**Federal Trade Commission**

**Supporting Statement for Standards for Safeguarding Customer Information**
**16 CFR Part 314**

**OMB Control No. 3084-0171**

The Federal Trade Commission ("FTC" or "Commission") is finalizing proposed amendments to its Standards for Safeguarding Customer Information ("Safeguards Rule"), 16 CFR part 314, which require financial institutions to report to the Commission a notification event where unencrypted customer information involving 500 or more consumers is acquired without authorization.

As part of this rulemaking, the Commission issued a Notice of Proposed Rulemaking ("NPRM") in 2019,[1] as well as a Supplemental Notice of Proposed Rulemaking ("SNPRM") in 2021.[2] Upon publication of the SNPRM, the Commission previously submitted an associated clearance request with Supporting Statement to OMB. In response, OMB filed a comment on February 4, 2022, requesting that the Commission resubmit the clearance request upon finalizing the proposed rule.

## (1) Necessity for Collecting the Information

In 1999, Congress enacted the Gramm Leach Bliley Act, Pub. L. 106–102, 113 Stat. 1338 (1999) ("GLBA"), which provides a framework for regulating the privacy and data security practices of a broad range of financial institutions. Among other things, the GLBA requires financial institutions to provide customers with information about the institutions' privacy practices and about their opt-out rights, and to implement security safeguards for customer information.

Subtitle A of Title V of the GLBA requires the FTC and other federal agencies to establish standards for financial institutions relating to administrative, technical, and physical safeguards for certain information.[3] Pursuant to the GLBA's directive, the Commission promulgated the Safeguards Rule in 2002, which requires financial institutions, among other things, to develop, implement, and maintain a comprehensive written information security program that contains administrative, technical, and physical safeguards that are appropriate to the institution's size and complexity, the nature and scope of the institution's activities, and the sensitivity of any customer information at issue. The Safeguards Rule became effective on May 23, 2003.

In 2019, the Commission issued an NPRM proposing certain amendments to the Safeguards Rule,[4] and specifically requesting public comment on whether the Safeguards Rule should be amended to require notice to the Commission in the event of a security event involving customer information. Upon consideration of the comments that the Commission received in response to the

[1] 84 FR 13158 (Apr. 4, 2019).
[2] 86 FR 70062 (Dec. 9, 2021).
[3] *See* 15 U.S.C. 6801(b), 6805(b)(2).
[4] 84 FR 13158 (Apr. 4, 2019).

NPRM, as well as a workshop that the Commission held in connection with the NPRM,[5] the Commission issued an SNPRM in 2021 proposing amendments to the Safeguards Rule to require financial institutions that experience a security event that meets identified criteria to promptly report the security event to the FTC.[6] The proposal was intended to facilitate the enforcement of the Rule by ensuring that the Commission is made aware of security events that may suggest that a financial institution's security program does not comply with the Rule's requirements. Compliance with the Rule is important because robust information security protects consumers from harm. In 2018, for example, almost 10 percent of Americans suffered some form of identity theft, costing many of them hundreds of dollars and dozens of hours of time.[7]

Upon consideration of the public comments, and further review by FTC staff, the Commission is now finalizing the information collection requirement that was proposed in the 2021 SNPRM, with the following minor changes. First, unlike the proposed amendments, the final rule requires notification when a financial institution discovers that unencrypted customer information has been acquired without authorization, rather than when misuse is considered likely. Because the proposed amendments would have required financial institutions that become aware of a security event to determine the likelihood that customer information has been or will be misused, this change simplifies the requirement and will make compliance with the new information collection requirement easier. Additionally, by drawing a distinction between unencrypted and encrypted customer information,[8] the finalized information collection requirement limits the burden on financial institutions by limiting the reporting requirement to security events that pose a greater risk. Second, the final rule presumes that unauthorized access results 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.

Third, while the proposed amendments would have required financial institutions to report security events that affect 1,000 or more consumers, the final rule lowers the trigger to 500 or more consumers. This lower threshold will help ensure that the Commission is aware of all security events that affect a significant number of consumers and may indicate a failure to comply with the Safeguards Rule.

Fourth, the final rule provides that public notification of breaches—but not notice to the Commission itself—should be delayed when a law enforcement official provides a written notice that the official has determined that notification would interfere with a criminal investigation or would damage national security.

Fifth, the final rule requires that the notice to the Commission must include the number of consumers affected or potentially affected by the notification event, so that the Commission will be

---

[5] *See* FTC, Information Security and Financial Institutions: An FTC Workshop to Examine Safeguards Rule Tr. (July 13, 2020), https://www ftc.gov/system/files/documents/public_events/1567141/transcript-glb-safeguards-workshop-full.pdf.

[6] 86 FR 70062 (Dec. 9, 2021). On the same date that the Commission issued the SNPRM, the Commission issued a final rule related to the NPRM's other proposals. 86 FR 70272 (Dec. 9, 2021).

[7] *See* Erika Harrell, Victims of Identity Theft, 2018, U.S. DEP'T OF JUST., at 1 (Apr. 2021), https://bjs.ojp.gov/content/pub/pdf/vit18.pdf.

[8] If the encryption key was also accessed without authorization, the customer information will be considered to be unencrypted.

better able to assess the impact of the security event.

Sixth, the final rule also adds a provision that specifies when a notification event is considered discovered for purposes of notification timing. Specifically, a notification event is treated as discovered as of the first day on which such event is known to the financial institution.

**(2) Use of the Information**

The reporting requirement will facilitate enforcement of the Rule and ensure that the Commission is aware of notification events that suggest that a financial institution's security program does not comply with the Rule's requirements. Consumers will also be able to use the information reported to and made public by the Commission to make their own determinations as to the security of their personal information in the hands of various financial institutions.

**(3) Consideration to Use Improved Information Technology to Reduce Burden**

To reduce the burden on affected financial institutions, the Commission will provide an online reporting form on the Commission's website to facilitate reporting of qualifying security events.

**(4) Efforts to Identify Duplication**

FTC staff have not identified any other sources for the covered information or any other federal statutes, rules, or policies that duplicate the notice requirement in the Rule. Many states require that covered financial institutions notify affected consumers of specified data breaches and security events, but state law requirements vary as to whether notice to relevant state regulators is required and as to whether such breach notifications are made public. Additionally, state laws do not require covered entities to notify the Commission when consumer data is or may be compromised. As a result, the notice requirement is necessary to ensure that the Commission is notified of covered security events. To the extent that state law already requires notification to consumers or state regulators, there is little additional burden in providing notice to the Commission.

**(5) Efforts to Minimize Burden on Small Businesses**

The reporting requirement will not impose a significant burden on financial institutions in general, including small businesses, and has been designed to minimize the burden on all financial institutions. For example, by limiting the reporting requirement to security events involving unencrypted customer information,[9] the reporting requirement is limited to incidents that pose a significant risk of consumer harm and suggest that a financial institution's security program does not comply with the Rule's requirements. Additionally, in order to simplify the reporting requirement and make compliance easier, the final rule requires notification when a financial institution discovers that unencrypted customer information has been acquired without authorization, rather than when misuse is considered likely, as originally proposed. This will lower the burden of determining when a report should be made.

[9] With the exception that, in instances in which an encryption key was accessed by an unauthorized person, the customer information is deemed to be unencrypted for the purpose of the Rule.

Furthermore, in most cases, the information requested by the reporting requirement is similar to information entities are already required to disclose under various states' data breach notification laws.[10] To reduce burden on affected financial institutions, the Commission will also provide an online reporting form on the Commission's website to facilitate reporting of qualifying security events. Finally, the reporting requirement would require that affected financial institutions report only information that the Commission believes financial institutions would acquire in the normal course of responding to a security event (including a general description of the event, the types of information affected, the number of consumers affected or likely affected, and the dates of the event).

**(6) Consequences of Conducting the Collection Less Frequently**

The reporting requirement only requires affected financial institutions to notify the Commission when a notification event has occurred. Permitting less frequent notifications would hinder the Commission's efforts to enforce the Safeguards Rule and prevent the Commission from receiving timely notice of notification events that indicate a financial institution's security program may not comply with the Rule's requirements. As noted above, compliance with the Rule is important because robust information security protects consumers from harm including identity theft and fraud. In addition, less frequent collection of this information could reduce the available information for consumers concerning the security of their information held by financial institutions.

**(7) Circumstances Requiring Collection Inconsistent with OMB Guidelines**

The information collection requirements are consistent with all applicable guidelines contained in 5 CFR § 1320.5(d)(2). While it is possible that financial institutions that suffer multiple triggering security events may be required to notify the Commission more than once in a single quarter, the Commission anticipates that this is unlikely to occur. Moreover, the fact that a financial institution suffered multiple triggering security events in a single quarter would be important information for the Commission in determining whether the financial institution is complying with the Safeguards Rule.

**(8) Consultation Outside the Agency**

Dating back to the Rule's inception, the Commission has had a long history of consultation with other federal and state agencies and other outside parties, including affected entities and consumers. On April 4, 2019, the Commission issued a Notice of Proposed Rulemaking ("NPRM") setting forth proposed amendments to the Safeguards Rule and requesting public comments.[11] In response, the Commission received 49 comments from various interested parties including industry groups, consumer groups, and individual consumers.[12] On July 13, 2020, the Commission held a workshop concerning the proposed changes and conducted panels with information security experts

[10] *See, e.g.*, Cal. Civil Code § 1798.82; Tex. Bus. & Com. Code § 521.053; Fla. Stat. § 501.171.
[11] 84 FR 13158 (Apr. 4, 2019).
[12] 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/docketBrowser?rpp=25&so=ASC&sb=docId&po=25&dct=PS&D=FTC- 2019-0019&refD=FTC-2019-0019-0011. The 11 relevant public comments relating to the subject matter of the July 13, 2020, workshop can be found at: https://www.regulations.gov/docketBrowser?rpp=25&so=ASC&sb=docId&po=0&dct=PS&D=FTC-2020-0038.

discussing subjects related to the proposed amendments.[13] The Commission received 11 comments following the workshop. In the NPRM, the Commission specifically requested comment on whether the Safeguards Rule should be amended to require notice to the Commission in the event of a security event. The Commission received several comments addressing the proposal.[14]

On December 9, 2021, the Commission issued an SNPRM proposing the adoption of the reporting requirement.[15] In response, the Commission received 14 comments from various interested parties, including industry groups, consumer groups, and individual consumers.[16] In the preparation of the final rule, the Commission has carefully considered the comments received throughout the rulemaking proceeding.

**(9) Payments or Gifts to Respondents**

Not applicable.

**(10) & (11) Assurances of Confidentiality/Matters of a Sensitive Nature**

The collection of information in the proposed reporting requirement is consistent with all applicable confidentiality and similar guidelines contained in 5 CFR § 1320.5(d)(2).

**(12) Estimated Annual Hours Burden and Associated Labor Cost**

**Estimated Annual Hours Burden: 575 hours**

**Associated Labor Cost: $37,950**

FTC staff estimates that the reporting requirement will affect approximately 115 financial institutions each year.[17] FTC staff estimates that compliance with this reporting requirement will require approximately five hours for affected financial institutions, for a total annual burden of approximately 575 hours (115 responses × 5 hours). FTC staff anticipates that the burden associated with the reporting requirement will consist of the time necessary to compile and report the requested

---

[13] *See* FTC, Information Security and Financial Institutions: An FTC Workshop to Examine Safeguards Rule Tr. (July 13, 2020), https://www.ftc.gov/system/files/documents/public_events/1567141/transcript-glb-safeguards- workshop-full.pdf.

[14] National Independent Automobile Dealers Association, Comment 48 at 7; American Council on Education, Comment 24 at 15; Consumer Reports, Comment 52 at 6; Princeton University Center for Information Technology Policy, Comment 54 at 7; Credit Union National Association, Comment 30 at 2; Heartland Credit Union Association, Comment 42 at 2; National Association of Federally-Insured Credit Unions, Comment 43 at 1-2.

[15] 86 FR 70062 (Dec. 9, 2021).

[16] 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.

[17] 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, 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. Although this number may exclude some entities that are covered by the Safeguard Rule but are not contained in the "Banking/Credit/Financial" category, not every security event will trigger the reporting obligations in the proposed requirement. Therefore, the Commission estimated in the SNPRM that 110 institutions would have reportable events. 86 FR 70062 (Dec. 9, 2021). Because of the change in the reporting threshold the Commission expects an additional 5 entities to have reporting obligations under the final rule.

information via the electronic form located on the Commission's website. The Commission does not believe that the reporting requirement will impose any new investigative costs on financial institutions. As noted above, the information requested by the reporting requirement is (1) information that financial institutions acquire in the normal course of responding to a security event, and (2) similar to information entities are already required to disclose under various states' data breach notification laws.[18]

The estimated labor cost reflects the hourly wages necessary to prepare the required reports. FTC staff anticipates that the 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 $57.63 (3 hours × $57.63 = $172.89).[19] 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).[20] 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).

**(13) Estimated Annual Capital or Other Non-Labor Costs**

Covered financial institutions are not likely to require any significant capital costs to comply with the reporting requirement. To reduce burden on affected financial institutions, the Commission will provide an online reporting form on the Commission's website to facilitate reporting of qualifying security 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.

**(14) Estimated Cost to the Federal Government**

FTC staff anticipates that the cost to the Federal Government for administering the final rule will be limited. FTC staff estimates that the Commission may incur approximately $18,903 per year ($56,709 over three years) as the cost to the Federal Government for implementing the amendments. This estimate is based on the assumption that one-eighth of an attorney work year may be expended in administering this program. In addition, the Commission will incur de minimis costs in creating an electronic form for affected financial institutions to allow reporting of security events.

**(15) Program Changes/Adjustments**

---

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

[19] 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.

[20] 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. Although the reporting requirement will largely be administrative, the Commission understands that affected financial institutions may engage attorneys to comply with the reporting requirement.

As described above, the amendments will result in an estimated 575 burden hours, annualized, as well as $37,950 in labor costs.

**(16) Statistical Use of Information**

There are no plans to publish any information for statistical use.

**(17) Exceptions for the Display of Expiration Date for OMB Approval**

Not applicable.

**(18) Exceptions to Certification**

The FTC certifies that this collection of information is consistent with the requirements of 5 CFR § 1320.9, and the related provisions of 5 CFR § 1320.8(b)(3), and is not seeking an exemption to these certification requirements.