[Billing Code: 6750-01-P]

FEDERAL TRADE COMMISSION

16 CFR Part 314

RIN 3084-AB35

Standards for Safeguarding Customer Information

AGENCY: Federal Trade Commission.

ACTION: Final rule.

SUMMARY: The Federal Trade Commission ("FTC" or "Commission") is issuing a final rule ("Final Rule") to amend the Standards for Safeguarding Customer Information ("Safeguards Rule" or "Rule") to require financial institutions to report to the Commission any notification event where unencrypted customer information involving 500 or more consumers is acquired without authorization.

DATES: The amendments are effective [INSERT DATE 180 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*].

FOR FURTHER INFORMATION CONTACT: David Lincicum, 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.

SUPPLEMENTARY INFORMATION:

I. Background

Congress enacted the Gramm Leach Bliley Act ("GLBA") in 1999.[1] The GLBA provides a framework for regulating the privacy and data security practices of a broad range of financial institutions. Among other things, the GLBA requires financial

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

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 GLBA's directive, the Commission promulgated the Safeguards Rule in 2002.[3] The Safeguards Rule became effective on May 23, 2003.[4]

II. Regulatory Review of the Safeguards Rule

On April 4, 2019, the Commission issued a Notice of Proposed Rulemaking ("NPRM") setting forth proposed amendments to the Safeguards Rule.[5] In response, the Commission received 49 comments from various interested parties including industry groups, consumer groups, and individual consumers.[6] On July 13, 2020, the Commission held a workshop concerning the proposed changes and conducted panels with information security experts discussing subjects related to the proposed amendments.[7] The Commission received 11 comments following the workshop. After reviewing the initial comments to the NPRM, conducting the workshop, and then reviewing the

---

[2] *See* 15 U.S.C. 6801(b), 6805(b)(2).
[3] 67 FR 36483 (May 23, 2002).
[4] *Id.*
[5] 84 FR 13158 (Apr. 4, 2019).
[6] The 49 relevant public comments received on or after March 15, 2019, can be found at Regulations.gov. *See FTC Seeks Comment on Proposed Amendments to Safeguards and Privacy Rules, 16 CFR Part 314, Project No. P145407*, https://www.regulations.gov/docket/FTC-2019-0019/comments. The 11 relevant public comments relating to the subject matter of the July 13, 2020, workshop can be found at: https://www.regulations.gov/document/FTC-2020-0038-0001/comment. This notice cites comments using the last name of the individual submitter or the name of the organization, followed by the number based on the last two digits of the comment ID number.
[7] *See* FTC, *Information Security and Financial Institutions: FTC Workshop to Examine Safeguards Rule Tr.* (July 13, 2020), https://www.ftc.gov/system/files/documents/public_events/1567141/transcript-glb-safeguards-workshop-full.pdf.

comments received following the workshop, the Commission issued final amendments to the Safeguards Rule on December 9, 2021.[8]

In the NPRM, the Commission explained that its proposed amendments to the Safeguards Rule were based primarily on the cybersecurity regulations issued by the New York Department of Financial Services, 23 NYCRR 500 ("Cybersecurity Regulations").[9] The Commission also noted that the Cybersecurity Regulations require covered entities to report security events to the superintendent of the Department of Financial Services.[10] Relatedly, for many years, some other federal agencies enforcing the GLBA have required financial institutions to provide notice to the regulator, and in some instances notice to consumers as well.[11] Although the Commission did not include a similar reporting requirement in the NPRM, it did seek comment on whether the Safeguards Rule should be amended to require that financial institutions report security events to the Commission. Specifically, the Commission requested comments on whether such a requirement should be added and, if so, (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 events

[8] 86 FR 70272 (Dec. 9. 2021).
[9] 84 FR 13158, 13163 (Apr. 4, 2019).
[10] *Id*. at 13169.
[11] *See* Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 FR 15736, 15752 (Mar. 29, 2005) (originally issued by the Office of the Comptroller of the Currency; the Board of Governors of the Federal Reserve System; the Federal Deposit Insurance Corporation; and the Office of Thrift Supervision) ("At a minimum, an institution's response program should contain procedures for the following: … Notifying its primary Federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of *sensitive* customer information, as defined below; … [and notifying] customers when warranted"), https://www.occ.treas.gov/news-issuances/federal-register/2005/70fr15736.pdf (emphasis in original).

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.[12]

The final rule, which the Commission published in the *Federal Register* on December 9, 2021, did not include a reporting requirement.[13] However, on the same date, the Commission published a Supplemental Notice of Proposed Rulemaking ("SNPRM") in the *Federal Register*, which proposed further amending the Safeguards Rule to require financial institutions to report to the Commission certain security events as soon as possible, and no later than 30 days after discovery of the event.[14] Specifically, the Commission proposed to require financial institutions to notify the Commission electronically through a form located on the FTC's website about any security event that resulted or is reasonably likely to result in the misuse of customer information affecting at least 1,000 consumers. The Commission proposed that the notification include a limited set of information, consisting of (1) the name and contact information of the reporting financial institution, (2) a description of the types of information involved in the security event, (3) the date or the date range of the security event, if it can be determined, and (4) a general description of the security event. In response to the SNPRM, the Commission received 14 comments from various interested parties, including industry groups, consumer groups, and individual consumers.[15]

---

[12] *Id*.
[13] 86 FR 70272 (Dec. 9. 2021).
[14] *See* 86 FR 70062, 70067 (Dec. 9, 2021).
[15] The 14 relevant public comments received can be found at Regulations.gov. *See* FTC Seeks Comment on Proposed Amendments to Safeguards and Privacy Rules, 16 CFR Part 314, Project No. P145407, https://www.regulations.gov/docket/FTC-2021-0071/comments.

After reviewing the comments, the Commission now finalizes the proposed amendments with minor changes.

III. Overview of Final Rule

The Final Rule requires financial institutions to report notification events, defined as the unauthorized acquisition of unencrypted customer information, involving at least 500 customers to the Commission.[16] The notice to the Commission must include: (1) the name and contact information of the reporting financial institution; (2) a description of the types of information that were involved in the notification event; (3) if the information is possible to determine, the date or date range of the notification event; (4) the number of consumers affected; (5) a general description of the notification event; and, if applicable, whether any law enforcement official has provided the financial institution with a written determination that notifying the public of the breach would impede a criminal investigation or cause damage to national security, and a means for the Federal Trade Commission to contact the law enforcement official. The notice must be provided electronically through a form located on the FTC's website, https://www.ftc.gov.

IV. Detailed Analysis

The following section discusses the comments that the Commission received in response to the SNPRM.

General Comments

Several commenters generally supported the inclusion of a notification requirement in the Rule.[17] Some of these commenters pointed to frequent data breaches

---

[17] *See* Anonymous (Comment 2); Briggs (Comment 4); Clearing House Association L.L.C. ("Clearing House") (Comment 11); Anonymous (Comment 14); Securities Industry and Financial Markets Association

as an indication that companies' data security practices are inadequate and stated that requiring companies to provide notice to the Commission would enable the Commission to more easily enforce the Rule.[18] The Clearing House argued that the requirement is appropriate because it would place financial institutions covered by the Rule in the same position as banks, which are required to report data breaches to their prudential regulators.[19] The Electronic Privacy Information Center ("EPIC") suggested that the amendment would incentivize "use of strong data security measures by financial institutions, bring additional accountability and transparency to the handling of security events, and enhance the data security and privacy of all consumers."[20]

Other commenters opposed the proposal.[21] Many of these commenters argued that the proposed notification requirement would be duplicative of state breach notification laws and is, therefore, unnecessary.[22] The Commission, however, disagrees that requiring financial institutions to provide notice to the Commission is redundant because of state breach notification laws. State breach notification laws provide notice to consumers and in some cases also to state regulators, while the notice requirement of the Final Rule requires notice to the Commission and is designed to ensure that the Commission receives notice of security breaches affecting financial institutions under the

("SIFMA") and Bank Policy Institute ("BPI") ("SIFMA/BPI") (Comment 15) (supporting notification requirement for financial institutions that are not regulated by non-FTC financial agencies); American Council on Education (Comment 18) (supporting proposed notice requirement with revisions); Electronic Privacy Information Center ("EPIC") (Comment 19).

[18] *See, e.g.*, Anonymous (Comment 2); Briggs (Comment 4); The Clearing House (Comment 11) at 2 (describing breaches in the fintech industry).

[19] Clearing House (Comment 11) at 1-2.

[20] EPIC (Comment 19) at 2.

[21] *See* American Financial Services Association ("AFSA") (Comment 12); Consumer Data Industry Association ("CDIA") (Comment 13); American Escrow Association (Comment 16); CTIA (Comment 20); National Automobile Dealers Association ("NADA") (Comment 21); U.S. Chamber of Commerce (Comment 22).

[22] *See, e.g.*, AFSA (Comment 12) at 3; CDIA (Comment 13) at 2-3; CTIA (Comment 20) at 2-4; NADA (Comment 21) at 2-3; U.S. Chamber of Commerce (Comment 22) at 3.

Commission's jurisdiction. Notice to consumers or to state regulators does not achieve this purpose. Receipt of these notices will enable the Commission to monitor for emerging data security threats affecting financial institutions and to facilitate prompt investigative response to major security breaches. CTIA argued that the Commission could achieve this goal by accessing and reviewing regulated entities' reports to consumers and state authorities under state notification laws.[23] The Commission disagrees that this indirect method would be as efficient or effective as requiring regulated financial institutions to directly notify the Commission.[24] Such an approach would be extremely burdensome on the Commission and would require the diversion of resources from enforcement to search for and collect information about breaches involving regulated financial institutions. Also, as some of the commenters noted,[25] state laws vary in what types of incidents must be reported and to whom.[26] The Safeguards Rule notice requirement will establish a uniform reporting requirement for all regulated financial institutions, assisting the Commission in getting consistent information about notification events affecting those financial institutions regardless of which state's consumers are affected. This benefit is not offset by the cost to financial institutions

[23] CTIA (Comment 20) at 6-7.

[24] While some states that require notification to a state agency make companies' breach notifications public, *see, e.g.,* N.H. Dep't of Just., Off. of Attorney Gen., *Security Breach Notifications*, https://www.doj.nh.gov/consumer/security-breaches/, other states do not make notifications public, and as noted above, not all states require notice to a state government agency. Some non-governmental sources report breach notifications, but there is no guarantee that such sources are comprehensive as they depend in part on reporting by consumers who received a breach notification letter. Thus, the Commission could not obtain comprehensive data relating to breaches at regulated financial institutions by compiling reports of breaches from other sources.

[25] *See*, *e.g.*, Clearing House (Comment 11) at 8; CDIA (Comment 13) at 3; CTIA (Comment 20) at 4.

[26] *See*, *e.g.*, Tex. Bus. & Com. Code § 521.053(i) (requiring companies to notify Texas Attorney General if a breach affects at least 250 Texas residents); Va. Code Ann. 18.2-186.6(E) (requiring companies to notify Virginia Attorney General if a breach affects at least 1,000 Virginia residents); Fla. Stat. 501.171(3) (requiring businesses to notify the Florida Department of Legal Affairs if a breach affects at least 500 individuals in Florida).

because the burden on individual financial institutions is minimal, as the Final Rule does not require an extensive report and, in many instances, financial institutions will already be preparing notices to consumers and state agencies.

Some commenters argued that the notification requirement would not improve financial institutions' data security.[27] Other commenters disagreed with this assertion, arguing that the notification requirement would further incentivize financial institutions to protect customer information.[28] The Commission agrees with these commenters that the notification requirement will increase the efficiency and effectiveness of the Commission's enforcement of the Rule. As noted above, while state breach notification laws require notice to consumers, some states do not require that such notices be provided to state regulators as well, and not all state regulators that do receive such notices publish them. By requiring financial institutions to provide notice directly to the Commission, the Commission will not have to devote resources to continually search for breach notifications posted by other sources in order to know that a financial institution has experienced a breach. Without a notification, the Commission would have no guarantee that it has found all breaches in its searches. The required notices will enable the Commission to identify breaches that merit investigation more quickly and efficiently. Also, receiving notice of breaches will allow the Commission to develop better awareness of emerging risks to financial institutions' security. The Commission expects that these benefits will enable more efficient enforcement of the Rule, which will in turn increase financial institutions' incentive to comply. In addition, as discussed

[27] *See, e.g.,* AFSA (Comment 12) at 1; CDIA (Comment 13) at 2-3; American Escrow Association (Comment 16) at 2; CTIA (Comment 20) at 3-6; NADA (Comment 21) at 2-3; U.S. Chamber of Commerce (Comment 22) at 2-3.
[28] *See* EPIC (Comment 19) at 2, *see also* Anonymous (Comment 2); Briggs (Comment 4).

below, making the notices public will enable consumers to make more informed decisions about which financial institutions they choose to entrust with their information, providing financial institutions with an additional incentive to comply with the Rule.

The National Automobile Dealers Association ("NADA") argued that a requirement for financial institutions to report events in order to facilitate enforcement against them is "unprecedented"[29] and "raises serious questions," including "potential First Amendment and potentially even Fifth Amendment concerns."[30] The Commission disagrees. Far from being unique, the requirement to report security events to law enforcement agencies that might result in enforcement actions against the notifying company is common. Many federal agencies[31] require regulated entities to report data breaches to them, and most states require that companies report breaches to state attorneys general or other state law enforcement and have done so for years.[32]

NADA also argued that requiring reporting security events to assist the Commission to enforce the Safeguards Rule is inappropriate because not every breach is

[29] NADA argues that banking regulations are not relevant examples because they are designed "to protect depositors and to ensure the public interest in the safety and soundness of banks," rather than to facilitate enforcement. NADA (Comment 21) at 4-5, n.8. The banking regulations, however, are also designed to facilitate enforcement. In addition, the Safeguards Rule is also designed to protect customers of financial institutions and ensure the public interest in the safety of consumer's financial information.
[30] NADA (Comment 21) at 4-5, n. 9.
[31] *See, e.g.,* Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 FR 15736, 15752 (Mar. 29, 2005) (originally issued by the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of Thrift Supervision); 45 CFR 164.408 (requiring covered entities to report breaches affecting 500 or more individuals to the Secretary of Health and Human Services); 12 CFR 53.3 (requiring banking organizations to report security events to the Office of the Comptroller of the Currency); 12 CFR 225.302 (requiring Board-supervised banking organization to report certain breaches to the Board); 12 CFR 304.23 (requiring certain bank organizations to report breaches to the FDIC); *see also* 87 FR 16590 (Mar. 23, 2022) (proposed rule requiring companies to report security incidents to the SEC).
[32] *See*, *e.g.*, Tex. Bus. & Com. Code 521.053(i) (requiring companies to notify Texas Attorney General if a breach affects at least 250 Texas residents); Va. Code Ann. 18.2-186.6(E) (requiring companies to notify Virginia Attorney General if a breach affects at least 1000 Virginia residents); Fla. Stat. 501.171(3) (requiring businesses to notify the Florida Department of Legal Affairs if a breach affects at least 500 individuals in Florida).

the result of a failure to comply with the Safeguards Rule.[33] NADA suggested that the reporting requirement should only "apply after a series of security events," because only multiple events can be "suggestive of compliance failures," while any single breach "certainly . . . is not."[34] While the Commission acknowledges that not every notification event is necessarily the result of a failure to comply with the Safeguards Rule, it disagrees that a single breach cannot be "suggestive of compliance failures."[35] Indeed, the fact that an institution has not experienced a breach does not necessarily mean that the institution is in compliance with the Rule's requirements. The Commission believes that taking action to correct a potential Safeguards Rule violation before additional security events can harm consumers is appropriate and desirable. The American Financial Services Association ("AFSA") contended that "the FTC should clarify what factors in a report could lead to enforcement concerns," arguing that otherwise "institutions may seek to minimize all risks associated with a report."[36] The Commission does not believe that providing a guide to when a report could possibly lead to enforcement is either possible or desirable because the reports are unlikely to contain all of the information that the Commission would need to determine that law enforcement is appropriate or necessary. Such determinations are typically made following investigations that afford entities the opportunity to provide context and information.

In addition, the Commission notes that requiring a financial institution to report an event is not suggesting that every notification event is the result of a violation of the

[33] NADA (Comment 21) at 3-5.
[34] NADA (Comment 21) at 4.
[35] *See*, *e.g.*, *FTC v. Equifax*, 1:19-cv-03297-TWT (N.D. Ga., July 22, 2019), *available at* https://www.ftc.gov/legal-library/browse/cases-proceedings/172-3203-equifax-inc.
[36] AFSA (Comment 12) at 1.

Rule and will result in an enforcement action or even investigation. Rather, the reporting requirement will provide the Commission with valuable information about security threats to financial institutions and assist in the determination of whether any individual event should be investigated further. This will improve the Commission's ability to respond to data breaches and may enable the Commission to issue business and consumer education about emerging threats.

Other commenters argued that the reporting requirement would be unduly burdensome.[37] Some of these commenters suggested that because the Rule's requirement may differ from state notification laws' requirements, complying with the Rule will be burdensome.[38] Other commenters disagreed, noting that the information required is limited to basic information about the company and the notification event.[39] The Commission agrees with these commenters. The information required to be reported is minimal and is very similar to the information required by many state notification laws.[40] The company will have this information as the result of even a basic investigation of the security event, an investigation that would be required in any event to comply with the Rule and basic security practices. The fact that some state laws may be triggered under different circumstances and may require different information does not render this simple report burdensome.

---

[37] CDIA (Comment 13) at 2-3; SIFMA/BPI (Comment 15) at 8; ETA (Comment 17) at 2-3; CTIA (Comment 20) at 3-6; NADA (Comment 21) at 2-3; U.S. Chamber of Commerce (Comment 22).
[38] CDIA (Comment 13) at 2-3; CTIA (Comment 20) at 6; NADA (Comment 21) at 2-3.
[39] American Escrow Association (Comment 16) at 2; ACE (Comment 18) at 2, 7-8; EPIC (Comment 19) at 6-7.
[40] *See, e.g.,* Ala. Code 8-38-5(d); Ariz. Rev. Stat. 18-552(E); Cal. Civ. Code 1798.82(d); Fla. Stat. 501.171(3)(b); Mich. Comp. Laws 445.72(6); Mo. Rev. Stat. 407.1500(2)(4); N.H. Rev. Stat. Ann. 359-C:20(IV); N.Y. U.C.C. Law 899-AA(7); and Or. Rev. Stat. 646A.604(5).

In addition to addressing the proposed amendment in general, commenters also addressed specific elements of the proposed amendments. These comments are addressed in the following detailed discussion.

Triggering Event

The Commission adopts proposed § 314.4(j) as originally proposed, with minor changes. Proposed paragraph (j) would have required financial institutions that become aware of a security event to promptly determine the likelihood that customer information has been or will be misused. Under the provision as originally proposed, financial institutions would have been required to make a report to the Commission upon determining that, among other conditions, "misuse of customer information ha[d] occurred or . . . [was] reasonably likely [to occur]." However, upon consideration of the comments, Commission is clarifying the triggering language by adding a new paragraph (m) in § 314.2, which defines the term "notification event" as the "acquisition of . . . [unencrypted customer] information without the authorization of the individual to which the information pertains." Section 314.2(m) further clarifies that: (1) "[c]ustomer information is considered unencrypted . . . if the encryption key was accessed by an unauthorized person;" and (2) "[u]nauthorized acquisition will be presumed to include unauthorized access to unencrypted customer information unless you have reliable evidence showing that there has not been, or could not reasonably have been, unauthorized acquisition of such information."

Several commenters addressed whether becoming aware of a security event is an appropriate trigger for the notification process. In a joint comment, the Securities Industry and Financial Markets Association ("SIFMA") and the Bank Policy Institute

("BPI") argued that the notification process should not begin when a financial institution becomes aware of an event, but instead begin when the financial institution "determines" a security event has occurred. SIFMA and BPI suggested that "determination" takes place sometime after "discovery," and that financial institutions should have 30 days to notify the Commission after making this determination rather than after discovery. SIFMA and BPI argued that "determination" "connotes a higher standard of certainty than 'discovery,'" and would include determining whether any further requirements for notice, such as number of consumers affected, had been met. The Commission disagrees that 30 days after discovery of a notification event is insufficient time to determine whether the event meets the requirements for notification and to prepare the notice. The Commission expects that companies will be able to decide quickly whether a notification event has occurred by determining whether unencrypted customer information has been acquired and, if so, how many consumers are affected, so there will not be a significant difference between "determination" and "discovery."[41] In addition, the notification to the Commission requires minimal details and will not take significant time to prepare and, as discussed above, many states require reports containing similar information, so the financial institutions will need to prepare such a report in any event.

Other commenters argued that the term "security event" is too broad a term to act as a trigger for the notification process, stating that the term encompasses types of incidents that pose little risk of consumer harm and for which notification is unnecessary.[42] Some commenters felt that notification should be required only when

[41] As discussed below, the Final Rule no longer requires the financial institution to determine whether misuse had occurred or was likely.
[42] *See, e.g.*, SIFMA/BPI (Comment 15) at 8-9; CTIA (Comment 20) at 11-12; NADA (Comment 21) at 2-3.

harm to consumers has occurred or is likely to occur, rather than when "misuse" has occurred or is reasonably likely.[43] Some commenters argued that a trigger that requires consumer harm would be more in accord with state notification laws.[44] Similarly, several commenters argued that the notification requirement should exclude security events that involve only encrypted customer information, because there is little chance of consumer harm in such cases.[45] Others argued that requiring financial institutions to report breaches that do not involve possible harm to consumers would be unduly burdensome on financial institutions and would produce an overwhelming number of reports to the Commission.[46] Conversely, EPIC argued that notice should be required for all security events regardless of whether misuse had occurred or was likely.[47] EPIC argued that removing the analysis of whether misuse was likely would lower the burden of determining whether a report should be made and would prevent attempts by financial institutions to avoid reporting to the Commission.[48]

The Commission agrees with EPIC that the trigger for notification requires clarification. The meaning of the term "misuse" in the proposed rule was ambiguous. It was not clear if acquisition of customer information alone constituted misuse, or if other forms of misuse, such as alteration of data, would fall within the notification requirement. Given this ambiguity, financial institutions would have had difficulty evaluating the likelihood of misuse of customer information that has been acquired without

---

[43] *See* CDIA (Comment 13) at 4-5; SIFMA/BPI (Comment 15) at 9-10; American Escrow Association (Comment 16) at 2-3; ETA (Comment 17) at 2; CTIA (Comment 20) at 11-14.
[44] *See, e.g.,* CDIA (Comment 13) at 4-5.
[45] AFSA (Comment 12) at 2; CDIA (Comment 13) at 6; SIFMA/BPI (Comment 15) at 9; ACE (Comment 18); CTIA (Comment 20) at 12; NADA (Comment 21) at 3; U.S. Chamber of Commerce (Comment 22) at 4.
[46] SIFMA/BPI (Comment 15) at 9; ETA (Comment 17) at 2; CTIA (Comment 20) at 11.
[47] EPIC (Comment 19) at 4.
[48] *Id.*

authorization. At the same time, the ambiguity could have been used as an opportunity to circumvent the reporting requirement. Specifically, because the proposed rule required the financial institution to assess the likelihood of misuse, it would have allowed financial institutions to underestimate the likelihood of misuse, and, thereby, the need to report the security event.

Accordingly, the Final Rule requires notification where customer information has been acquired, rather than when misuse is considered likely. Specifically, the Commission is adding a new § 314.2(m) that defines the term "[n]otification event" to mean the acquisition of unencrypted customer information without the authorization of the individual to which the information pertains. Section 314.2(m) also provides that unauthorized access of information will be presumed to result in unauthorized acquisition unless the financial institution can show that there has not been, or could not reasonably have been, unauthorized acquisition of such information. This rebuttable presumption is consistent with the Health Breach Notification Rule. See 16 CFR 318.2(a) ("Unauthorized acquisition will be presumed to include unauthorized access to unsecured PHR identifiable health information unless the vendor of personal health records, PHR related entity, or third party service provider that experienced the breach has reliable evidence showing that there has not been, or could not reasonably have been, unauthorized acquisition of such information.").[49] Here, too, the presumption is

[49] *See also* 74 FR 42962, 42966 (Aug. 25, 2009). Examples of this rebuttable presumption cited in that rulemaking, and equally relevant here, included a circumstance where "an unauthorized employee inadvertently accesses an individual's PHR and logs off without reading, using, or disclosing anything. If the unauthorized employee read the data and/or shared it, however, he or she 'acquired' the information, thus triggering the notification obligation in the rule." Another example related to a lost laptop: "If an entity's employee loses a laptop in a public place, the information would be accessible to unauthorized persons, giving rise to a presumption that unauthorized acquisition has occurred. The entity can rebut this presumption by showing, for example, that the laptop was recovered, and that forensic analysis revealed that files were never opened, altered, transferred, or otherwise compromised." *Id.* at 42966.

"intended to address the difficulty of determining whether access to data (*i.e.*, the opportunity to view the data) did or did not lead to acquisition (*i.e.*, the actual viewing or reading of the data)."[50]

The Commission also agrees that notification should not be required when harm to consumers is rendered extremely unlikely because the customer information is encrypted. Accordingly, the Final Rule does not require notification if the customer information acquired is encrypted, so long as the encryption key was not accessed by an unauthorized person. *See* § 314.2(m). By requiring notice relating to unauthorized acquisition only of unencrypted customer information, this change brings the Rule into accord with the majority of state breach notification laws. If customer information was encrypted but the encryption key was also accessed without authorization, then the customer information will be considered to be unencrypted. Someone who has both the encrypted information and the encryption key can easily decrypt the information.[51]

In summary, the Final Rule requires notification in the event that the financial institution discovers that *unencrypted* customer information has been acquired without authorization. *See* § 314.2(m). Unlike under the proposed rule, notification is not conditioned on the assessment of likelihood of misuse. The Commission believes that determining whether acquisition has occurred simplifies the requirement and will enable financial institutions to more speedily determine whether a notification event has occurred. In addition, the Commission believes that this change will reduce the number of notifications by excluding events where encrypted information was acquired, while

---

[50] *Id*.

[51] *See, e.g.*, Ala. Code 8-38-2(6)(b)(2); Alaska Stat. 45.48.090(7); Colo. Rev. Stat. 6-1-716 (2)(a.4); 815 Ill. Comp. Stat. 530/5 ("Personal Information" definition); NY Gen. Bus. Law 899-aa(b); Tex. Bus. & Com. Code 521.053(a).

ensuring that it receives notice of events that are more likely to result in harm. As noted earlier, the Rule also includes a rebuttable presumption stating that when there is unauthorized access to data, unauthorized acquisition will be presumed unless the entity that experienced the breach "has reliable evidence showing that there has not been, or could not reasonably have been, unauthorized acquisition of such information." *See* § 314.2(m).

Some commenters argued that the notification requirement should trigger only when especially "sensitive" information is involved.[52] These commenters argue that requiring notification when any kind of customer information is involved would result in notifications when there is no risk of harm to consumers.[53] The Commission disagrees with this contention. The definition of "customer information" in the Rule does not encompass all information that a financial institution has about consumers. "Customer information" is defined as records containing "non-public personal information" about a customer.[54] "Non-public personal information" is, in turn, defined as "personally identifiable financial information," and excludes information that is publicly available or not "personally identifiable."[55] The Commission believes that security events that trigger the notification requirement—where customers' non-public personally identifiable, unencrypted financial information has been acquired without authorization—are serious and support the need for Commission notification.

[52] AFSA (Comment 12) at 2; CDIA (Comment 13) at 5-6; ETA (Comment 17) at 2; CTIA (Comment 20) at 11-12.
[53] AFSA (Comment 12) at 2; CDIA (Comment 13) at 5-6; ETA (Comment 17) at 2; CTIA (Comment 20) at 11-12.
[54] 16 CFR 314.2(d).
[55] 16 CFR 314.2(l).

In the SNPRM, the Commission asked whether, rather than having a stand-alone reporting requirement, the Rule should require reporting only when another state or federal statute, rule, or regulation requires a financial institution to provide notice of a security event or similar event to a governmental entity. Some commenters supported this suggestion, arguing that such a requirement would reduce duplicative notice and consumer confusion.[56] Other commenters opposed it, arguing that because of the varied nature of state notification laws, this would produce inconsistent reporting to the Commission.[57] The Commission agrees that a stand-alone requirement will help ensure that the Commission receives consistent information regarding security events.

Determination of Scope of Security Event

After a financial institution becomes aware of a security event, the proposed rule would have required it to determine whether at least 1,000 consumers have been affected or reasonably may be affected and, if so, to notify the Commission.

A number of commenters expressed views pertaining to the minimum threshold for the number of affected customers. Some commenters agreed that notification of security events should not be required if the number of consumers that could be affected fell below the proposed threshold (1,000 consumers).[58] The Clearing House, however,

[56] CTIA (Comment 20) at 9-10; NADA (Comment 21) at 7.
[57] Clearing House (Comment 11) at 9; ACE (Comment 18) at 7; EPIC (Comment 19) at 6-7.
[58] CDIA (Comment 13) (suggesting a requirement of notification when a security event affects at least 1,000 consumers and may cause substantial harm); American Escrow Association (Comment 16) at 2 (supporting 1,000 consumer requirement while suggesting other changes to the notice requirement); ACE (Comment 17) at 2 (stating that requiring notice when 1,000 consumers are affected would be appropriate, if notices were required only when there was a risk of substantial harm); EPIC (Comment 19) at 4 (suggesting that notice be required whenever an event involves the information of at least 1,000 consumers regardless of the likelihood of misuse).

suggested that notification should be required in all cases, regardless of the number of consumers potentially affected.[59]

AFSA suggested that there should be a higher threshold of affected consumers before notice is required.[60] AFSA argued that the thousand consumer threshold was too low because of "the large number of financial institutions with many more customers."[61] The Commission disagrees that the fact that some financial institutions hold the information of millions of consumers suggests that a higher threshold is appropriate. The Clearing House, conversely, argues that the Rule should require that the Commission receive notice whenever any consumer is affected, because otherwise consumers whose information was involved in smaller breaches would have no notice of the breach and would be "without the benefit of important notices" if financial institutions were not required to report breaches affecting fewer consumers.[62] The Commission does not agree that setting a minimum threshold of consumers affected before requiring notification would leave consumers involved in smaller breaches without notice, as consumers will typically receive direct notification under state breach notification laws, regardless of whether notice to the Commission is required. In determining the proper threshold, the Commission notes that numerous state laws require notification of breaches either with no minimum threshold, or with a threshold of 250 or 500 people. The

[59] Clearing House (Comment 11) at 4-5 (suggesting a requirement for notice for any security event involving sensitive customer information, regardless of the number of consumers potentially affected by the event).
[60] AFSA (Comment 12) at 2; *see also* Anonymous (Comment 2) (arguing that threshold should be proportional to the size of the financial information).
[61] *Id.*
[62] Clearing House (Comment 11) at 5. While the Rule requires direct notice of breaches only to the Commission, consumers affected by smaller breaches could learn of those breaches when the Commission makes the notices public. Also, the Rule does not limit state consumer notification laws that require direct notification of consumers.

Commission's own Health Breach Notification Rule, and the HIPAA Breach Notification Rule,[63] also require notification of breaches involving 500 or more people. The Commission concludes that a lower threshold than in the proposed rule is appropriate. Accordingly, the Commission is adopting a minimum threshold of 500 consumers, rather than the minimum threshold of 1,000 consumers that was in proposed § 314.4(j). The Commission believes that a security event that involves the acquisition of unencrypted customer information involving at least 500 consumers is significant enough to warrant notification of the Commission, regardless of the size of the financial institution.

Time to Report

The proposed Rule would have required Commission notification within 30 days from discovery of the notification event. Some commenters that addressed this deadline agreed that this would provide financial institutions sufficient time to make the required determinations and to notify the Commission.[64] Other commenters argued that financial institutions should be given significantly less time to notify the Commission.[65] Other commenters argued that financial institutions should be given more time to notify the Commission.[66] The Commission believes that a 30-day deadline properly balances the need for prompt notification with the need to allow financial institutions to investigate a security event, determine whether the information was acquired without authorization and how many consumers were affected, and learn enough about the event to make the

[63] 45 CFR §§ 164.400-.414.
[64] *See, e.g.*, CDIA (Comment 13) at 7; ACE (Comment 18) at 8; U.S. Chamber of Commerce (Comment 22) at 4.
[65] Anonymous (Comment 2) (suggesting a two-week deadline); Clearing House (Comment 11) at 6 (recommending a 36-hour deadline).
[66] *See* SIFMA/BPI (Comment 15) at 8 (arguing that 30 days should not begin until financial information has determined that security event meets notification requirements); CTIA (Comment 20) at 14 (same).

notification to the Commission meaningful. Accordingly, finalized § 314.2(j)(1) retains the 30-day deadline from the SNPRM.

Some commenters argued that financial institutions should be permitted to delay or withhold notification of a security event to the Commission at the request of a law-enforcement agency or if notification would interfere with a law enforcement investigation.[67] Alternatively, EPIC suggested that the Commission should not allow companies to delay reporting in cases of a law enforcement investigation, but should instead delay publication of the notice in cases where publication would interfere with an investigation.[68] The Commission agrees that, while notifications to the Commission should not be made public if law enforcement has requested a delay, there is no reason to delay notice to the Commission itself on that basis. This conclusion is consistent with the approach taken by the Securities and Exchange Commission and by other federal financial regulators in rulemakings that require notice of cyber incidents to a regulator, as opposed to notice directly to consumers.[69] Accordingly, § 314.4(j)(1)(vi) of the Final Rule provides that a financial institution's notice must (1) indicate whether any law enforcement official has provided the institution with a written determination that public disclosure of the breach would impede a criminal investigation or cause damage to

[67] *See* SIFMA/BPI (Comment 15) at 10; ACE (Comment 18) at 4-5; CTIA (Comment 20) at 15; U.S. Chamber of Commerce (Comment 22) at 5.
[68] EPIC (Comment 19) at 5-6.
[69] *See* Securities and Exchange Commission, *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, 88 FR 51896, 51898 (Aug. 8, 2023) (allowing delay of required disclosure of material cybersecurity incidents if the United States Attorney General determines that immediate disclosure would pose a substantial risk to national security or public safety and notifies the Commission of such determination in writing); Office of the Comptroller of the Currency, Federal Reserve System, Federal Deposit Insurance Corporation, *Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers*, 86 FR 66424 (Nov. 23, 2021) (adopting regulations that require banking organizations to notify their primary Federal Regulator of any "computer security incident" that rises to the level of a "notification incident," as soon as possible and no longer than 36 hours after the banking organization determines that a notification incident has occurred).

national security, and (2) provide a means for the Commission to contact the law enforcement official. In order that notice to the public is not delayed indefinitely, the provision also provides that a law enforcement official may request an initial delay of up to 30 days following the date when the disclosure is filed with the Commission. The delay may be extended for an additional period of up to 60 days if the law enforcement official seeks such an extension in writing. Additional delay may be permitted only if the Commission staff determines that public disclosure of a notification event continues to impede a criminal investigation or cause damage to national security.

The proposed § 314.4(j) did not address when a security event should be treated as discovered. The Commission believes that adding such a provision will clarify the rule and prevent confusion. Accordingly, under the Final Rule, a notification event shall be treated as discovered as of the first day on which such event is known. Financial institutions will be deemed to have knowledge of a notification event if the event is known to any person, other than the person committing the breach, who is the financial institution's employee, officer, or other agent. Therefore, in instances where an employee, officer, or other agent of the financial institution accesses customer information without authorization, a financial institution will be deemed to have knowledge of a notification event if the event is known to another employee, officer, or other agent of the financial institution.

Contents of Notice

The proposed Rule required that a notice be made electronically on a form on the FTC's website,[70] and that such notice must include the following information: (1) the name and contact information of the reporting financial institution; (2) a description of the types of information that were involved in the notification event; (3) if the information is possible to determine, the date or date range of the notification event; and (4) a general description of the notification event.

Several commenters supported these elements as an appropriate level of detail.[71] However, NADA was opposed to the requirement that the report include a description of the security event,[72] while EPIC suggested that the Rule should require a more detailed description of the security event.[73] EPIC argued that financial institutions should also be required to provide a comprehensive description of the types of information involved in the security event and a comprehensive description of the security event, because "it is critical that financial institutions provide a sufficiently detailed account of each security event to enable the FTC and affected consumers to assess whether and how personal information is at risk."[74] The Commission believes that, with the exception noted below, the proposed elements generally provide sufficient information to the Commission and the public without imposing undue burdens on reporting financial institutions. In the

[70] SIFMA/BPI argued that financial institutions should be allowed to notify the Commission by phone because that "could foster confidentiality." SIFMA/BPI (Comment 15) at 7. Similarly, the U.S. Chamber of Commerce suggested that financial institutions should be allowed to notify the Commission by alternative means, such as mail, "where covered entities may lack access to the internet." U.S. Chamber of Commerce (Comment 22) at 4. The Commission believes that notification should be limited to the form on the Commission's website, as this will ensure that all notifications are received and recorded in the same way. The Commission believes that it is not likely that a financial institution that has suffered a notification event will not be able to access the internet for the entirety of the 30-day reporting window.
[71] *See* AFSA (Comment 12) at 2; ACE (Comment 18) at 2; U.S. Chamber of Commerce (Comment 22) at 4.
[72] NADA (Comment 21) at 6.
[73] EPIC (Comment 19) at 3.
[74] *Id.*

event that the Commission determines that more information is needed, it will obtain that information from the financial institution. The Commission believes, however, that knowing the number of consumers affected or potentially affected by the notification event would allow it to better evaluate the impact of a particular event. Providing this information, which financial institutions will typically determine in the course of responding to a breach, will not significantly add to the burden to financial institutions. Accordingly, the Final Rule retains the proposed elements, while adding a requirement to provide the number of consumers affected or potentially affected by the notification event.[75]

Publication of Notices

The SNPRM requested public comment on whether submitted reports should be made public. Several commenters argued that making the reports public would benefit consumers by helping them to make informed decisions about which financial institutions to entrust with their financial information or to determine whether they might have been affected by a security event.[76] Other commenters argued that the reports should be confidential and not shared with the public.[77] Some commenters argued that making the reports public could encourage further cybersecurity attacks on affected financial institutions by making potential attackers aware of vulnerabilities that have not been

[75] As noted above, if applicable, financial institutions would also inform the Commission whether any law enforcement official has provided a written determination that notifying the public of the breach would impede a criminal investigation or cause damage to national security, and a means for the FTC to contact the law enforcement official.
[76] Briggs (Comment 4); Clearing House (Comment 11) at 10; EPIC (Comment 19) at 5-6.
[77] AFSA (Comment 12) at 2-3; CDIA (Comment 13) at 7; SIFMA/BPI (Comment 15) at 5-7; ACE (Comment 18) at 5-7; CTIA (Comment 20) at 15-16; NADA (Comment 21) at 5-6; U.S. Chamber of Commerce (Comment 22) at 5.

remedied by the time the notice is made public.[78] NADA argued that the description of the event in particular should not be made public, suggesting that the description provided no benefit to consumers and would not improve data security.[79] The Commission disagrees that making the reports public will increase risk to financial institutions' data security. As discussed above, most financial institutions are already subject to state breach notification laws, many of which require notification to a state agency that then makes the notification public. In addition, the general nature of the information required to be included in the report is unlikely to provide potential attackers any advantage in comprising the financial institution's security.

Other commenters argued that publication of the notices could create undue media coverage and that the information would be too general to assist consumers in making informed decisions.[80] Similarly, CDIA argued that because state law requires direct consumer notification to those affected by the breach, making the information public to all consumers would cause "consumer confusion and angst about whether the consumer's information has been compromised."[81] CTIA also argued that financial institutions that have suffered a security event should not be subject to the punishment of "name and shame."[82] SIFMA and BPI suggested that making the reports public would limit the information financial institutions are willing to share in the reports in order to avoid public revelation of the details of the breach.[83]

---

[78] SIFMA/BPI (Comment 15) at 7; ACE (Comment 18) at 5-7; CTIA (Comment 20) at 15-16; NADA (Comment 21) at 6.
[79] NADA (Comment 21) at 6.
[80] AFSA (Comment 12) at 2-3; NADA (Comment 21) at 5.
[81] CDIA (Comment 13) at 7; *see also* SIFMA/BPI (Comment 15) at 6 (suggesting that publication of the reports could cause confusion for consumers and investors); ACE (Comment 18) at 5-7.
[82] CTIA (Comment 20) at 16.
[83] SIFMA/BPI (Comment 15) at 6.

As discussed above, the Commission acknowledges that not all security events at financial institutions are the result of a failure to comply with the Safeguards Rule. Nevertheless, the Commission believes that providing more information to consumers about these events will both benefit consumers and incentivize companies to better protect that information. The Commission is not persuaded that attention given to breaches is "undue" or otherwise inappropriate, as suggested by some commenters. Apart from providing actionable information for individuals who are directly affected, reporting provides a broader value to the general public to consider proactive measures, such as implementing a credit freeze, prioritizing methods to secure their own data, and determining where to do business. The Commission does not believe that a confidential reporting system is needed in order to incentivize more comprehensive reporting by financial institutions. The general level of detail required to be reported under § 314.4(j)(1) will not compromise a financial institution's security posture going forward—the report requires only the most general information, and cannot provide a meaningful roadmap for attackers. Accordingly, the Commission intends to enter notification event reports into a publicly available database.

The SNPRM also asked for comment on whether the Commission should require financial institutions that suffer a security event to directly notify affected consumers, as well as the Commission. Some commenters were in favor of requiring consumer notification, at least when notification of the Commission was required.[84] Most commenters who addressed the issue, however, opposed such a requirement, pointing to the existing regime of state consumer notification laws and arguing that a separate FTC

[84] Clearing House (Comment 11) at 8-9; EPIC (Comment 19); *see also* Anonymous (Comment 14) (stating that if there is a data breach, consumers "need to know what happened to their information."

notification requirement would be duplicative and unduly burdensome.[85] The Commission agrees that, because all states have some form of consumer notification requirement, a direct consumer notification requirement in the Safeguards Rule would be largely duplicative of those state laws. Therefore, the Commission has not included such a requirement in the Final Rule.

Finally, the Commission is revising § 314.4(c) to correct a typographical error. As originally promulgated, that section required a financial institution to "[d]esign and implement safeguards to control the risks you identity through risk assessment…." Actually, a financial institution must "[d]esign and implement safeguards to control the risks you identify through risk assessment…." In the Final Rule, this error is corrected.

Section 314.5: Effective Date

The proposed rule revised § 314.5 so that the reporting requirement in § 314.4(j) would not go into effect until six months after the publication of a final rule. As proposed, finalized § 314.5 provides that § 314.4(j) will become effective on [INSERT DATE 180 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*].

V. Paperwork Reduction Act

The Paperwork Reduction Act ("PRA"), 44 U.S.C. 3501 *et seq.*, requires federal agencies to obtain Office of Management and Budget ("OMB") approval before undertaking a collection of information directed to ten or more persons. Pursuant to the regulations implementing the PRA (5 CFR 1320.8(b)(3)(vi)), an agency may not collect

[85] *See* AFSA (Comment 12) at 3; CDIA (Comment 13) at 8; SIFMA/BPI (Comment 15) at 10; CTIA (Comment 20) at 16-17; NADA (Comment 21) at 7; *see also* American Council on Education (Comment 18) at 8 (stating that the Commission should engage with covered financial institutions about existing notification requirements before establishing a consumer notification requirement).

or sponsor the collection of information, nor may it impose an information collection requirement, unless it displays a currently valid OMB control number.

The amendment requiring financial institutions to report certain security events to the Commission discussed above constitutes a "collection of information" for purposes of the PRA.[86] As required by the PRA, the FTC submitted the proposed information collection requirement to OMB for its review at the time of the publication of the SNPRM. OMB directed the Commission to resubmit the requirement at the time the Final Rule is published. Accordingly, FTC staff has estimated the information collection burden for this requirement as set forth below.

The amendment will affect only those financial institutions that suffer a security event in which unencrypted customer information affecting at least 500 consumers is acquired without authorization. Although the SNPRM proposed a 1,000-consumer cut-off for notification, the Commission believes that the reducing the reporting threshold by 500 consumers will likely make only a small difference in the number of breaches reported.[87] Assuming that reducing the reporting threshold by 500 individuals will lead an additional 5% of financial institutions to report—a generous estimate—FTC staff estimates that the reporting requirement will affect approximately 115 financial institutions each year.[88] FTC staff anticipates that the burden associated with the

[86] 44 U.S.C. 3502(3)(A)(i).

[87] According to the Identity Theft Resource Center, 108 entities in the "Banking/Credit/Financial" category suffered data breaches in 2019, which affected more than 100 million consumers. 2019 End-of-Year Data Breach Report, Identity Theft Resource Center at 2, available at https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf. On average, each breach would have involved more than 930,000 consumers, far over both the 500 and the 1,000 consumer thresholds.

[88] According to the Identity Theft Resource Center, 108 entities in the "Banking/Credit/Financial" category suffered data breaches in 2019. *2019 End-of-Year Data Breach Report*, Identity Theft Resource Center at 2, *available at* https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-

reporting requirement will consist of the time necessary to compile the requested information and report it via the electronic form located on the Commission's website. FTC staff estimates that this will require approximately five hours for affected financial institutions, for a total annual burden of approximately **575 hours** (115 responses × 5 hours).

The Commission does not believe that the reporting requirement would impose any new investigative costs on financial institutions. The information about notification events required by the reporting requirement is information the Commission believes financial institutions would acquire in the normal course of responding to a notification event. In addition, in many cases, the information requested by the reporting requirement is similar to information entities are required to disclose under various states' data breach notification laws.[89] As a result, FTC staff estimates that the additional costs imposed by the reporting requirement will be limited to the administrative costs of compiling the requested information and reporting it to the Commission on an electronic form located on the Commission's website.

FTC staff derives the associated labor cost by calculating the hourly wages necessary to prepare the required reports. FTC staff anticipates that required information will be compiled by information security analysts in the course of assessing and responding to a notification event, resulting in 3 hours of labor at a mean hourly wage of

---

Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf. Although this number may exclude some entities that are covered by the Safeguards Rule but are not contained in the "Banking/Credit/Financial" category, not every security event will trigger the reporting obligations (*e.g.*, breaches affecting less than 500 people). Therefore, Commission staff estimated in the SNPRM that 110 institutions would have reportable events. Because of the change in the reporting threshold the Commission expects an additional 5 entities to have reporting obligations.

[89] *See, e.g.,* Cal. Civil Code 1798.82; Tex. Bus. & Com. Code 521.053; Fla. Stat. 501.171.

$57.63 (3 hours × $57.63 = $172.89).[90] FTC staff also anticipates that affected financial institutions may use attorneys to formulate and submit the required report, resulting in 2 hours of labor at a mean hourly wage of $78.74 (2 hours × $78.74 = $157.48).[91] Accordingly, FTC staff estimates the approximate labor cost to be $330 per report (rounded to the nearest dollar). This yields a total annual cost burden of $37,950 (115 annual responses × $330).

The Commission is providing an online reporting form on the Commission's website to facilitate reporting of qualifying notification events. As a result, the Commission does not anticipate that covered financial institutions will incur any new capital or non-labor costs in complying with the reporting requirement.

Pursuant to Section 3506(c)(2)(A) of the PRA, the FTC invited comments on: (1) whether the disclosure requirements are necessary, including whether the information will be practically useful; (2) the accuracy of our burden estimates, including whether the methodology and assumptions used are valid; (3) ways to enhance the quality, utility, and clarity of the information to be collected; and (4) ways to minimize the burden of providing the required information to the Commission. Although the Commission received several comments that argued that the required notifications would be burdensome for businesses, none addressed the accuracy of the Commission's burden

[90] This figure is derived from the mean hourly wage for Information security analysts. See "Occupational Employment and Wages–May 2022," Bureau of Labor Statistics, U.S. Department of Labor (April 5, 2023), Table 1 ("National employment and wage data from the Occupational Employment Statistics survey by occupation, May 2023"), *available at* https://www.bls.gov/news.release/pdf/ocwage.pdf.
[91] This figure is derived from the mean hourly wage for Lawyers. See "Occupational Employment and Wages–May 2019," Bureau of Labor Statistics, U.S. Department of Labor (March 31, 2020), Table 1 ("National employment and wage data from the Occupational Employment Statistics survey by occupation, May 2019"), *available at* https://www.bls.gov/news.release/pdf/ocwage.pdf.

estimate.[92] Other commenters argued that the reporting requirement would create little burden.[93] For the reasons discussed above, the Commission agrees with these commenters and does not believe that reporting requirement will create a significant burden for businesses.

VIII. Regulatory Flexibility Act

The Regulatory Flexibility Act ("RFA")[94] requires that the Commission provide an Initial Regulatory Flexibility Analysis ("IRFA") with a proposed rule, and a Final Regulatory Flexibility Analysis ("FRFA") with the final rule, unless the Commission certifies that the Rule will not have a significant economic impact on a substantial number of small entities.[95] As discussed in the IRFA, the Commission does not believe that this amendment to the Safeguards Rule has the threshold impact on small entities. The reporting requirement will apply to financial institutions that, in most cases, already have an obligation to disclose similar information under certain federal and state laws and regulations and will not require additional investigation or preparation.

In this Notice, the Commission adopts the amendments proposed in its SNPRM with only minimal modifications. In its IRFA, the Commission determined that the proposed rule would not have a significant impact on small entities because of the minimal information being requested. Although the Commission certifies under the RFA that the rule will not have a significant impact on a substantial number of small entities, and hereby provides notice of that certification to the Small Business Administration, the

[92] CDIA (Comment 13) at 2-3; SIFMA/BPI (Comment 15) at 8; ETA (Comment 17) at 2-3; CTIA (Comment 20) at 3-6; NADA (Comment 21) at 2-3; U.S. Chamber of Commerce (Comment 22).
[93] American Escrow Association (Comment 16) at 2; ACE (Comment 18) at 2, 7-8; EPIC (Comment 19) at 6-7.
[94] 5 U.S.C. 601–612.
[95] 5 U.S.C. 603–605.

Commission nonetheless has determined that publishing a FRFA is appropriate to ensure that the impact of the rule is fully addressed. Therefore, the Commission has prepared the following analysis:

1. Need for and Objectives of the Final Rule

The need for and the objective of the Final Rule is to ensure that the Commission is aware of notification events that could suggest a financial institution's security program does not comply with the Rule's requirements, thus facilitating Commission enforcement of the Rule. To the extent the reported information is made public, the information will also assist consumers by providing information as to notification events experienced by various financial institutions.

2. Significant Issues Raised in Public Comments in Response to the IRFA

Although the Commission received several comments that argued that the required notifications would be burdensome for businesses,[96] none argued specifically that smaller businesses in particular would be subject to special burden. Other commenters argued that the reporting requirement would create little burden.[97] One commenter specifically argued that the requirement would not create significant burden for small businesses.[98] As discussed above, the Commission does not anticipate that covered financial institutions will incur any new capital or non-labor costs in complying with the reporting requirement. Additionally, the average annual labor costs per covered financial institution are de minimis because most entities, including small entities, will only

[96] CDIA (Comment 13) at 2-3; SIFMA/BPI (Comment 15) at 8; ETA (Comment 17) at 2-3; CTIA (Comment 20) at 3-6; NADA (Comment 21) at 2-3; U.S. Chamber of Commerce (Comment 22).
[97] American Escrow Association (Comment 16) at 2; ACE (Comment 18) at 2, 7-8; EPIC (Comment 19) at 6-7.
[98] American Escrow Association (Comment 16) at 2 (stating that the reporting requirement "does not appear to be onerous as a reporting matter and we also agree with the FTC's conclusion that there would not be a significant impact on small business").

infrequently be required to file a report. Thus, the Commission does not believe that the reporting requirement will create a significant burden for financial institutions in general, including small businesses.

The Commission did not receive any comments filed by the Chief Counsel for Advocacy of the Small Business Administration ("SBA").

3. Description and an Estimate of the Number of Small Entities to Which the Final Rule Will Apply, or Explanation Why No Estimate Is Available

As explained in the IRFA, determining a precise estimate of the number of small entities[99] that would have to report a notification event in a given year is not readily feasible. No commenters addressed this issue. Both small entities and larger ones experience security incidents involving disclosure of consumer information.[100] However, other factors complicate the analysis. There are no estimates available reflecting the percentage of financial institutions under the Commission's jurisdiction that would be considered small entities, and small entities may be more likely to experience notification events that fall below the notification threshold, for example. Such factors are not reflected in industry and economic sector data, and, therefore, it is not possible to

[99] 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 $15 million or less. Consumer lending institutions (NAICS code 52291) are classified as small if their annual receipts are $47 million or less. Commercial banking and savings institutions (NAICS codes 522110 and 522120) are classified as small if their assets are $850 million or less. Assets are determined by averaging the assets reported on businesses' four quarterly financial statements for the preceding year. The 2023 Table of Small Business Size Standards is available at https://www.sba.gov/document/support--table-size-standards.

[100] *See, e.g.,* 2023 Verizon Data Breach Investigations Report at 65, available at https://www.verizon.com/business/resources/reports/dbir/ (reporting cybersecurity incidents and confirmed data disclosures for companies with fewer than or more than 1000 employees).

estimate the number of small entities covered by the Rule from such data. Projecting from entities' past experiences of actual breaches, however, as discussed in the section discussing the PRA, FTC staff estimates that the Rule's reporting requirement would affect approximately 115 entities per year in the future. Accordingly, even if every financial institution required to report in a given year were a small entity, the reporting requirement would affect only approximately 115 such entities. Regardless, as discussed above, these amendments will not add any significant additional burdens on any covered small businesses.

4. Projected Reporting, Recordkeeping, and Other Compliance Requirements

The notification requirement imposes reporting requirements. As outlined above, the amendment will affect only those financial institutions that suffer a notification event in which unencrypted customer information affecting at least 500 consumers is acquired without authorization. If such an event occurs, the affected financial institution may expend costs to provide the Commission with the information required by the reporting requirement. As noted in the PRA analysis above, the total estimated annual cost burden for all entities subject to the reporting requirement will be approximately $37,950.

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

The Commission did not propose any specific small entity exemption or other significant alternatives because the burden imposed upon small businesses is minimal. In drafting the reporting requirement, the Commission has made every effort to avoid unduly burdensome requirements for entities. The reporting requirement only mandates

that affected financial institutions provide the Commission with information necessary to assist it in its regulatory and enforcement efforts. The rule minimizes burden on all covered financial institutions, including small businesses, by providing for reporting through an online form on the Commission's website. In addition, the rule requires that only notification events involving at least 500 consumers must be reported, which will reduce potential burden on small businesses that retain information on fewer consumers. Therefore, the Commission does not believe that any alternatives for small entities are required or appropriate.

IX. Other Matters

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

List of Subjects in 16 CFR Part 314

Consumer protection, Computer technology, Credit, Privacy, Trade practices.

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

PART 314—STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

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

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

2. In § 314.2:

a. Redesignate paragraphs (m) through (r) as paragraphs (n) through (s), respectively; and

b. Add a new paragraph (m).

The addition reads as follows:

§ 314.2 Definitions

* * * * *

(m) ***Notification Event*** means acquisition of unencrypted customer information without the authorization of the individual to which the information pertains. Customer information is considered unencrypted for this purpose if the encryption key was accessed by an unauthorized person. Unauthorized acquisition will be presumed to include unauthorized access to unencrypted customer information unless you have reliable evidence showing that there has not been, or could not reasonably have been, unauthorized acquisition of such information.

* * * * *

3. In § 314.4, revise the introductory text of paragraph (c) and add a new paragraph (j). The revision and addition read as follows:

§ 314.4 Elements.

* * * * *

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

* * * * *

(j) Notify the Federal Trade Commission about notification events in accordance with paragraphs (j)(1) - (2) of this section.

(1) *Notification requirement.* Upon discovery of a notification event as described in paragraph (j)(2) of this section, if the notification event involves the information of at least 500 consumers, you must notify the Federal Trade Commission as soon as possible, and no later than 30 days after discovery of the event. The notice shall

be made electronically on a form to be located on the FTC's website, https://www.ftc.gov. The notice shall include the following:

(i) the name and contact information of the reporting financial institution;

(ii) a description of the types of information that were involved in the notification event;

(iii) if the information is possible to determine, the date or date range of the notification event;

(iv) the number of consumers affected or potentially affected by the notification event;

(v) a general description of the notification event; and

(vi) whether any law enforcement official has provided you with a written determination that notifying the public of the breach would impede a criminal investigation or cause damage to national security, and a means for the Federal Trade Commission to contact the law enforcement official. A law enforcement official may request an initial delay of up to 30 days following the date when notice was provided to the Federal Trade Commission. The delay may be extended for an additional period of up to 60 days if the law enforcement official seeks such an extension in writing. Additional delay may be permitted only if the Commission staff determines that public disclosure of a security event continues to impede a criminal investigation or cause damage to national security.

(2) *Notification event treated as discovered.* A notification event shall be treated as discovered as of the first day on which such event is known to you. You shall

be deemed to have knowledge of a notification event if such event is known to any person, other than the person committing the breach, who is your employee, officer, or other agent.

4. Revise § 314.5 to read as follows:

§ 314.5 Effective date.

Section 314.4(j) is effective as of [INSERT DATE 180 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*].

By direction of the Commission.

April J. Tabor

Secretary