an annual assessment of key personnel's knowledge of threats related to their information system. This requirement would be in addition to the proposed requirement that data security personnel be provided ongoing

[115] Proposed 16 CFR 314.4(e)(2). This proposed amendment is based on 23 NYCRR 500.10(a)(1) and is functionally identical.
[116] Proposed 16 CFR 314.4(e)(3). This proposed amendment is based on 23 NYCRR 500.10(a)(2) and is functionally identical.
[117] Proposed 16 CFR 314.4(e)(4). This proposed amendment is based on 23 NYCRR 500.10(a)(3) and is functionally identical.

training. The proposed amendment does not define "key personnel" as the Commission believes that which personnel are "key" will vary considerably from entity to entity and that each financial institution will need to determine which employees must maintain this knowledge based on their structure and risk assessments. In most cases, though, the Commission believes that at a minimum the CISO and senior cybersecurity personnel would be covered by this amendment. Although the Commission believes the proposed approach is sufficiently flexible, it seeks comment on whether these proposals create unintended consequences for businesses, may be more stringent than necessary to achieve the objective, and/or unnecessarily modifies the current rule without creating a material benefit to security. In particular, the Commission is interested in any data, research or case studies that the Commission could use to analyze what commenters advocate.

Proposed paragraph (f)

Proposed paragraph (f) would retain the current Rule's requirement in existing paragraph (d) regarding the oversight of service providers, and add a requirement that financial institutions periodically assess service providers "based on the risk they present and the continued adequacy of their safeguards."[118] The current Rule requires an assessment of service providers' safeguards only at the onboarding stage; the proposed addition is designed to require 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.[119] This ongoing oversight could

[118] Proposed 16 CFR 314.4(g).
[119] The proposed addition is based on a similar provision in the Cybersecurity Regulations. 23 NYCRR 500.11(a)(4).

include investigating red flags raised by service providers' practices or conducting periodic assessments of service provider practices, depending on the circumstances.

Proposed paragraph (g)

Proposed paragraph (g) would retain the language of existing paragraph (e) in the current Rule, which would continue to require 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.[120] While proposed paragraph (d) would amplify the testing required under the current Rule, the requirement to evaluate and adjust the program in light of such testing remains the same.

Proposed paragraph (h)

Proposed paragraph (h) would require financial institutions to establish incident response plans.[121] The written response plans would be required to be "designed to promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity, or availability of customer information" in the financial institution's possession. The amendment would require the incident response plans to address the following areas: 1) the goals of the incident response plan; 2) the internal processes for responding to a security event; 3) the definition of clear roles, responsibilities and levels of decision-making authority; 4) external and internal

[120] Proposed 16 CFR 314.4(g).

[121] Proposed 16 CFR 314.4(h). This proposed amendment is based on 23 NYCRR 500.16. The proposed amendment, however, requires the plan to address situations when customer information has been compromised, rather than a portion of the financial institution's information system. In addition, proposed section 314.4(h) does not require the incident response plan to address the continuing functionality of any aspect of the financial institution's business or operations, as continuity of operations is not relevant to Congress' mandate under the GLBA, which is to protect customer information.

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. The proposed incident response plan requirement focuses on preparing financial institutions to respond promptly and appropriately to security events and to mitigate any weaknesses in their information systems accordingly. It is not intended to create any independent reporting or notification requirements, nor to conflict with any such requirements to which financial institutions are already subject. The proposed requirement regarding "documentation and reporting regarding security events and related incident response activities" would require incident response plans to document any notification or reporting requirements imposed by other federal or state laws, but does not in itself impose any such requirement.

The Commission seeks comment on whether the proposed amendment should require that financial institutions report security events to the Commission. The Cybersecurity Regulations require covered entities to report security events to the superintendent of the Department of Financial Services, but the proposed rule does not have a similar provision. The Commission seeks comment on whether such a provision should be added and, if so, what the elements of such a provision should be. Specifically, the Commission seeks comment on 1) the appropriate deadline for reporting security events after discovery; 2) whether all security events should require notification or whether notification should be required only under certain circumstances, such as a determination of a likelihood of harm to customers or that the event affects a certain

number of customers; 3) whether such reports should be made public; 4) whether the events involving encrypted information should be included in the requirement; and 5) whether the requirement should allow law enforcement agencies to prevent or delay notification if notification would affect law-enforcement investigations.

In addition to seeking comment on the content of the plan, the Commission seeks comment on whether the proposed amendment would conflict with breach notification or reporting laws already in existence. Some states have enacted breach notification laws that exempt companies that maintain breach response procedures that are compliant with certain federal regulations from having to meet the requirements of the state's breach notification law. For example, Delaware's breach notification law states:

> A person that is regulated by state or federal law, including . . . the Gramm Leach Bliley Act . . . and that maintains procedures for a breach of security pursuant to the laws, rules, regulations, guidance, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with this chapter if the person notifies affected Delaware residents in accordance with the maintained procedures when a breach of security occurs.[122]

The Commission seeks comment on whether the introduction of the proposed requirement for an incident response plan would cause financial institutions to be exempt from this, or similar, state breach notification laws, and if so, how this should affect the Commission's decision about whether to require an incident response plan in the Rule.[123]

Proposed paragraph (i)

---

[122] Del. Code tit. 6, § 12B-103(b).

[123] The Commission is not proposing adding an independent breach notification to the Rule. A federal standard under GLB would be largely redundant because of state breach notification laws and because a requirement under the Rule would have limited effect, because the Commission cannot obtain civil penalties for violations of the Rule. The Commission, however, seeks comments on whether adding a breach notification requirement to the Rule would benefit consumers.

Proposed paragraph (i) would require 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 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.[124] For financial institutions that do not have a board of directors or equivalent, the CISO must make the report to a senior officer responsible for the financial institution's information security program. This amendment is designed 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, an annual written report may create accountability for the CISO by requiring the CISO to set forth the status of information security program for the governing body. The Commission requests comment on whether the burden of a required annual report would outweigh the benefits, whether the report should have other required components, or whether particular components are unnecessary.

In addition, the Commission requests comments on whether the proposed rule should also require the Board or equivalent governing body to certify compliance with the Rule. The Commission seeks comment on whether such a requirement would

[124] Proposed 16 CFR 314.4(i). This proposed amendment is based on 23 NYCRR 500.04(b), but borrows from the Model Law the requirements for the contents of the annual report. Model Law, Section E(2). The Commission believes the language from the Model Law is clearer and tied more directly to the requirements of the proposed amendments.

appropriately increase the engagement of the governing body of the financial institution in the information security program or whether it would create too much burden on financial institutions to independently assess the program.

The Commission also requests comment on how such a requirement would impact corporate governance; what precedents exist for federally-mandated board reporting on specific management issues, and analyses of their efficacy; and what effect requiring reporting to the board or certification by it would have.

Proposed amendments to section 314.5: Effective date

This proposed amendment replaces the existing effective date of the Rule. In its place, this amendment provides 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 are: 314.4(a), related to the appointment of a CISO; 314.4(b)(1), relating to conducting a written risk assessment; 314.4(c)(1)-(10), 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 CISO. The effective date of these elements would be delayed because financial institutions may need to take steps to bring their information security programs into compliance with these new requirements. All other requirements under the Safeguards Rule would remain in effect during this six-month period. The elements that would be required immediately upon publication are ones that are already required under the

current Rule, such as the requirement to have a written security program (314.3(a)); to conduct a risk assessment (314.4(b)); to design and implement safeguards to control the risks identified in the risk assessment (314.4(c)); to regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures (314.4(d)(1)); to oversee service providers at the onboarding stage (314.4(f)); and to evaluate and adjust the security program in light of the results of testing and monitoring (314.4(g)). These remaining requirements largely mirror the requirements of the existing Rule. The Commission requests comment on this approach.

Proposed section 314.6: Exceptions

Proposed section 314.6 is a new section that would exempt financial institutions that maintain relatively small amounts of customer information from certain requirements of the amended Safeguards Rule. The exceptions would apply to financial institutions that maintain customer information concerning fewer than five thousand consumers.[125] Such financial institutions would not be required to comply with the following subsections: 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. This proposed section is intended to reduce the burden on smaller financial institutions. The Commission believes that the paragraphs subject to this exemption are the ones that are most likely to cause undue burden on smaller financial institutions. For example, requiring continuous monitoring or a set schedule of testing might be too expensive, depending on the circumstances.

[125] Proposed 16 CFR 314.6.

The remaining sections of the amended Safeguards Rule would apply to these smaller financial institutions in the same way as other financial institutions. Exempted financial institutions would still need to conduct risk assessments (314.4(b)), design and implement a written information security program with the required elements (314.3 and 314.4(c)), utilize qualified information security personnel and train employees (314.4(e)), monitor activity of authorized users (314.4(c)(10)), oversee service providers (314.4(f)), and evaluate and adjust their information security program (314.4(g)). The Commission seeks comment on whether such exceptions are appropriate or whether all financial institutions should be required to comply with all of the proposed amendments. The Commission also seeks comment on whether the exempted paragraphs are appropriate. Finally, the Commission seeks comment on 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 is an appropriate number.

IV. Request for Comment

You can file a comment online or on paper. For the Commission to consider your comment, we must receive it on or before [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]. Write "Safeguards Rule, 16 CFR Part 314, Project No. 145407" on the comment. Your comment, including your name and your state, will be placed on the public record of this proceeding, including the https://www.regulations.gov website.

Postal mail addressed to the Commission is subject to delay due to heightened security screening. As a result, we encourage you to submit your comment online. To

make sure that the Commission considers your online comment, you must file it at https://www.regulations.gov by following the instructions on the web-based form.

If you file your comment on paper, write "Safeguards Rule, 16 CFR Part 314, Project No. P145407" on your comment and on the envelope, and mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue N.W., Suite CC-5610 (Annex B), Washington, D.C. 20580; or deliver your comment to the following address: Federal Trade Commission, Office of the Secretary, Constitution Center, 400 7th Street S.W., 5th Floor, Suite 5610 (Annex B), Washington, D.C. 20024. If possible, please submit your paper comment to the Commission by courier or overnight service.

Because your comment will be placed on the publicly accessible website, https://www.regulations.gov, you are solely responsible for making sure that your comment does not include any sensitive or confidential information. In particular, your comment should not include any sensitive personal information, such as your or anyone else's Social Security number, date of birth, driver's license number or other state identification number or foreign country equivalent, passport number, financial account number, or credit or debit card number. You are also solely responsible for making sure that your comment does not include any sensitive health information, such as medical records or other individually identifiable health information. In addition, your comment should not include any "trade secret or any commercial or financial information which . . . is privileged or confidential," as provided by section 6(f) of the FTC Act, 15 U.S.C. 46(f), and FTC Rule 4.10(a)(2), 16 CFR 4.10(a)(2), including in particular, competitively

sensitive information such as costs, sales statistics, inventories, formulas, patterns, devices, manufacturing processes, or customer names.

Comments containing material for which confidential treatment is requested must be filed in paper form, must be clearly labeled "Confidential," and must comply with FTC Rule 4.9(c). In particular, the written request for confidential treatment that accompanies the comment must include the factual and legal basis for the request, and must identify the specific portions of the comments to be withheld from the public record.[126] Your comment will be kept confidential only if the FTC General Counsel grants your request in accordance with the law and the public interest. Once your comment has been posted on the www.regulations.gov website, we cannot redact or remove your comment from the FTC website, unless you submit a confidentiality request that meets the requirements for such treatment under FTC Rule 4.9(c), and the General Counsel grants that request.

Visit the Commission website at https://www.ftc.gov to read this document and the news release describing it. The FTC Act and other laws that the Commission administers permit the collection of public comments to consider and use in this proceeding as appropriate. The Commission will consider all timely and responsive public comments that it receives on or before [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]. For information on the Commission's privacy policy, including routine uses permitted by the Privacy Act, see https://www.ftc.gov/site-information/privacy-policy.

[126] *See* 16 CFR 4.9(c).

IV. Communications by Outside Parties to the Commissioners or Their Advisors

Written communications and summaries or transcripts of oral communications respecting the merits of this proceeding, from any outside party to any Commissioner or Commissioner's advisor, will be placed on the public record.[127]

V. 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.[128] A "collection of information" occurs when ten or more persons are asked to report, provide, disclose, or record information in response to "identical questions."[129] Applying these standards, neither the Safeguards Rule nor the proposed amendments constitute a "collection of information."[130] 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

[127] *See* 16 CFR 1.26(b)(5).
[128] 44 U.S.C. 3502(3)(A)(i).
[129] *See* 44 U.S.C. 3502(3)(A).
[130] *See* 67 FR 36484, 36491 (May 23, 2002).

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 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 proposed amendments would not change this analysis because they would 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, the proposed amendment to section 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, the proposed amendment to section 314.4(h), which would require 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 CISOs to produce annual reports under proposed section 314.4(i) does not consist of answers to identical questions, as the content of these reports would vary considerably between financial institutions and CISOs are given flexibility in deciding what to include in the reports.

Finally, the proposed amendments that would modify 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 would not trigger the PRA's requirements.

VI. 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.[131] The Commission does not expect that this Rule, if adopted, would have the threshold impact on small entities. First, most of the burdens flow from the mandates of the Act, not from the specific provisions of the proposed Rule. Second, the proposed Rule imposes requirements that are scalable according to the size and complexity of each institution, the nature and scope of its activities, and the sensitivity of its information. Thus, the burden is likely to be less on small institutions, to the extent that their operations are smaller or less complex. In addition, smaller entities are exempted from many requirements of the proposed amendments. Nonetheless, the Commission has determined that it is appropriate to publish an Initial Regulatory Flexibility Analysis in order to inquire into the impact of the proposed Rule on small entities. The Commission invites comment on the burden on any small entities that would now be covered, but previously were not covered, if the definition of "financial institution" is modified as proposed, and the

[131] 5 U.S.C. 603 *et seq*.

burden on small entities created by the other proposed amendments. The Commission has prepared the following analysis.

1. Reasons for the Proposed Rule

The Commission proposes to make the rule clearer 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 Commission also proposes expanding 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 would harmonize the Rule with other agencies' rules and would require finders that collect consumers' sensitive financial information to comply with the Safeguards Rule's process-based approach to protect that data.

In addition, the Commission proposes to modify the Safeguards Rule to include more detailed requirements for the information security program required by the Rule. The Rule would continue to be process-based and flexible based on the financial institution's size and complexity. The Commission does propose to exempt smaller institutions from certain requirements that require additional written product and might pose a greater burden on smaller entities.

2. Statement of Objectives and Legal Basis

The objectives of the proposed Rule are discussed above. The legal basis for the proposed rule is section 501(b) of the GLBA.

3. Description of Small Entities to Which the Rule Will Apply

Determining a precise estimate of the number of small entities[132]—including newly covered entities under the modified definition of financial institution—is not readily feasible. Financial institutions already covered by the existing Rule 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 meaning of the Rule. If the proposed Rule is finalized, finders will also be covered. However, it is not known whether any finders are small entities, and if so, how many there are. The Commission requests 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.

4. Projected Reporting, Recordkeeping, and Other Compliance Requirements

The proposed Rule does not impose any reporting or any specific recordkeeping requirements within the meaning of the PRA, as discussed herein.

With regard to other compliance requirements, the proposed 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, if any. (The

[132] 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 $7.5 million or less. Consumer lending institutions (NAICS code 52291) are classified as small if their annual receipts are $38.5 million or less. Commercial banking and savings institutions (NAICS codes 522110 and 522120) are classified as small if their assets are $550 million or less. Assets are determined by averaging the assets reported on its four quarterly financial statements for the preceding year. The 2017 Table of Small Business Size Standards is available at https://www.sba.gov/sites/default/files/files/Size_Standards_Table_2017.pdf.

preceding section of this analysis discusses classes of covered financial institutions that may qualify as small entities.) The proposed addition of "finders" to the definition of financial institutions will impose the obligations of the Rule on entities that engage in "finding" activity and also collect customer information. The proposed addition of more detailed requirements may require some financial institutions to perform additional risk assessments, monitoring, or to create additional safeguards as set forth in the proposed rule. These obligations will require employees or third-party service providers with skills in information security, but the Commission believes that most financial institutions will have already complied with many parts of the proposed rule as part of their information security programs already 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 in the absence of supporting data, the Commission is unable to provide a complete or specific cost estimate. The Commission invites comment on the costs of the amended Rule for small entities to comply and to newly covered financial institutions (finders) of establishing and operating an information security program for such entities, to the extent, if any, they are small entities.

5. Identification of Duplicative, Overlapping, or Conflicting Federal Rules

As mentioned above, the Commission is proposing to incorporate the definition of "financial institution" and the accompanying examples from the Privacy Rule to the Safeguards Rule. This modification will have no substantive effect on the scope of the Rule or its enforcement. The change is designed only to increase the clarity of the Rule. The Commission believes that incorporating this definition will not cause any additional burden on covered entities. Separately, as also noted above, the Commission proposes to

revise the definition of "financial institution" to cover finders. The Commission is requesting comment on the extent to which other federal standards involving privacy or security or information may duplicate and/or satisfy or possibly conflict with the Rule's requirements for newly covered financial institutions.

The Commission is also proposing amending the Rule to include more detailed requirements for the written information security plan required by the Rule. The Commission does not believe that the proposed amendments would conflict with any existing data security regulations, such as the Health Insurance Portability and Accountability Act Security Rule.[133] The Commission is requesting comment on the extent to which other federal standards involving privacy or security or information may duplicate and/or satisfy or possibly conflict with the proposed amendments to the Rule.

6. Discussion of Significant Alternatives

The standards in the proposed 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 Commission is proposing to include certain design standards (e.g., a company must implement encryption, authentication, 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 the additional burden will be minimal, as most information security programs under the rule already meet most of these requirements. In addition, the proposed requirements are still designed to allow financial institutions flexibility in how

[133] 45 CFR Part 160; 45 CFR Part 164, Subparts A and C.

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 they are infeasible for a given financial institution.

In addition, the Proposed Rule exempts financial institutions that maintain relatively small amounts of customer information from certain requirements of the amended Safeguards Rule. The exceptions would apply to financial institutions that maintain customer information concerning fewer than five thousand consumers. The Commission believes that exempted financial institutions will generally be small entities. Such financial institutions would not be 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 CISO. These proposed exemptions are intended to reduce the burden on smaller financial institutions. The Commission believes that the obligations subject to this exemption 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 employee, 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 welcomes comment on any significant alternative consistent with the GLBA that would minimize the impact on small entities of these proposed

amendments, including institutions that would be newly covered under the amended definition of "financial institution."

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 proposes to amend 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 Section 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 section 314.2 to read as follows:

§ 314.2 Definitions.

(a) *In general*. Except as modified by this part or unless the context otherwise requires, the terms used in this part have the same meaning as set forth in the Commission's rule governing the Privacy of Consumer Financial Information, 16 CFR Part 313.

(b) *Authorized user* means 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.

(c) *Security event* means an event resulting in unauthorized access to, or disruption or misuse of, an information system or information stored on such information system.

(d) *Customer information* means any record containing nonpublic personal information, as defined in 16 CFR 313.3(n), 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) *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.

(f)(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, 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.

(g) *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.

(h) *Information system* means 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 controls systems.

(i) *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.

(j) *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.

(k) *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.

4. Revise section 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 section 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, "Chief Information Security Officer" or "CISO"). The CISO 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 CISO; 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:

(1) 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;

(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) Restrict access at physical locations containing customer information only to authorized individuals;

(4) 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 CISO;

(5) 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;

(6) Implement multi-factor authentication for any individual accessing customer information. Multi-factor authentication shall be utilized for any individual accessing your internal networks that contain customer information, unless your CISO has approved in writing the use of reasonably equivalent or more secure access controls;

(7) Include audit trails within the information security program designed to detect and respond to security events;

(8) Develop, implement, and maintain procedures for the secure disposal of customer information in any format that is no longer necessary for business operations or for other legitimate business purposes, except where such information is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained;

(9) Adopt procedures for change management; and

(10) Implement policies, procedures and controls designed to monitor 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) 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. Biannual 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.

(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 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 possession. 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 CISO to report in writing, 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 section 314.5 to read as follows:

§ 314.5 Effective date.

Sections 314.4(a), 314.4(b)(1), 314.4(c)(1)-(10), 314.4(d)(2), 314.4(e), 314.4(f)(3), 314.4(h), and 314.4(i) are effective as of [six months after publication of the final rule].

7. Add section 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, Commissioner Phillips and Commissioner Wilson dissenting.

April J. Tabor,
Acting Secretary