[Billing Code: 6750-01-S]

FEDERAL TRADE COMMISSION

16 CFR Part 314

RIN 3084-AB35

Standards for Safeguarding Customer Information

AGENCY: Federal Trade Commission ("FTC" or "Commission").

ACTION: Supplemental notice of proposed rulemaking; request for public comment.

SUMMARY: The Commission requests public comment on its proposal to further amend the Standards for Safeguarding Customer Information ("Safeguards Rule" or "Rule") 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 likely and that at least 1,000 consumers have been affected or reasonably may be affected.

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

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

Commission, Office of the Secretary, Constitution Center, 400 7th Street S.W., 5th Floor, Suite 5610 (Annex B), Washington, D.C. 20024.

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

SUPPLEMENTARY INFORMATION:

I. Background

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

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

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

II. Regulatory Review of the Safeguards Rule

On September 7, 2016, the Commission solicited comments on the Safeguards Rule as part of its periodic review of its rules and guides.[3] The Commission sought comment on a number of general issues, including the economic impact and benefits of the Rule; possible conflicts between the Rule and state, local, or other federal laws or regulations; and the effect on the Rule of any technological, economic, or other industry changes. The Commission received 28 comments from individuals and entities representing a wide range of viewpoints.[4] Most commenters agreed that there is a continuing need for the Rule and that it benefits consumers and competition.[5]

On April 4, 2019, the Commission issued a Notice of Proposed Rulemaking (NPRM) setting forth proposed amendments to the Safeguards Rule.[6] In response, the Commission received 49 comments from various interested parties including industry groups, consumer groups, and individual consumers.[7] On July 13, 2020, the Commission held a workshop concerning the proposed changes and conducted panels with

---

[3] Safeguards Rule, Request for Comment, 81 FR 61632 (Sept. 7, 2016).
[4] The 28 public comments received prior to March 15, 2019, are posted at: https://www.ftc.gov/policy/public-comments/initiative-674.
[5] *See, e.g.*, Mortgage Bankers Association, (comment 39); National Automobile Dealers Association, (comment 40; Data & Marketing Association, (comment 38); Electronic Transactions Association, (comment 24; State Privacy & Security Coalition, (comment 26).
[6] FTC Notice of Proposed Rulemaking ("NPRM"), 84 FR 13158 (April 4, 2019).
[7] 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. 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

information security experts discussing subjects related to the proposed amendments.[8] The Commission received 11 comments following the workshop. After reviewing the initial comments to the NPRM, conducting the workshop, and then reviewing the comments received following the workshop, the Commission issued final amendments to the Safeguards Rule on XXXXX.

III. Proposal for Requirement that Financial Institutions Report Security Events to the Commission

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, federal agencies enforcing the GLBA have required financial institutions to provide notice to the regulator, and in some instances notice to consumers as well, for many years.[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

---

[8] *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.

[9] NPRM, 84 FR at 13163.

[10] *Id*. at 13169.

[11] See Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (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), 70 FR 15736, 15752 (Mar. 29, 2005), https://www.occ.treas.gov/news-issuances/federal-register/2005/70fr15736.pdf ("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").

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 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]

Several commenters supported adding a reporting requirement.[13] For example, the Princeton University Center for Information Technology Policy ("PUCITP") noted that such a reporting requirement would "provide the Commission with valuable information about the scope of the problem and the effectiveness of security measures across different entities" and that it would "also help the Commission coordinate responses to shared threats."[14] PUCITP also recommended that all security events that affect a certain number of customers should be reported without regard to the likelihood of harm and that such reports should be made public.[15] The National Association of Federally-Insured Credit Unions ("NAFCU") argued that requiring financial institutions to report security events to the Commission would provide an "appropriate incentive for covered financial companies to disclose information to consumers and relevant regulatory

[12] *Id*.
[13] 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.
[14] Princeton University Center for Information Technology Policy, (comment 54), at 7.
[15] *Id*.

bodies."[16] NAFCU also suggested that notification requirements are important because they "ensure independent assessment of whether a security incident represents a threat to consumer privacy."[17]

Two commenters opposed the inclusion of a reporting requirement.[18] The American Council on Education ("ACE") argued that such a requirement "would simply add another layer on top of an already crowded list of federal and state law enforcement contacts and state breach reporting requirements."[19] ACE also suggested that any notification requirement should be limited to a more restricted definition of "security event" than the definition in the proposed Rule, so that financial institutions would only be required to report incidents that could lead to consumer harm.[20] The National Independent Automobile Dealers Association noted that it "objects to any proposed amendment that would require a financial institution to report security events to the FTC."[21]

After reviewing the comments, the Commission proposes 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. Such reports would ensure that the Commission is aware of security 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. While many states already require notice of certain breaches, the state law requirements vary as to whether notice to the state regulator is required and as to whether such breach notifications are

---

[16] National Association of Federally-Insured Credit Unions, (comment 43), at 1.
[17] *Id*. at 1-2.
[18] National Independent Automobile Dealers Association, (comment 48), at 7; American Council on Education, (comment 24), at 15.
[19] American Council on Education, (comment 24), at 15.
[20] *Id.*
[21] National Independent Automobile Dealers Association, (comment 48), at 7.

made public. 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. In order to address concerns expressed by commenters that a reporting requirement would add additional burden to financial institutions, the Commission proposes limiting the reporting requirement to only those security events where the financial institutions determine that misuse of customer information has occurred or is reasonably likely, and where at least 1,000 consumers have been affected or reasonably may be affected.[22] The notice to the Commission would involve a limited set of information, as typically required under existing breach notification requirements.[23] Financial institutions would be required to promptly provide the Commission: (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. To further reduce costs, the Commission proposes the notice be provided electronically through a form located on the FTC's website, https://www.ftc.gov.

The Commission will input the information it receives from affected financial institutions into a database that it will update periodically and make available to the public. The FTC does not believe the information to be provided to the Commission under the proposed reporting requirement will include confidential or proprietary

[22] *See* Princeton University Center for Information Technology Policy, (comment 54), at 7 (endorsing notification requirement for events that affect at least a certain number of consumers).
[23] *See, e.g.,* 23 CRR-NY 500.17; Cal. Civil Code 1798.82; Tex. Bus. & Com. Code 521.053; Fla. Stat. 501.171.

information and, as a result, does not anticipate providing a mechanism for financial institutions to request confidential treatment of the information.

The Commission invites comments on its proposed amendment requiring financial institutions to report certain security events to the Commission. Specifically, commenters may wish to address the following:

(1) The information to be contained in any notice to the Commission. Is the proposed list of elements sufficient? Should there be additional information? Less?

(2) Whether the Commission's proposed threshold for requiring notice – for those security events for which misuse of the information of 1,000 or more consumers has occurred or is reasonably likely to occur – is the appropriate one. What about security events in which misuse is possible, but not likely? Should there be a carve-out for security events solely involving encrypted data?

(3) The timing for notification to be given to the Commission. Is the current proposal of a maximum of 30 days after discovery of the security event reasonable? Is a shorter period practicable?

(4) Whether the requirement should allow law enforcement agencies to prevent or delay notification if notification to the Commission would affect law-enforcement investigations. The proposed rule does not include such a requirement. Comments are also welcome on whether such a law enforcement right to prevent or delay notification is only necessary to the extent that notices are made public.

(5) Whether the information reported to the Commission should be made public. Should the Commission permit affected financial institutions to request confidential treatment of the required information? If so, under what circumstances? Should affected financial

institutions be allowed to request delaying the public publication of the security event information and, if so, on what basis?

(6) Whether, instead of implementing a stand-alone reporting requirement, the Commission should only require notification to the Commission whenever a financial institution is required to provide notice of a security event or similar to a governmental entity under another state or federal statute, rule, or regulation. How would such a provision affect the Commission's ability to enforce the Rule? Would such an approach affect the burden on financial institutions? Would such an approach generate consistent reporting due to differences in applicable laws?

(7) Whether a notification requirement should be included at all.

(8) Whether notification to consumers, as well as to the Commission, should be required, and if so, under what circumstances.

IV. Section-by-Section Analysis

Proposed Amendments to Section 314.4: Elements

The proposed amendment to Section 314.4 would add a new paragraph (j). Proposed paragraph (j) would require financial institutions that experience a security event in which the misuse of customer information has occurred or is reasonably likely, and at least 1,000 consumers have been affected or reasonably may be affected, to provide notice of the security event to the Commission. Proposed paragraph (j) would also require that any such notice be made electronically on a form on the FTC's website, https://www.ftc.gov, within 30 days from discovery of the security event and 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 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.

Proposed Amendments to Section 314.5: Effective Date

The proposed amendment to Section 314.5 states that the proposed reporting requirement would not be effective until six months after the publication of a final rule. The effective date of this element would be delayed to allow financial institutions appropriate time to incorporate such a reporting requirement into their security event response plans. All other requirements under the Safeguards Rule would remain in effect during this six-month period. The Commission welcomes comment on this approach.

V. Request for Comment

You can file a comment online or on paper. For the Commission to consider your comment, we must receive it on or before [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]. Write "Safeguards Rule, 16 CFR Part 314, Project No. P145407" on the comment. Postal mail addressed to the Commission is subject to delay due to heightened security screening. As a result, we encourage you to submit your comments online. To make sure that the Commission considers your online comment, you must file it through the https://www.regulations.gov website by following the instructions on the web-based form provided. Your comment, including your name and your state – will be placed on the public record of this proceeding, including the https://www.regulations.gov website.

If you file your comment on paper, write "Safeguards Rule, 16 CFR Part 314, Project No. P145407" on your comment and on the envelope, and mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600

Pennsylvania Avenue, NW, Suite CC-5610 (Annex J), Washington, DC 20580, or deliver your comment to the following address: Federal Trade Commission, Office of the Secretary, Constitution Center, 400 7th Street SW, 5th Floor, Suite 5610, Washington, DC 20024. If possible, please submit your paper comment to the Commission by courier or overnight service.

Because your comment will be placed on the public record, you are solely responsible for making sure that your comment does not include any sensitive or confidential information. In particular, your comment should not include any sensitive personal information, such as your or anyone else's Social Security number, date of birth, driver's license number or other state identification number or foreign country equivalent, passport number, financial account number, or credit or debit card number. You are also solely responsible for making sure that your comment does not include any sensitive health information, such as medical records or other individually identifiable health information. In addition, your comment should not include any "trade secret or any commercial or financial information which . . . is privileged or confidential," as provided by Section 6(f) of the FTC Act, 15 U.S.C. 46(f), and FTC Rule 4.10(a)(2), 16 CFR 4.10(a)(2), including in particular, competitively sensitive information such as costs, sales statistics, inventories, formulas, patterns, devices, manufacturing processes, or customer names.

Comments containing material for which confidential treatment is requested must be filed in paper form, must be clearly labeled "Confidential," and must comply with FTC Rule 4.9(c). In particular, the written request for confidential treatment that accompanies the comment must include the factual and legal basis for the request and

must identify the specific portions of the comments to be withheld from the public record. *See* FTC Rule 4.9(c). Your comment will be kept confidential only if the General Counsel grants your request in accordance with the law and the public interest. Once your comment has been posted on the public website—as legally required by FTC Rule 4.9(b)—we cannot redact or remove your comment from the FTC website, unless you submit a confidentiality request that meets the requirements for such treatment under FTC Rule 4.9(c), and the General Counsel grants that request.

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

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

Written communications and summaries or transcripts of oral communications respecting the merits of this proceeding, from any outside party to any Commissioner or Commissioner's advisor, will be placed on the public record.[24]

VII. 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

[24] *See* 16 CFR 1.26(b)(5).

regulations implementing the PRA (5 CFR 1320.8(b)(2)(vi)), an agency may not collect or sponsor the collection of information, nor may it impose an information collection requirement, unless it displays a currently valid OMB control number.

The proposed reporting requirement discussed above constitutes a "collection of information" for purposes of the PRA.[25] As required by the PRA, the FTC has submitted this proposed information collection requirement to OMB for its review, and staff has estimated the paperwork burden for this requirement as set forth below.

The proposed reporting requirement will only affect those financial institutions that suffer a 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. Therefore, FTC staff estimates that the proposed reporting requirement will affect approximately 110 financial institutions each year.[26] FTC staff anticipates that the burden associated with the proposed 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 **550 hours** (110 responses × 5 hours).

The Commission does not believe that the proposed reporting requirement would impose any new investigative costs on financial institutions. The information about

---

[25] 44 U.S.C. 3502(3)(A)(i).

[26] 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 Safeguards 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.

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 many cases, the information requested by the proposed reporting requirement is similar to information entities are required to disclose under various states' data breach notification laws.[27] As a result, FTC staff estimates that the additional costs imposed by the proposed 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. 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).[28] 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).[29] Accordingly, FTC staff estimates 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).

---

[27] *See, e.g.,* Cal. Civil Code 1798.82; Tex. Bus. & Com. Code 521.053; Fla. Stat. 501.171.
[28] 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.
[29] 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.

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.

Pursuant to Section 3506(c)(2)(A) of the PRA, the FTC invites 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. All comments should be filed as prescribed in the ADDRESSES section above and must be received on or before [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*].

Comments on the proposed information collection requirements subject to review under the PRA should also be submitted to OMB. If sent by U.S. mail, comments should be addressed to Office of Information and Regulatory Affairs, Office of Management and Budget, Attention: Desk Officer for the Federal Trade Commission, New Executive Office Building, Docket Library, Room 10102, 725 17th Street NW, Washington, DC 20503. Comments can also be sent by email to MBX.OMB.OIRA.Submission@OMB.eop.gov.

VIII. Regulatory Flexibility Act

The Regulatory Flexibility Act ("RFA"), as amended by the Small Business Regulatory Enforcement Fairness Act of 1996, requires an agency to either provide

an Initial Regulatory Flexibility Analysis with a proposed rule, or certify that the proposed rule will not have a significant impact on a substantial number of small entities.[30] The Commission recognizes some affected entities may qualify as small businesses under the relevant thresholds. However, the Commission does not expect that the proposed reporting requirement, if adopted, would have the threshold impact on small entities. The proposed reporting requirement will apply to financial institutions that, in many instances, already have an obligation to disclose similar information under certain state laws.

This document serves as notification to the Small Business Administration of the agency's certification of no effect. Although the Commission certifies under the RFA that these proposed amendments would not, if promulgated, have a significant impact on a substantial number of small entities, the Commission has determined it is appropriate to publish an Initial Regulatory Flexibility Analysis to inquire into the impact of the proposed amendments on small entities. The Commission invites comment on the burden on any small entities that would be covered and has prepared the following analysis:

1. Reasons for the Proposed Rule

The proposed reporting requirement would ensure that the Commission is aware of security 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

[30] 5 U.S.C. 603 *et seq*.

information will also assist consumers by providing information as to the security of their personal information in the hands of various financial institutions.

2. Statement of Objectives and Legal Basis

The objectives of the proposed reporting requirement are discussed above. The legal basis for the proposed requirement is Section 501(b) of the GLBA.

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

Determining a precise estimate of the number of small entities[31] is not readily feasible. Financial institutions already covered by the Safeguards Rule include lenders, financial advisors, loan brokers and servicers, collection agencies, financial advisors, tax preparers, and real estate settlement services, to the extent that they have "customer information" within the meaning of the Rule. However, it is not known how many of these financial institutions are small entities. The Commission requests comment and information on the number of small entities that would be affected by the proposed reporting requirement.

4. Projected Reporting, Recordkeeping, and Other Compliance Requirements

[31] The U.S. Small Business Administration Table of Small Business Size Standards Matched to North American Industry Classification System Codes ("NAICS") are generally expressed in either millions of dollars or number of employees. A size standard is the largest that a business can be and still qualify as a small business for Federal Government programs. For the most part, size standards are the annual receipts or the average employment of a firm. Depending on the nature of the financial services an institution provides, the size standard varies. By way of example, mortgage and nonmortgage loan brokers (NAICS code 522310) are classified as small if their annual receipts are $8 million or less. Consumer lending institutions (NAICS code 52291) are classified as small if their annual receipts are $41.5 million or less. Commercial banking and savings institutions (NAICS codes 522110 and 522120) are classified as small if their assets are $600 million or less. Assets are determined by averaging the assets reported on businesses' four quarterly financial statements for the preceding year. The 2019 Table of Small Business Size Standards is available at https://www.sba.gov/document/support--table-size-standards.

The proposed notification requirement imposes reporting requirements within the meaning of the PRA. The Commission is seeking clearance from OMB for these requirements.

Specifically, as outlined above, the proposed reporting requirement will apply to financial institutions that experience a security event in which the misuse of customer information has occurred or is reasonably likely and affects, or reasonably may affect, at least 1,000 consumers. If such an event occurs, the affected financial institution may expend costs to provide the Commission with the information required by the proposed reporting requirement. As noted in the PRA analysis above, the estimated annual cost burden for all entities subject to the proposed reporting requirement will be approximately $31,900.

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

The Commission has not identified any other federal statutes, rules, or policies currently in effect that would conflict with the proposed reporting requirement. The Commission invites comment on any potentially duplicative, overlapping, or conflicting federal statutes, rules, or policies.

6. Discussion of Significant Alternatives to the Proposed Amendment

In drafting the proposed reporting requirement, the Commission has made every effort to avoid unduly burdensome requirements for entities. The proposed reporting requirement only requires that affected financial institutions provide the Commission with information necessary to assist it in the Commission's regulatory and enforcement efforts. The proposed rule minimizes burden on all covered financial institutions,

including small business, by providing for reporting through an online form on the Commission's website.

In addition, 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 Commission has invited comment on the 1,000-consumer threshold and whether an alternative threshold would better serve the goal of ensuring that security events are reported while minimizing burden on covered institutions.

The Commission welcomes comment on any significant alternative consistent with the GLBA that would minimize the impact on small entities of the proposed reporting requirement.

List of Subjects in 16 CFR Part 314

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

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

PART 314—STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

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

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

2. Revise Section 314.4 as follows:

§ 314.4 Elements.

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

* * * * *

(j) When you become aware of a security event, promptly determine the likelihood that customer information has been or will be misused. If you determine that misuse of customer information has occurred or is reasonably likely and that at least 1,000 consumers have been affected or reasonably may be affected, 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:

(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.

3. Revise Section 314.5 as follows:

§ 314.5 Effective date.

Section 314.4(j) is effective as of [SIX MONTHS AFTER DATE OF PUBLICATION OF THE FINAL RULE IN THE *FEDERAL REGISTER*].

By direction of the Commission.

April J. Tabor

Acting Secretary