**Federal Trade Commission**
**Supporting Statement for Standards for Safeguarding Customer Information**
**16 CFR Part 314**
**OMB Control No. 3084-XXXX**

The Federal Trade Commission ("FTC" or "Commission") proposes amendments to the Commission's Standards for Safeguarding Customer Information ("Safeguards Rule"), 16 CFR part 314, to require financial institutions to report to the Commission any security event where the financial institutions have determined misuse of customer information has occurred or is reasonably possible and that at least 1,000 consumers have been affected or reasonably may be affected.

## (1) Necessity for Collecting the Information

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 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 Federal Trade Commission ("FTC" or "Commission") and other federal agencies to establish standards for financial institutions relating to administrative, technical, and physical safeguards for certain information.[2] Pursuant to the Act's directive, the Commission promulgated the Safeguards Rule in 2002. The Safeguards Rule became effective on May 23, 2003. In 2020, the Commission amended the Safeguards Rule in five main ways. First, it added provisions designed to provide covered financial institutions with more guidance on how to develop and implement specific aspects of an overall information security program, such as access controls, authentication, and encryption. Second, it added provisions designed to improve the accountability of financial institutions' information security programs, such as by requiring periodic reports to boards of directors or governing bodies. Third, it exempted financial institutions that collect less customer information from certain requirements. Fourth, it expanded the definition of "financial institution" to include entities engaged in activities that the Federal Reserve Board determines to be incidental to financial activities. Finally, the Commission defined several terms and provided related examples in the Rule itself rather than incorporate them by reference from the Privacy of Consumer Financial Information Rule, 16 CFR part 313.

In this rulemaking, the Commission is proposing to amend the Safeguards Rule to require financial institutions that suffer a security event that meets identified criteria to promptly report the security event to the FTC. The proposed amendment is designed to ensure that the Commission is aware of security events that could suggest that a financial institution's security

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

program does not comply with the Rule's requirements, thus facilitating enforcement of the Rule.

**(2) Use of the Information**

The proposed reporting requirement would facilitate Commission enforcement of the Rule and ensure that the Commission is aware of security events that could 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 the Commission to determine 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 burden on affected financial institutions, the Commission proposes to 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 proposed 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. State laws do not require covered entities to notify the Commission when consumer data is or may be compromised. As a result, the proposed rule 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, moreover, there is little additional burden in providing notice to the Commission as well.

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

The proposed reporting requirement has been designed to minimize the burden on all financial institutions, including small businesses. The proposed rule requires that only security events involving at least 1,000 consumers must be reported, which will reduce potential burden on small businesses that retain information on fewer consumers. The rule minimizes burden on all covered financial institutions, including small business, by providing for reporting through an online form on the Commission's website. Finally, the proposed 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 (i.e., a general description of the event, the types of information affected, and the dates of the event).

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

The proposed reporting requirement only requires affected financial institutions to notify the Commission when a triggering security 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 security events that indicate a financial institution's security program may not comply with the Rule's requirements. 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 proposed information collection requirements are consistent with all applicable guidelines contained in 5 C.F.R. § 1320.5(d)(2). While it is possible that a 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, 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. Most recently, 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.[3] In response, the Commission received 49 comments from various interested parties including industry groups, consumer groups, and individual consumers.[4] 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.[5] 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 notifying the Commission in the event of a security event. The Commission

---

[3] FTC Notice of Proposed Rulemaking, 84 FR 13158 (April 4, 2019).

[4] 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.

[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.

received several comments addressing the proposal.[6] Consistent with 5 CFR § 1320.12(c), the FTC is seeking public comment on the proposed new reporting requirement and the associated PRA burden contemporaneous with this submission.

**(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**

**Total Estimated Hours Burden of the Proposed Rulemaking: 550 hours**
**Total Associated Labor Cost: $31,900**

Burden estimates below are based on the Commission's enforcement experience in administering the Safeguards Rule and addressing data breaches, the rulemaking record, and relevant industry data.

The proposed reporting rule requires covered financial institutions to report to the Commission any security event in which the misuse of customer information has occurred or is reasonably likely and that affects, or reasonably may affect, at least 1,000 consumers. Affected financial institutions would be required to report the following information regarding a covered security event: (1) the name and contact information of the reporting financial institution; (2) a description of the types of information that were involved in the security event; (3) if the information is possible to determine, the date or date range of the security event; and (4) a general description of the security event. Affected financial institutions would be required to report this information via an online reporting form on the Commission's website.

FTC staff estimates that the proposed reporting requirement will affect approximately 110 financial institutions each year.[7] FTC staff estimates that compliance with this reporting requirement will require approximately five hours for affected financial institutions, for a total

[6] 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..

[7] 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 believes 110 to be a reasonable estimate.

annual burden of approximately **550 hours** (110 responses × 5 hours). FTC staff anticipates that the burden associated with the proposed reporting requirement will consist of the time necessary to compile and report the requested information via the electronic form located on the Commission's website. The Commission does not believe that the proposed reporting requirement would impose any new investigative costs on financial institutions. The information about security events requested in the proposed reporting requirement (i.e., a general description of the event, the types of information affected, and the dates of the event) is information the Commission believes financial institutions would acquire in the normal course of responding to a security event. In addition, in most cases, the information requested by the proposed reporting requirement is similar to information entities are already required to disclose under various states' data breach notification laws.[8]

FTC staff derives the associated labor cost by calculating the hourly wages necessary to prepare the required reports. Staff anticipates that required information will be compiled by information security analysts in the course of assessing and responding to a security event, resulting in 3 hours of labor at a mean hourly wage of $50.10 (3 hours × $50.10 = $150.30).[9] 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 $69.86 (2 hours × $69.86 = $139.72).[10] Accordingly, FTC staff estimates that the approximate labor cost to be $290 per report (rounded to the nearest dollar). This yields a total annual cost burden of **$31,900** (110 annual responses × $290).

## (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 proposed reporting requirement. To reduce burden on affected financial institutions, the Commission proposes to 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 proposed reporting requirement.

## (14) Estimated Cost to the Federal Government

FTC staff anticipates that the cost to the FTC for administering the proposed Rule changes will be limited. FTC staff estimates that the Commission may incur approximately $22,067 per year as the cost to the Federal Government for implementing the proposed amendments. This estimate is based on the assumption that one-eighth of an attorney work year

---

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

[9] This figure is derived from the mean hourly wage for Information security analysts. 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.

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

may be expended in administering this program. In addition, the Commission may incur *de minimis* costs in creating an electronic form for affected financial institutions to allow reporting of security events.

**(15) Program Changes/Adjustments**

As described above, the proposed amendments will result in an estimated 550 burden hours, annualized, as well as $31,900 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.